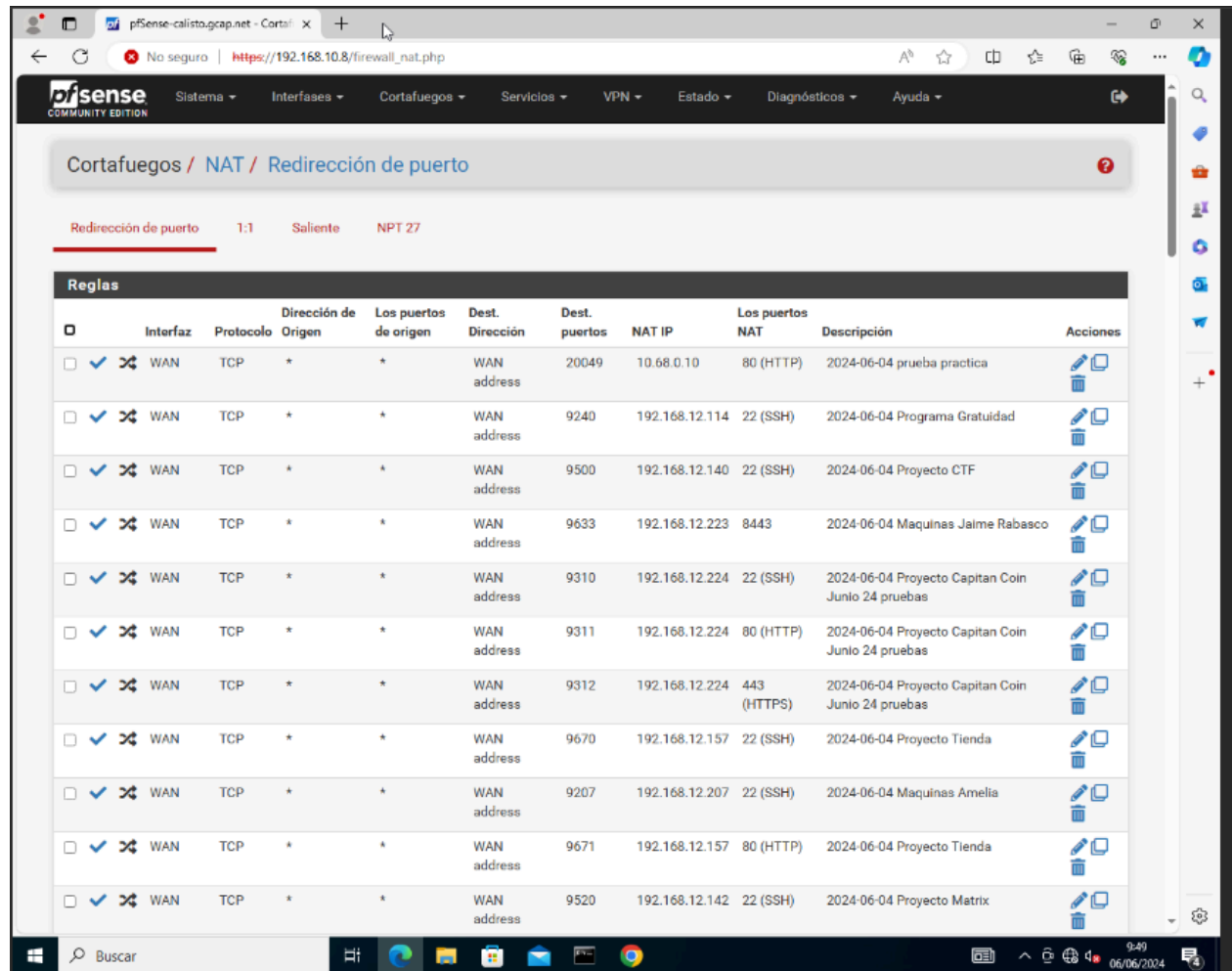
























Migración Proxy y DNAT en Cortafuegos

1. Reglas DNAT	3
2. Proxy	7

1.Reglas DNAT

Para las reglas de DNAT hemos seguido la tabla que creamos la semana pasada en la cual dividimos las máquinas de luna y de calisto con reglas y sin reglas, una vez hecho esto nos dirigimos a la sección de cortafuegos y a NAT:



Reglas	Interfaz	Protocolo	Dirección de Origen	Los puertos de origen	Dest. Dirección	Dest. puertos	NAT IP	Los puertos NAT	Descripción	Acciones
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	20049	10.68.0.10	80 (HTTP)	2024-06-04 prueba practica	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9240	192.168.12.114	22 (SSH)	2024-06-04 Programa Gratuidad	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9500	192.168.12.140	22 (SSH)	2024-06-04 Proyecto CTF	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9633	192.168.12.223	8443	2024-06-04 Maquinas Jaime Rabasco	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9310	192.168.12.224	22 (SSH)	2024-06-04 Proyecto Capitan Coin Junio 24 pruebas	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9311	192.168.12.224	80 (HTTP)	2024-06-04 Proyecto Capitan Coin Junio 24 pruebas	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9312	192.168.12.224	443 (HTTPS)	2024-06-04 Proyecto Capitan Coin Junio 24 pruebas	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9670	192.168.12.157	22 (SSH)	2024-06-04 Proyecto Tienda	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9207	192.168.12.207	22 (SSH)	2024-06-04 Maquinas Amelia	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9671	192.168.12.157	80 (HTTP)	2024-06-04 Proyecto Tienda	 
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	9520	192.168.12.142	22 (SSH)	2024-06-04 Proyecto Matrix	 

Marcos Cáceres García
Pablo Valencia Palomino

Una vez aquí debemos de añadir las reglas según nuestra tabla, para ello debemos de seleccionar en Añadir Regla:

The screenshot shows the pfSense web interface for editing a NAT rule. The breadcrumb trail is "Cortafuegos / NAT / Redirección de puerto / Editar". The page title is "Editar entrada de redirección".

Configuration options include:

- Deshabilitado:** ☐ Desactivar esta regla
- Sin RDR (NO):** ☐ desactivar la redirección de tráfico que coincide con esta regla. Esta opción rara vez es necesaria. No utilice esto sin conocimiento profundo de las implicaciones.
- Interfaz:** WAN (dropdown menu). Elige qué interfaz se aplica esta regla. En la mayoría de los casos "WAN" se especifica.
- Dirección de Familia:** IPv4 (dropdown menu). Seleccione el protocolo de Internet versión se aplica esta regla.
- protocolo:** Cualquiera (dropdown menu). Elija el protocolo que esta regla debe coincidir. En la mayoría de los casos "TCP" se especifica.
- Fuente:**
- Destino:** ☐ Invertir partido. WAN address (dropdown menu). Tipo: Dirección / máscara.
- IP de destino de redirección:** Address or Alias (dropdown menu). Tipo: Dirección. Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4. In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1).
- Descripción:** (text input). Se puede ingresar una descripción aquí para referencia administrativa (no analizada).
- Sin XMLRPC sincronización:** ☐ No sincronizar automáticamente a otros miembros de la carpeta. Esto evita que la regla sobre el Master se sincronice automáticamente a otros miembros del CARP. Esto no impide que la regla de la sobrescritura de esclavo.

Una vez en la pantalla de selección de reglas debemos de seleccionar la interfaz a la interfaz que va a afectar, en este caso a la WAN (192.168.12.X/24), una vez hecho esto debemos de seleccionar el rango de puertos de origen, como en las reglas los puertos son exactos, es decir, no son un rango, debemos de poner el mismo puerto en los dos apartados, una vez hecho esto debemos de escribir la IP de la máquina de a red interna VM, en nuestro caso hemos clonado la máquina de pruebas de windows y le hemos instalado IIS y la hemos añadido a la red de VM con la IP 10.68.0.10, una vez hecho esto, debemos de seleccionar el puerto de destino, que normalmente suele ser el puerto 80 o 22:

Editar entrada de redirección

Deshabilitado ☐ Desactivar esta regla

Sin RDR (NO) ☐ desactivar la redirección de tráfico que coincide con esta regla
Esta opción rara vez es necesaria. No utilice esto sin conocimiento profundo de las implicaciones.

Interfaz: WAN
Elige qué interfaz se aplica esta regla. En la mayoría de los casos "WAN" se especifica.

Dirección de Familia: IPv4
Seleccione el protocolo de Internet versión se aplica esta regla.

protocolo: TCP
Elija el protocolo que esta regla debe coincidir. En la mayoría de los casos "TCP" se especifica.

Fuente [mostrar avanzada](#)

Destino ☐ Invertir partido. WAN address
Tipo Dirección / máscara

El rango de puerto de destino Otras instrucciones 20049 Otras instrucciones 20049
Desde el puerto Personalizado Hacia el puerto Personalizado
Especificar el puerto o rango de puertos para el destino del paquete para esta correspondencia. El campo "a" se puede dejar vacío si solamente la asignación de un solo puerto.

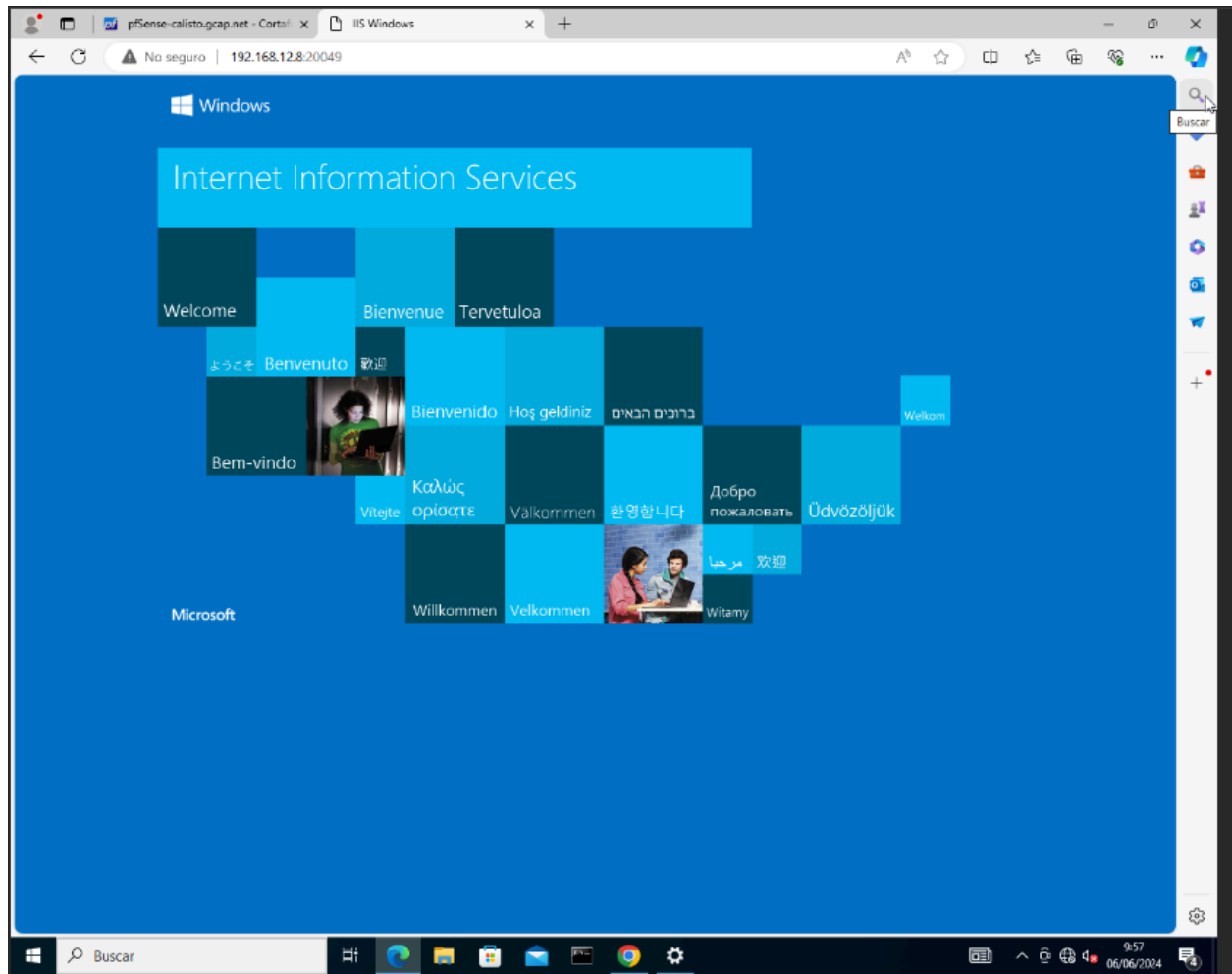
IP de destino de redirección Address or Alias 10.68.0.10
Tipo Dirección
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)

Puerto de destino de redirección HTTP
Puerto Personalizado
Especifique el puerto en el equipo con la dirección IP introducida anteriormente. En caso de un rango de puertos, especifique el puerto de inicio del rango (el puerto final será calculado automáticamente).
Este es comúnmente idéntico al valor en "Desde el puerto" introducido más arriba.

Descripción 2024-06-04 prueba practica

Marcos Cáceres García
Pablo Valencia Palomino

Para comprobar que funciona, debemos de poner la IP de la interfaz WAN del cortafuegos seguido del puerto que hayamos escrito en la regla (20049) y si la regla funciona bien deberíamos ver la página IIS de la máquina windows en la red de VM, ahora debemos repetir el proceso con todas las reglas de la tabla de reglas:



2.Proxy

Para la configuración Proxy, hemos elegido la herramienta HAProxy, ya que ofrece la mejor estabilidad y eficiencia en el procesamiento de tráfico para pfSense, además de protegerlo contra ataques DDoS, entre otros.

La configuración del proxy consta de 2 bloques: backend y frontend. Se ha creado un backend por cada sitio configurado en nginx en la antigua arquitectura del sistema, y un frontend para todos los backend, con las ACLs correspondientes para cada sitio.























































Los sitios creados son:

- archivo.iesgrancapitan.org
- backyincanas.iesgrancapitan.org
- ctf.iesgrancapitan.org
- confirmacpd.iesgrancapitan.org
- documental.iesgrancapitan.org
- erasmusplus.iesgrancapitan.org
- fabidis.iesgrancapitan.org
- fct.iesgrancapitan.org
- frontyincanas.iesgrancapitan.org
- gratuidads.iesgrancapitan.org
- hi.iesgrancapitan.org
- intranets.iesgrancapitan.org
- intranet2223.iesgrancapitan.org
- inventario.iesgrancapitan.org
- itop.iesgrancapitan.org
- kioskos.iesgrancapitan.org
- openprojects.iesgrancapitan.org
- moodle-old.iesgrancapitan.org
- pedidos.iesgrancapitan.org
- shikoba.iesgrancapitan.org
- proyectos.iesgrancapitan.org
- sysmanas.iesgrancapitan.org
- tvs.iesgrancapitan.org
- www-old.iesgrancapitan.org
- matrix.iesgrancapitan.org
- nagios.iesgrancapitan.org

Services / HAProxy / Backend

Settings Frontend Backend Files Stats Stats FS Templates





Backends

Advanced	Name	Servers	Check	Frontend	Actions
<input type="checkbox"/>	backend_archivo	1	HTTP	frontal	  
<input type="checkbox"/>	backend_baciyincanas	1	HTTP	frontal	  
<input type="checkbox"/>	backend_ctf	1	HTTP	frontal	  
<input type="checkbox"/>	backend_confirmacpd	1	HTTP	frontal	  
<input type="checkbox"/>	backend_documental	1	HTTP	frontal	  
<input type="checkbox"/>	backend_pruebais	1	HTTP	frontal	  
<input type="checkbox"/>	backend_erasmusplus	1	HTTP	frontal	  
<input type="checkbox"/>	backend_fabidis	1	HTTP	frontal	  
<input type="checkbox"/>	backend_fct	1	HTTP	frontal	  
<input type="checkbox"/>	backend_frontyincanas	1	HTTP	frontal	  
<input type="checkbox"/>	backend_gratuidads	1	HTTP	frontal	  
<input type="checkbox"/>	backend_hi	1	HTTP	frontal	  
<input type="checkbox"/>	backend_intranets	1	HTTP	frontal	  
<input type="checkbox"/>	backend_intranet2223	1	HTTP	frontal	  
<input type="checkbox"/>	backend_inventario	1	HTTP	frontal	  
<input type="checkbox"/>	backend_itop	1	HTTP	frontal	  
<input type="checkbox"/>	backend_kioskos	1	HTTP	frontal	  
<input type="checkbox"/>	backend_openproject	1	HTTP	frontal	  

Services / HAProxy / Frontend

Settings Frontend Backend Files Stats Stats FS Templates

Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		frontal		192.168.12.8:80	http	backend_archivo if(acl_archivo) backend_baciyincanas if(acl_baciyincanas) backend_pruebais if(acl_pruebais) backend_ctf if(acl_ctf) backend_confirmacpd if(acl_confirmacpd) backend_documental if(acl_documental) backend_erasmusplus if(acl_erasmusplus) backend_fabidis if(acl_fabidis) backend_fct if(acl_fct) backend_frontyincanas if(acl_frontyincanas) backend_gratuidads if(acl_gratuidads) backend_hi if(acl_hi) backend_intranet2223 if(acl_intranet2223) backend_intranets if(acl_intranets) backend_inventario if(acl_inventario) backend_itop if(acl_itop) backend_kioskos if(acl_kioskos) backend_mapass if(acl_mapass) backend_matrix if(acl_matrix) backend_moodle-old if(acl_moodle-old) backend_nagios if(acl_nagios) backend_openproject if(acl_openproject) backend_pedidos if(acl_pedidos) backend_proyectos if(acl_proyectos) backend_shikoba if(acl_shikoba) backend_sysmanas if(acl_sysmanas) backend_tvs if(acl_tvs) backend_www-old if(acl_www-old)	  

Agregar
Borrar
Guardar