

MANUAL DE CONFIGURACIÓN AVANZADA 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:

- 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.

🚼 vApp01 Running												
vApp Diagram Virtual Machin	vApp Diagram Virtual Machines Networking											
+ 🖻 🕨 💷	S 💿 🔅 -											
Console	Name 1 🛦	Status	OS	Networks	IP Address	Extern						
e e e e e e e e e e e e e e e e e e e	🛱 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.

A	Configure Services: GTW01				3	8									
)-C	DHCP NAT Firewall Add Load Balancer Member	Static Routing VPN L	oad Balancer Pool Servers Virtual Ser	vers	Q	*									
1	Name & Description Configure Service Select the services supported by this pool.														
	Configure Service	Enable	Service	Balancing Method	Port	1 1									
I	Configure Health-Check		нттр	Round Robin 💌	80]									
	Manage wembers	\checkmark	HTTPS	Round Robin 💌	443	1									
I	Ready to Complete		ТСР	Round Robin		j									
I															
I															
		Load balancing algorithms d and Least Connected.	etermine how traffic is distributed across	pool members. Supported balancing algo	rithms are IP Hash, Round Robin, URI,										

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

organizacion01 ×							_				226.1	and the second se	
All My Cloud	atalogs 🔄 A	Configure Services: GTW01		-		_	-				0	(*)	
ion	NDC.C	DHCP NAT Firewall	Static Rout										
sources	VApps												
ont dens	+ -	Add Load Balancer Memb	Add Load Balancer Member Pool										A
IDG-Org01	g GTW01	Name & Description	Configure Define the	Health-Cl	neck saith check paran	neters for ea	ich se	rvice.				- attents	e Deganization VDC Nati
t & Found		Configure Service	Service	Port	Mamitor Port	Mode		Interval (sec)	Timeout (sec)	Health Threshold	Unhealth Threshold		
toral .		Configure Health-Check	HTTP	80	80	HTTP	-	5	15	2	3		
all		Ready to Complete	HTTPS	443	443	SSL	•	5	15	2	3		
ip des			TCP			TCP		5	15	2	3		
est Personalization													
adata			D										

Puede configurar también una URI concreta para monitorizar el servicio:





Agregar las IPs privadas de los servidores Web:

lay Cloud	Catalogs 👫 A	Configure Services: GTW01					0	×		
	The vDC-C	DHCP NAT Firewall	Static Routing VPN	Load Balancer				1		
ies staaratara	vApps			Pool Servers	Virtual Servers					
nacemens	+ @-	Add Load Balancer Memb	er Pool	_			 (*) 			All
)rg01	CTW01	Name & Description	Manage Members Add back-end server	sata-crita	9.2	# Organis				
bund		Conligure Service	10 4 4 4 4 4	Ratio Weight		Service and health che				
		Configure Health-Check	IF Address	Nabo Weght	Service	Port	Monitor Port			
		Manage Members Ready to Complete	192.168.90.3	1	HTTP HTTPS	80 443	80 443			
			192.168.90.4	1	HTTP HTTPS	80 443	80 443			
rsonalization										

Finalizar el asistente.

Comprobar los datos de configuración:

	ž												
atalogs 👫 A	Configure Services:	GTW01								0			
S vDC-C	DHCP NAT	Firewall Stat	tic Routing V	PN Load Ba	lancer								
vApps					Pool Servers	Virtual Serve	Irs						
+ 0-	Pool is a constru	uct used to man	age and share t	the backend m	ember instances	s more flexibly a	nd efficiently. A po	ol manages its ba	ickend membe	rs <mark>, health-check</mark>			
	monitors and lo	adbalancer distr	ibution method.				Service and	health check			40	etworks	The Lase
GTW01	Name	Description	Members	Status	Service	Port	Monitor Port	Balancing Method	Interval (sec)	Timeout (sec)			2 2
	Grupos de Ser	Grupo de servi	2	0	HTTP HTTPS	80 443	80 443	Round Robin Round Robin	5 5	15 15			
	atalogs 🐴 A vApps • 🖉 CTW01	Atalogs A Configure Services: A VDC-C VApps Configure Services: DHCP NAT Pool is a constr monitors and lo Name Grupos de Ser	Configure Services: GTW01 Configure Services: GTW01 Configure Services: GTW01 DHCP NAT Firewall State Vepps Pool is a construct used to man monitors and loadbalancer dist Name Description Grupos de Ser Grupo de servi	atalogs Configure Services: GTW01 Image: Configure Services: GTW01	Configure Services: GTW01 YADC C DHCP NAT Firewall Static Routing VPN Load Bar VAPps Pool is a construct used to manage and share the backend me monitors and loadbalancer distribution method. Variation Rame Description Members Status Variation Grupos de Ser Grupo de service 2 2	Configure Services: GTWD1 Configure Services: GTWD1 DHCP NAT Firewall Static Routing VPN Load Balancer Pool Servers Pool Servers Pool Servers Pool Servers Pool Servers Convol Name Description Members Status Service Grupos de Ser Grupo de serv 2 Pool HTTP HTTP	Configure Services: GTW01 Proc. VAPps Pool is a construct used to manage and share the backend member instances more flexibly a monitors and loadbalancer distribution method. Name Description Name Description Grupos de Ser Grupo de servi 2 HTTP 80 HTTP 80 HTTP 80	Configure Services: GTW01 Procession Procession Pool is a construct used to manage and share the backend member instances more flexibly and efficiently. A pomonitors and loadbalancer distribution method. Pool is a construct used to manage and share the backend member instances more flexibly and efficiently. A pomonitors and loadbalancer distribution method. Name Description Members Status Services Post Member Post Grupos de Ser Grupo de servi 2 Image: Add	Configure Services: GTW01 Op/C Op/C VApps Pool Servers Virtual Servers Pool is a construct used to manage and share the backend member instances more flexibly and efficiently. A pool manages its bamonitors and loadbalancer distribution method. Service Pool Members Name Description Members Status Service Poil Members Service Poil Members Balancing Method Grupos de Ser Grupo de servi 2 Image: Poil HTTP 80 80 Round Robin	Configure Services: GTW01 Image: Static Routing VPN Load Balancer Pool Servers Virtual Servers Service and health check Service and health check Grupps de Ser Grup de servi 2 HTTP 80 80 Round Robin 5 Grund Robin 5 Service Pool HTTP 80 80 Round Robin 5	Status Configure Services: GTW01 Proof Service Urbual Service Pool is a construct used to manage and share the backend member instances more flexibly and efficiently: A pool manages its backend members, health-check monitors and loadbalancer distribution method. Name Description Members Status Service and health check Grupos de Ser Grupo de servi 2 Part HTTP 80 80 Round Robin 5 15	Configure Services: GTW01 Image: Configure Services: GTW01 WDC-C VAPps Pool is a construct used to manage and share the backend member instances more flexibly and efficiently. A pool manages its backend members, health-check monitors and loadbalancer distribution method. Pool is a construct used to manage and share the backend member instances more flexibly and efficiently. A pool manages its backend members, health-check Mame Description Mame Description GTW01 Stetus Services Port Members Stetus Services Port Members Stetus Services Port Members 15 HTTPS 443 Round Robin 5 15	Configure Services: GTW01 Image: Configure Services: GTW01 Image: Construct used to manage and share the backend member instances more flexibly and efficiently. A pool manages its backend members, health-check monitors and loadbalancer distribution method. Image: Construct used to manage and share the backend member instances more flexibly and efficiently. A pool manages its backend members, health-check monitors and loadbalancer distribution method. Image: Construct used to manage and share the backend member instances more flexibly and efficiently. A pool manages its backend members, health-check monitors and loadbalancer distribution method. Image: Construct used to manage and share the backend member instances more flexibly and efficiently. A pool manages its backend members, health-check monitors and loadbalancer distribution method. Image: Construct used to manage and share the backend member instances more flexibly and efficiently. A pool manages its backend members, health-check monitors and loadbalancer distribution method. Image: Construct used to manage and share the backend member instances more flexibly and efficiently. A pool manages its backend members, health-check monitors and loadbalancer distribution method. Image: Construct used to manage and share the backend m

Dar ok para terminar.



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.

VDC-Ora01	Configure Services	GTW01	_	_	_	_	Add Virtual Server						9	
vApps vApp Templates Me-	DHCP NAT	Firewall Static	Routing VPN	Load Balancer	Load Balancer			Vi	rtual Server (Grupo !			*	
+ @-				Poo	Servers Virtual	Servers	Descript	on:						
Nama	Virtual server is a highly scalable and highly available server built on a cluster or real servers called me transmared to lengate, and the tenants interact with the cluster system as if it were only a signification of													
GTW01	The second se	Name 19 Address Description		Serv		Services	Applied	n: E	ternal-VLAN-1854 *		•			
	Ziame	IP Address	Description		Name	Pon	IP addre	10	0.8.8.243		-	*		
							Pool: Services	G	rupos de Ser	vidores 1	•	Supports (HTTP,HTTPS)		
							Enabled	Nama	Port	Persistence k	lethod	Coolie name	Coo	Ale mode
							Z	HTTP	80	None				
								HTTPS	443	Session Id	+			
								TCP		None	T.			
							Enabl	ed etwork tra	affic for virtu:	al server				

Crear ahora las reglas del Firewall correspondientes:

ogs 🚳 Administration	Configure Services: G	5TW01						0		
vApps vApp Templates Me	DHCP NAT	Firewall Static Routing VPN	Load Balancer							
• 🔯•	Rules can be add dropping them at	led to the Firewall to allow or deny the desired location in the list. Th	specific network traffic. The or e order of any selected rules is	der of these rules ca preserved after drop	n be changed oping them int	by selecting o a different lo	ne or more ation withi	rules, dragging and n the list.	t	All # Organiza
GTW01	Enable firewall Default action (Applicable to traffic	 Deny Allow Log that does not match the rules in the list 	vy O Allow D Log es not match the rules in the list.							2 2
	Rule Id	Name	Source	Destination	Protocol	Action	Log	Enabled		
		HTTP_BALANCEO	Any:Any	10.8.8.243:80	TCP	Allow	-	×		
		HTTPS_BALANCEO	Any:Any	10.8.8.243:443	TCP	Allow	-	*		

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



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".





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 aprovisionado.

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..."

🚹 Inicio 🛆 Mi nube 📋 Catál	ogos 🍇 Administración					
Administración	VDC_IPLAN-DEMO					
✓ Recursos de nube ✓ ⓓ Centros de datos virtuales Elementos recientes	vApps Plantillas de vApp	Medios y otros D	irectivas de alma Puertas de e	nlace Redes de	VDC de Grupos de recursos	•
The VDC_IPLAN-DEMO	Nombre	1 🔺 Estado	Modo de múltiples interfaces	NICS utilized	las Nº de redes externas	Nº de
✓ Miembros	Sedge-IPLAN-DEMO	Accio	nes: Edge-IPLAN-DEMO	3	-2 1	9.2
 Guards Perdidos y encontrados Configuración General Correo electrónico LDAP Directivas 		Servicios de pu Asignaciones d Volver a aplicar Volver a implem Actualizar config Sincronizar la c Eliminar	erta de enlace Edge le IPs externas configuración de servicio nentar guración onfiguración de servidor syslog			
Personalización de invitado		Propiedades				

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

onfigurar servicios: Edge-IPLAN-DEMO											
DHCP NAT Firewall Enrutamiento El protocolo de configuración dinámica de organización. Puede configurar y gestiona conectadas a esta puerta de enlace Edge. Habilitar DHCP	estático VPN Load Bala host (DHCP) automatiza la as rangos de direcciones IP y pa	ncer signación de direcciones IP a m arámetros de concesión para c	iáquinas virtuales conectadas a la ada una de las redes de VDCs de	as redes de VDCs de e organización							
Aplicado/a sobre	Rango de IPs	Concesión pred	Concesión máxima	Habilitado							

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'

DHCP	NAT	Firewall	Enrutamiento e	stático VPN	Load Balancer						
El servicio VPN IPSec le ayuda a crear VPNs seguras entre puertas de enlace. Se pueden configurar VPN de sitio a sitio entre puertas de enlace Edge de esta organización, entre organizaciones e incluso en puertas de enlace VPN de terceros.											
 ✓ Habilitar VPN Configurar IP públicas Las IP públicas se quedes configurar para cada una de las redes externas: esto resulta útil cuando se utiliza NAT en el entorno. 											
Las IP p	mbre	Se puede	n configurar para c	Punto de acceso	s redes externas; esto resulta util cuando se utiliza NAT en el entorno. .o 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 siste	mas del mismo nivel		
Redes locales y de siste	emas del mismo r	nivel				to room.		•	•
Redes locales: InternaConSalida (11 Iplan_Interna (10.10.1	1.11.1.0/24)			•	**	ID del mismo nivel:	D para identificar el mismo nivel de forma exclusiva. Si la dirección del mismo nivel está en esta red VDC de organización e en otra, debe ser la dirección P nativa del mismo nivel. Si el mismo nivel es de NAT, debe ser la dirección IP del mismo nivel privada.	*	
Redes de sistemas d	Redes de sistemas del mismo nivel: Introduzca la dirección de red en formato CIDR, Por ejempio: 192.168.2.0/24, 192.168.3.0/24.					IP del mismo nivel: Protocolo de cifrado:	Dirección IP para conectarse con el mismo nivel. Si el mismo nivel es de NAT, debe ser la dirección del lado público de NAT. AES-256	•	
Configuración de con Extremo local: ID local:	ADHPLAN-78057	192.168.3.0/24. 71-1150 •				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 digito.		
ID del mismo nivel:	1		•			MTU	Mostrar clave *		•
							Aceptar Can	celar	ן

- 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.



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.