



JUPITER LABS

Informe Ejecutivo de Infraestructura de Red

Keepcoding

Profesor: Sergio Vilches

Realizado por: Mónica Durán Alfonso

Email: monicadual1915@gmail.com

Linkedin: Mónica Durán

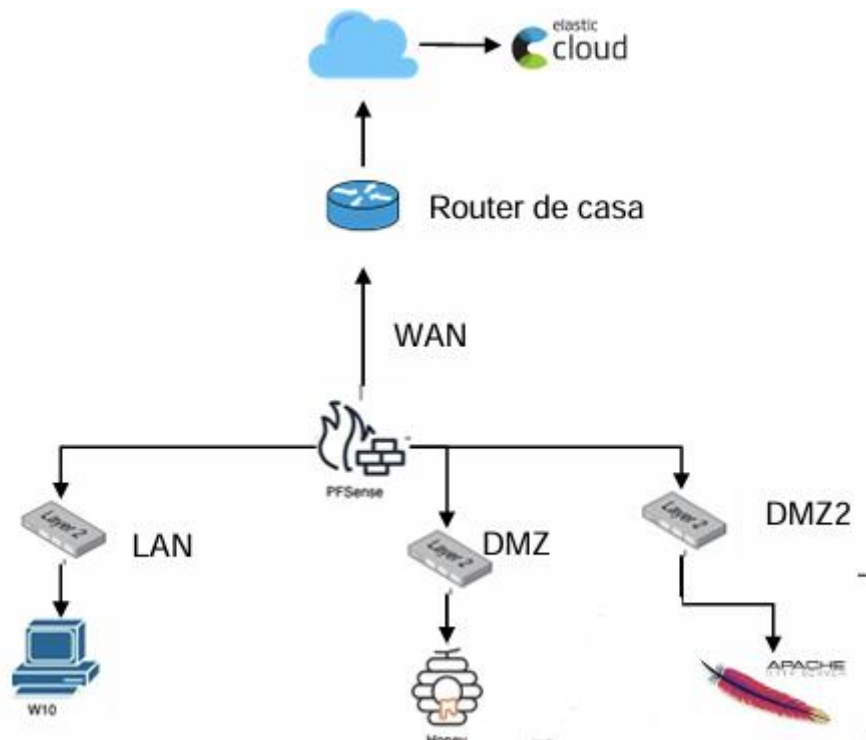
Octubre 2024

Índice

1. Introducción.
2. Descripción de la Estructura de Red.
 1. Configuración de pfSense
 2. Redes LAN, DMZ y DMZ2
3. Reglas de pfSense.
 1. Reglas para la Red LAN
 2. Reglas para la Red DMZ
 3. Reglas para la Red DMZ2
 4. Reglas de NAT y WAN
 - 5.
4. Detalles de Implementación.
 1. Red LAN
 2. Red DMZ
 3. Red DMZ2
5. Configuración del Servidor Elastic.
6. Integraciones de Elastic Cloud.
7. Conclusión

1. Introducción

Este informe detalla la configuración de una estructura de red utilizando pfSense para interconectar las redes LAN, DMZ y DMZ2. Se describen los componentes y la configuración necesaria para asegurar la correcta recolección y visualización de logs en un servidor Elastic.



2. Descripción de la Estructura de Red

2.1 Configuración de pfSense

pfSense se utilizará como firewall y router para gestionar el tráfico entre las redes LAN, DMZ y DMZ2. La configuración incluye reglas de firewall específicas para asegurar la segmentación y seguridad de cada red.

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.134/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.200.1/24
DMZ2 (opt2)    -> em3      -> v4: 192.168.250.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

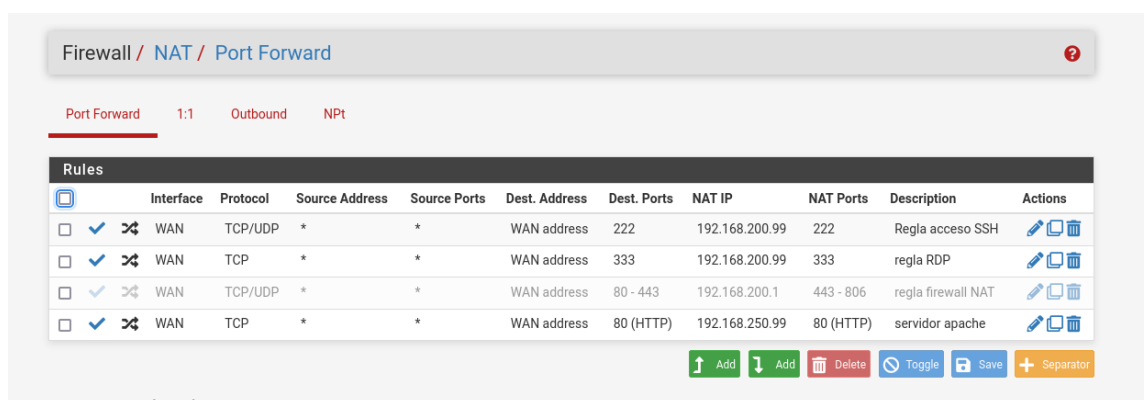
Enter an option:
Message from syslogd@UTM at Oct 12 19:33:03 ...
php-fpm[399]: /firewall_nat.php: Successful login for user 'admin' from: 192.168.200.99 (Local Database)

Message from syslogd@UTM at Oct 12 21:23:00 ...
php-fpm[41297]: /services_dhcp.php: Successful login for user 'admin' from: 192.168.200.99 (Local Database)
```

3. Reglas de pfSense

3.1 Reglas de NAT

- NAT saliente automático: Configurar pfSense para que utilice NAT saliente automático, lo que traducirá el tráfico saliente de las redes internas (LAN, DMZ, DMZ2) a la dirección IP de la interfaz WAN.
- NAT entrante para el Honeypot: Crear reglas de NAT entrante para redirigir el tráfico de la WAN al honeypot en la DMZ.



3.2 Reglas para la Red WAN

- **Permitir tráfico entrante específico:** Configurar reglas para permitir el tráfico entrante específico necesario, como el acceso al honeypot desde la WAN.
- **Bloquear tráfico no autorizado:** Asegurar que todo el tráfico no autorizado desde la WAN sea bloqueado para proteger las redes internas.

COMMUNITY EDITION

Firewall / Rules / WAN ⌵ ⌵ ?

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress.

Floating **WAN** LAN DMZ DMZ2 OpenVPN

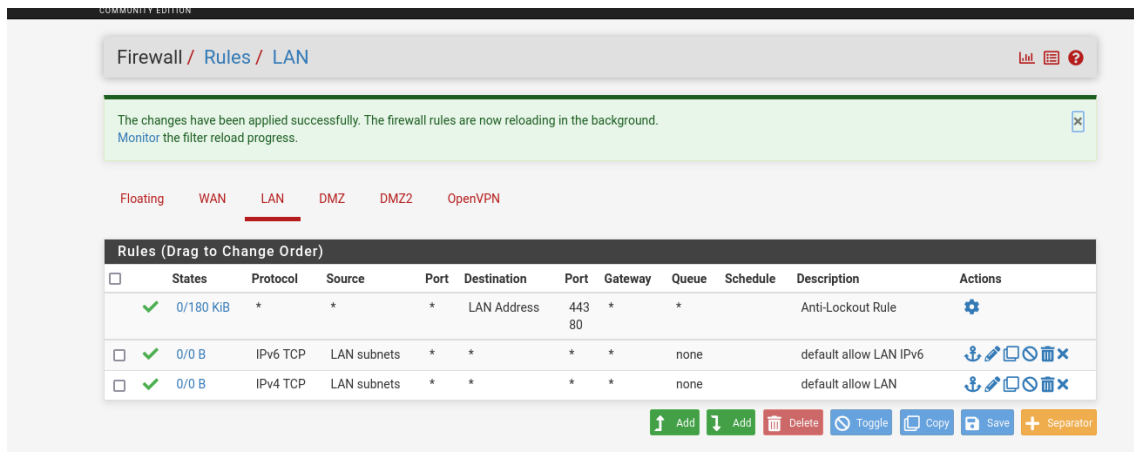
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/480 B	IPv4 ICMP any	*	*	*	*	*	none			⌵ ✎ ⌵ ⌵ ✖
<input type="checkbox"/>	✓ 0/260 B	IPv4 TCP	*	*	192.168.200.1	222	*	none		Regla acceso SSH	⌵ ✎ ⌵ ⌵ ✖
<input type="checkbox"/>	✓ 0/24 KiB	IPv4 TCP	*	*	192.168.250.99	80 (HTTP)	*	none		NAT servidor apache	⌵ ✎ ⌵ ⌵ ✖
<input type="checkbox"/>	✓ 0/121 KiB	IPv4 TCP	*	*	192.168.200.99	333	*	none		NAT regla RDP	⌵ ✎ ⌵ ⌵
<input type="checkbox"/>	✓ 0/38 KiB	IPv4 TCP/UDP	*	*	192.168.200.99	222	*	none		NAT Regla acceso SSH	⌵ ✎ ⌵ ⌵

[⬆ Add](#) [⬇ Add](#) [🗑 Delete](#) [🔄 Toggle](#) [📄 Copy](#) [💾 Save](#) [+ Separator](#)

[i](#)

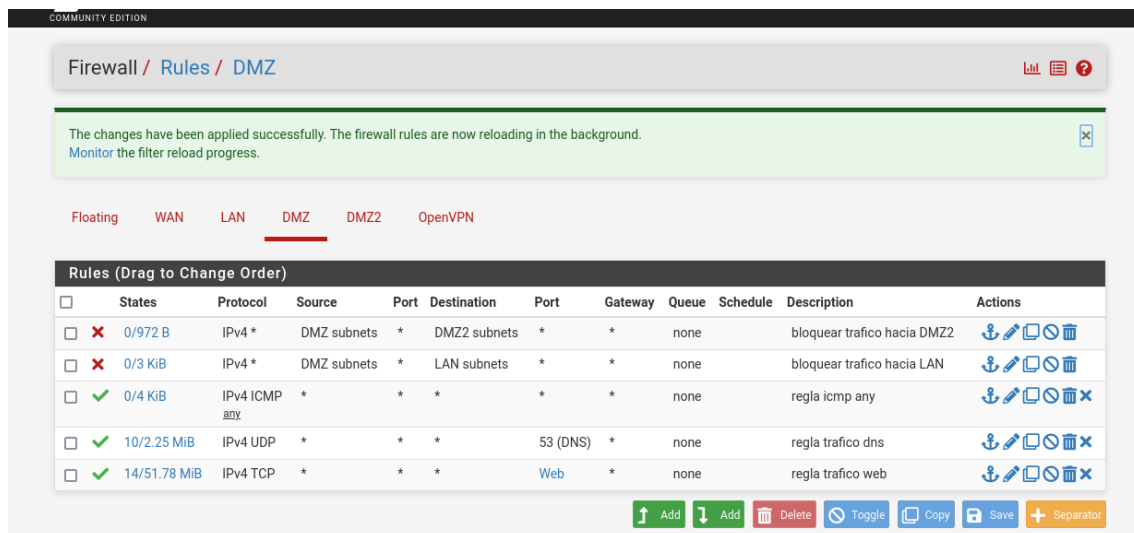
3.3 Reglas para la Red LAN

- **Permitir tráfico saliente:** Permitir que los dispositivos en la LAN puedan acceder a Internet.
- **Bloquear tráfico entrante no solicitado:** Asegurar que solo el tráfico iniciado desde la LAN pueda recibir respuestas.



3.4 Reglas para la Red DMZ

- **Permitir acceso desde WAN al Honeypot:** Configurar reglas para que el honeypot en la DMZ sea accesible desde la red WAN en ambos sentidos.
- **Bloquear acceso a redes internas:** Asegurar que el honeypot no tenga acceso a la LAN ni a la DMZ2.



3.5 Reglas para la Red DMZ2

- **Permitir tráfico saliente hacia el servidor Elastic:** Configurar reglas para que la fuente de logs en DMZ2 pueda enviar datos al servidor Elastic.
- **Bloquear tráfico entrante no solicitado:** Asegurar que solo el tráfico iniciado desde DMZ2 pueda recibir respuestas.

COMMUNITY EDITION

Firewall / Rules / DMZ2 🔍 📄 ?

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#) ✕

Floating WAN LAN DMZ **DMZ2** OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/1 KiB	IPv4 ICMP any	*	*	*	*	*	none		regla icmp	🔗 ✎ 📄 🗑️ ✖
<input type="checkbox"/>	✓ 0/1.77 MiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		regla trafico dns	🔗 ✎ 📄 🗑️ ✖
<input type="checkbox"/>	✓ 0/62.01 MiB	IPv4 TCP	*	*	*	Web	*	none		regla trafico web	🔗 ✎ 📄 🗑️ ✖

[↑ Add](#) [↓ Add](#) [🗑️ Delete](#) [🔄 Toggle](#) [📄 Copy](#) [💾 Save](#) [+ Separator](#)

[?](#)

3.6 Reglas Generales

- **Permitir tráfico entre redes específicas:** Configurar reglas específicas para permitir el tráfico necesario entre las redes LAN, DMZ y DMZ2 según los requisitos del proyecto.
- **Registrar y monitorear tráfico:** Configurar reglas para registrar y monitorear el tráfico relevante para análisis y auditoría.

COMMUNITY EDITION

Firewall / Aliases / All 🔍 ?

IP Ports URLs **All**

Firewall Aliases All

Name	Type	Values	Description	Actions
ElasticCloud	Host(s)	34.107.161.234	Alias para Elastic Cloud	✎ 📄 🗑️
Web	Port(s)	80, 443	puerto para trafico web	✎ 📄 🗑️

[+ Add](#) [📄 Import](#)

[?](#)

[📄 Save](#)

DHCP Static Mappings

Static ARP	MAC address	IP address	Hostname	Description	Actions
✓	08:00:27:89:6d:88	192.168.200.99	hoenypot		✎ 🗑️



[+ Add Static Mapping](#)

Network Booting
Display Advanced

Custom DHCP Options
Display Advanced

Save

DHCP Static Mappings

Static ARP	MAC address	IP address	Hostname	Description	
✓	08:00:27:89:6d:88	192.168.250.99	kali	servidor apache	 

+ Add Static Mapping

4. Detalles de Implementación

4.1 Red LAN

- **Equipo Windows 11:** Este equipo enviará logs al servidor Elastic.

4.2 Red DMZ

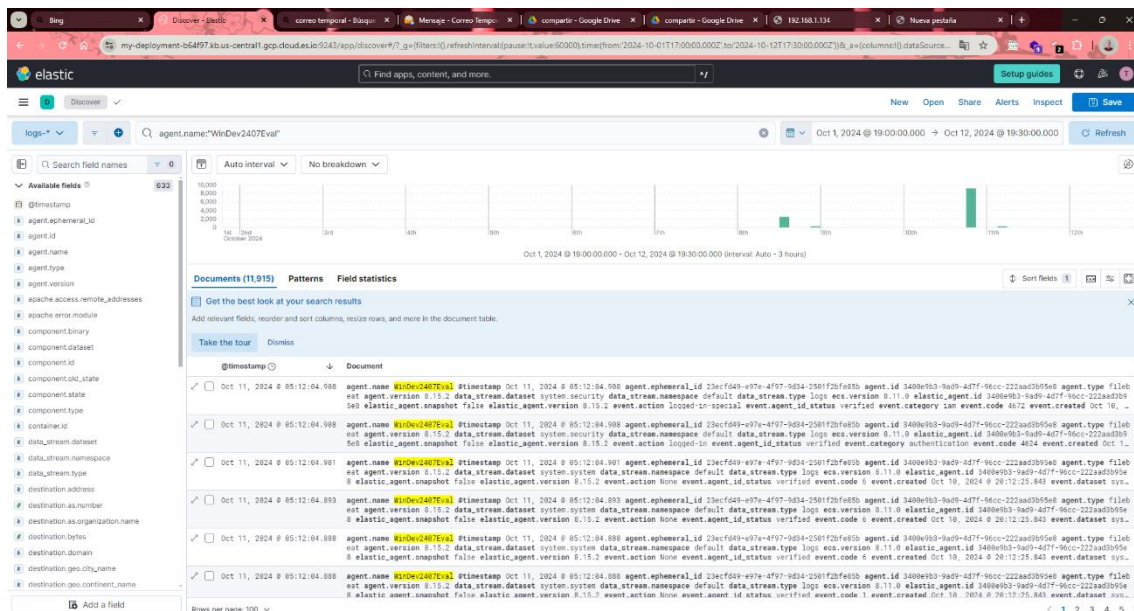
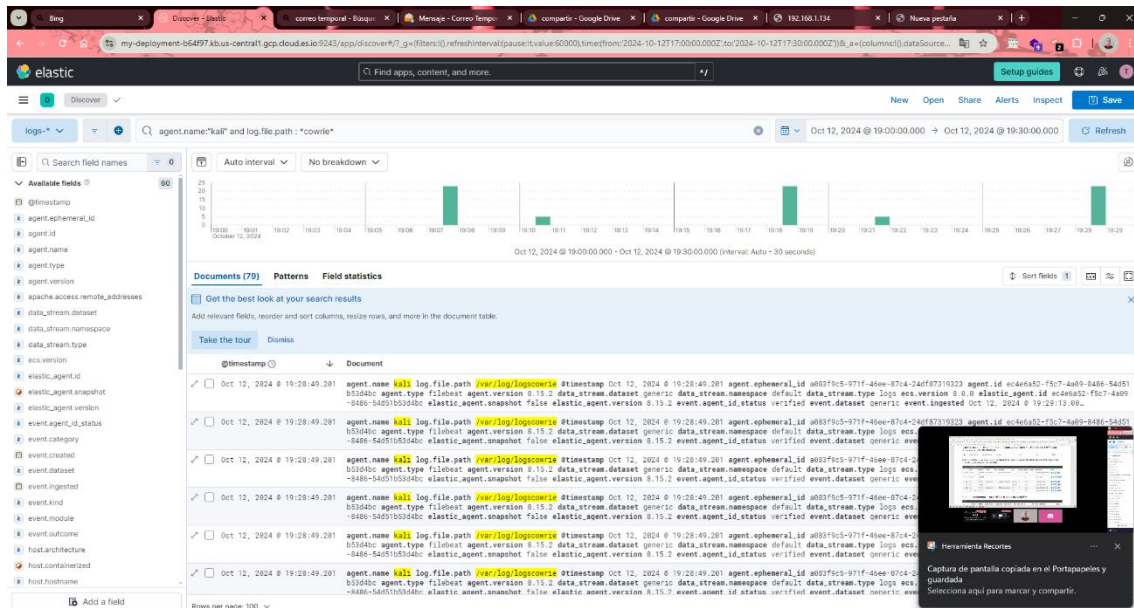
- **Honeypot:** Se implementará un honeypot que enviará logs al servidor Elastic. Este honeypot no tendrá acceso a ninguna red interna (LAN, DMZ2) y será accesible desde la red WAN en ambos sentidos.

4.3 Red DMZ2

- **Fuente de Logs:** Se elegirá una fuente de logs diferente a las mencionadas anteriormente, como Suricata o Apache Server. Esta fuente también enviará logs al servidor Elastic.

5. Configuración del Servidor Elastic

El servidor Elastic recibirá, almacenará y permitirá la visualización de los logs provenientes del equipo Windows 11, el honeypot y la fuente de logs en DMZ2. Se configurarán los pipelines de ingestión y los dashboards necesarios para el monitoreo.



Fleet

Centralized management for Elastic Agents.

[Agents](#)[Agent policies](#)[Enrollment tokens](#)[Uninstall tokens](#)[Data streams](#)[Settings](#)

Ingest Overview Metrics

Agent info Metrics

Agent activity

Add Fleet Server

Add agent

Filter your data using KQL syntax

Status 4Tags 0Agent policy 3Upgrade available

Showing 3 agents

Clear filters

Healthy 3Unhealthy 0Updating 0Offline 0Inactive 0Unenrolled 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	WinDev2407Eval	Politica Windows rev. 1	1.40 %	160 MB	14 seconds ago	8.15.2	...
Healthy	kali	MiPrimeraPolitica rev. 3	1.09 %	212 MB	16 seconds ago	8.15.2	...
Healthy	debc5549aa93	Elastic Cloud agent policy rev. 5	N/A	N/A	31 seconds ago	8.15.2	...

Rows per page: 20

< 1 >

MiPrimeraPolitica · Agent policies

my-deployment-b64f97.kb.us-central1.gcp.cloud.es.io:9243/app/fleet/policies/874e07e9-8cfa-4c92-a4c5-1a059c14340

elastic

Find apps, content, and more.

Setup guides

Send feedback

View all agent policies

Revision 4Integrations 4Agents 1 agentLast updated on Oct 12, 2024Actions

IntegrationsSettings

Search...

NamespaceAdd Integration

Name	Integration	Namespace	Actions
apache-1	Apache HTTP Server v1.25.0	default	...
log-1	Custom Logs v2.3.2	default	...
suricata-1	Suricata v2.21.3	default	...
system-1	System v1.61.0	default	...

System · Integrations · Elastic

my-deployment-b64f97.kb.us-central1.gcp.cloud.es.io:9243/app/integrations/detail/system-1.61.0/policies

elastic

Find apps, content, and more.

Setup guides

Connection details

Back to integrations

System

Elastic Agent

Version 1.61.0Agent policies 2Add System

OverviewIntegration policiesAssetsSettingsConfigsAPI reference

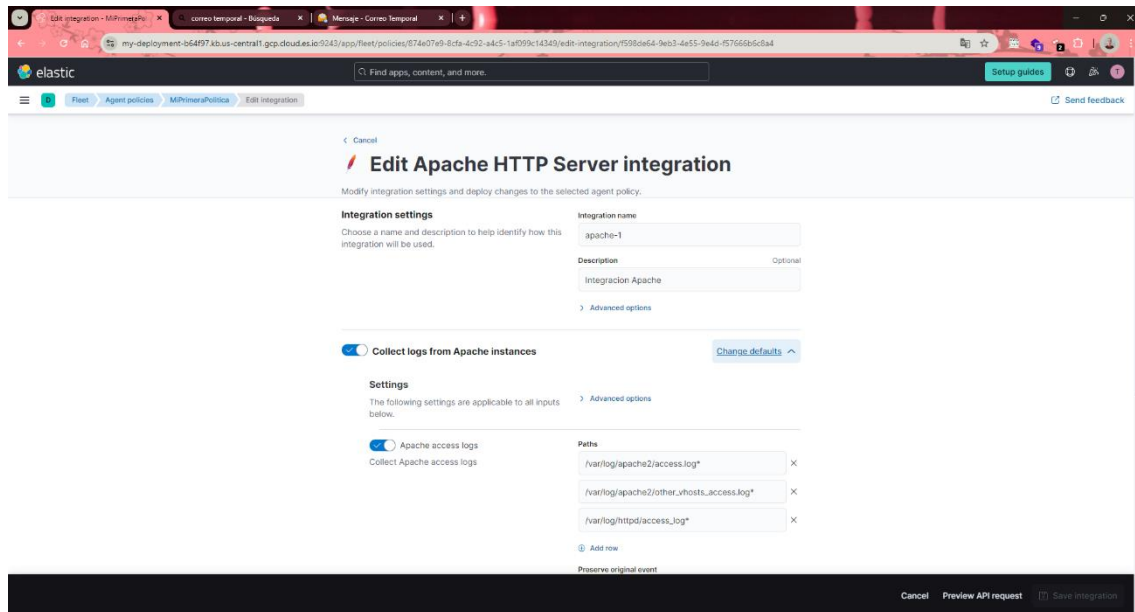
Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
system-2	v1.61.0	Politica Windows rev. 2	2221680266	4 days ago	1	...
system-1	v1.61.0	MiPrimeraPolitica rev. 4	2221680266	last week	1	...

Rows per page: 20

< 1 >

1. Apache:

- **Descripción:** Hemos integrado los logs de Apache en Elastic Cloud para un análisis detallado del tráfico web y la detección de posibles amenazas.
- **Beneficios:** Esta integración nos permite identificar patrones de acceso inusuales, realizar auditorías de seguridad y optimizar el rendimiento del servidor web.



2. Honeypot Cowrie:

- **Descripción:** Cowrie es un honeypot que simula un entorno de servidor SSH y Telnet para atraer y registrar actividades maliciosas.
- **Beneficios:** La integración de Cowrie en Elastic Cloud nos proporciona visibilidad sobre los intentos de intrusión y las tácticas utilizadas por los atacantes, permitiéndonos mejorar nuestras defensas.

Edit Custom Logs integration

Modify integration settings and deploy changes to the selected agent policy.

Integration settings
Choose a name and description to help identify how this integration will be used.

Integration name: log-1

Description: HoneyPot Cowrie

Custom log file

Log file path: /var/log/logscowrie

Dataset name: generic

Buttons: Cancel, Preview API request, Save integration

3. Windows:

- **Descripción:** Los eventos de seguridad y logs del sistema operativo Windows se envían a Elastic Cloud para su análisis y correlación.
- **Beneficios:** Esta integración facilita la detección de comportamientos anómalos, la identificación de posibles vulnerabilidades y la respuesta rápida a incidentes de seguridad.

Edit Windows integration

Choose a name and description to help identify how this integration will be used.

Integration name: system-2

Collect logs from System instances

System auth logs (log)
Collect System auth logs using log input

Paths: /var/log/auth.log*, /var/log/secure*

System syslog logs (log)
Collect System syslog logs using log input

Paths: /var/log/messages*, /var/log/syslog*

Buttons: Cancel, Preview API request, Save integration

7. Conclusión

La configuración descrita asegura una estructura de red segura y eficiente, con una correcta recolección y visualización de logs en el servidor Elastic. Esto permitirá un monitoreo continuo y una respuesta rápida ante posibles incidentes de seguridad.

Para concluir, se adjunta una imagen que muestra la comprobación realizada mediante pings a las redes. En esta imagen se puede observar que no hay tráfico en ninguna de las redes internas (LAN y DMZ2) y, al mismo tiempo, se confirma que es accesible desde el exterior.


```
1 2 3 4 5 6
/home/kali
Archivo Acciones Editar Vista Ayuda

(kali@kali)-[~]
$ ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
^C
— 192.168.100.1 ping statistics —
18 packets transmitted, 0 received, 100% packet loss, time 17396ms

(kali@kali)-[~]
$ ping 192.168.250.1
PING 192.168.250.1 (192.168.250.1) 56(84) bytes of data.
^C
— 192.168.250.1 ping statistics —
6 packets transmitted, 0 received, 100% packet loss, time 5108ms

(kali@kali)-[~]
$ ping 192.168.200.1
PING 192.168.200.1 (192.168.200.1) 56(84) bytes of data.
64 bytes from 192.168.200.1: icmp_seq=1 ttl=64 time=0.456 ms
64 bytes from 192.168.200.1: icmp_seq=2 ttl=64 time=0.649 ms
64 bytes from 192.168.200.1: icmp_seq=3 ttl=64 time=0.619 ms
^C
— 192.168.200.1 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.456/0.574/0.649/0.084 ms

(kali@kali)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=3.89 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=30.4 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=30.0 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=63 time=3.85 ms
^C
— 192.168.1.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 3.848/17.042/30.417/13.172 ms

(kali@kali)-[~]
$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=6.30 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=56 time=6.21 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=56 time=6.42 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=56 time=7.46 ms
^C
— 1.1.1.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3019ms
rtt min/avg/max/mdev = 6.211/6.598/7.463/0.504 ms

(kali@kali)-[~]
$
```

