Memoria Ciberseguridad

Evaluación BlueTeam

Nombre del Auditor: Kacper Mariusz Koper Mielczarek

Fecha: 19/01/2025

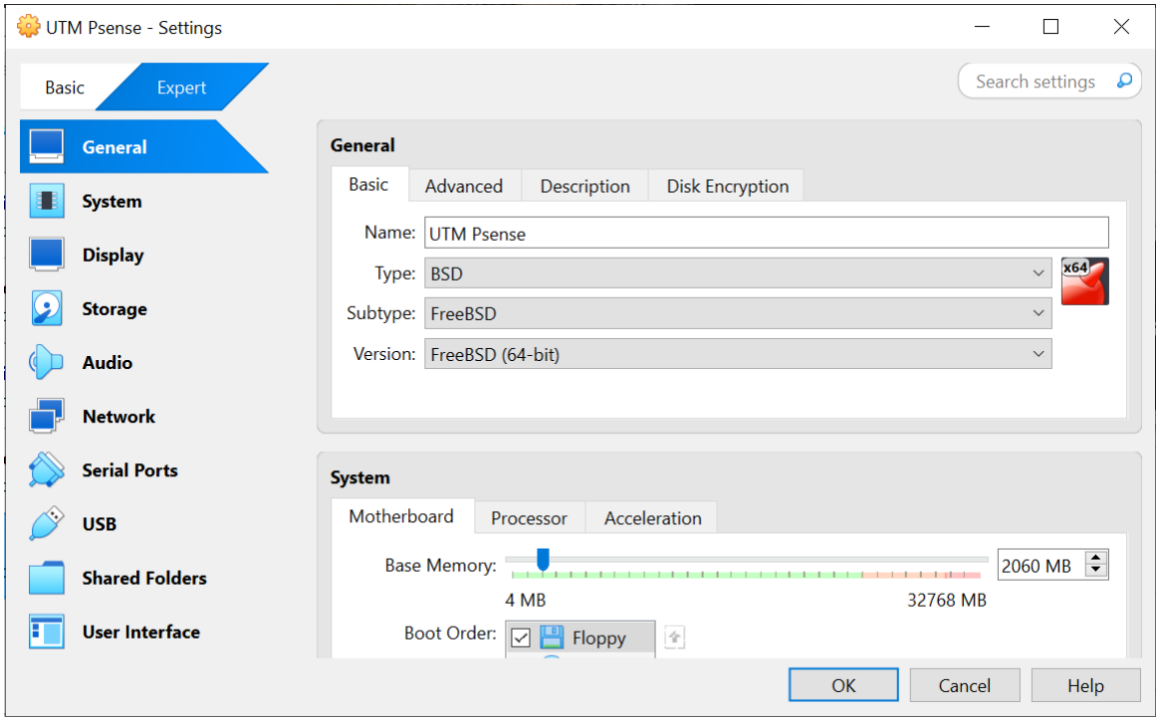
Índice

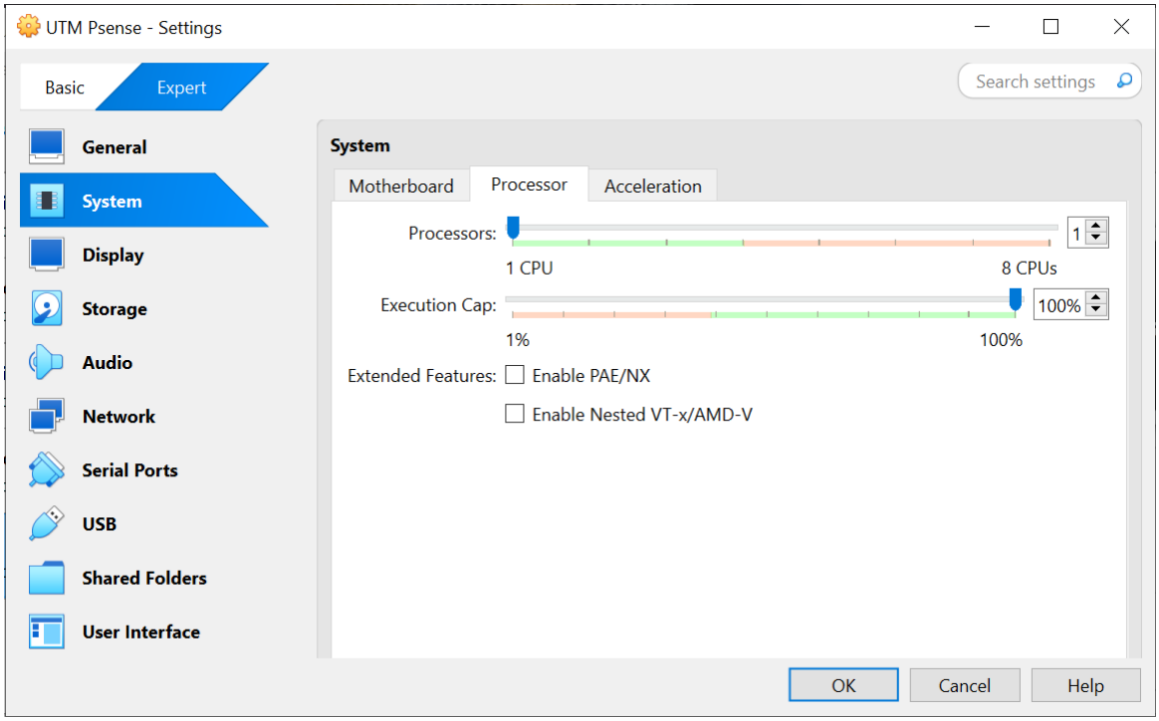
1. Instalar y Configurar Pfsense

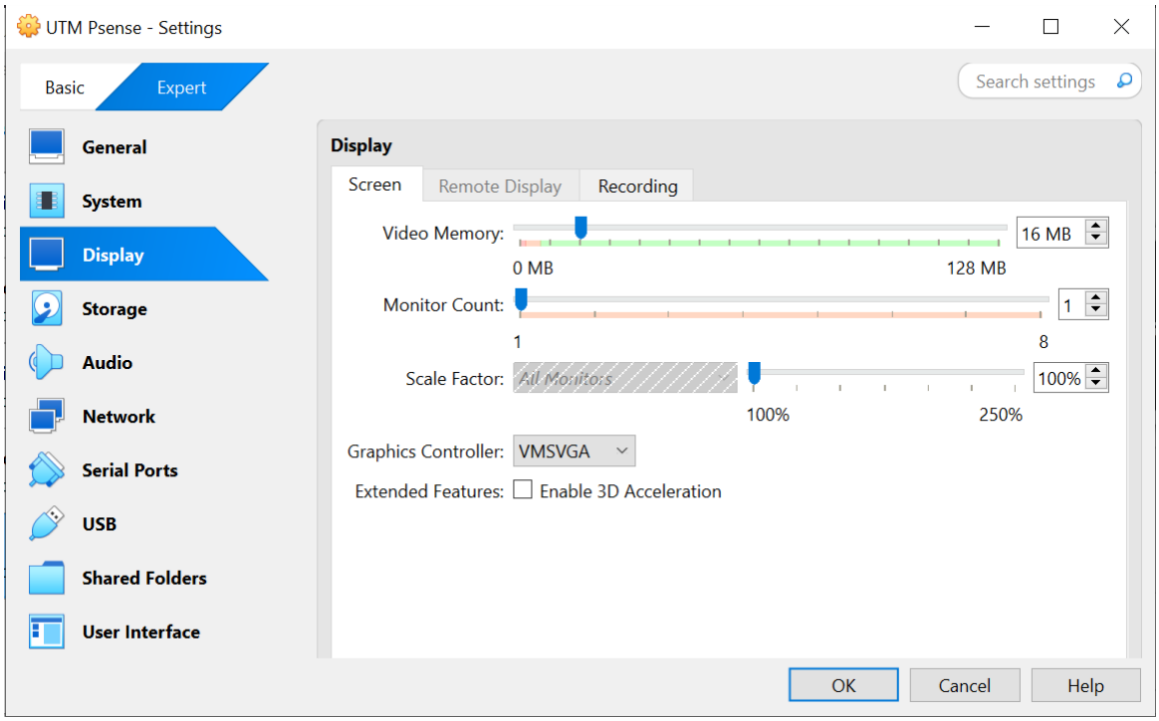
1.1. Instalación

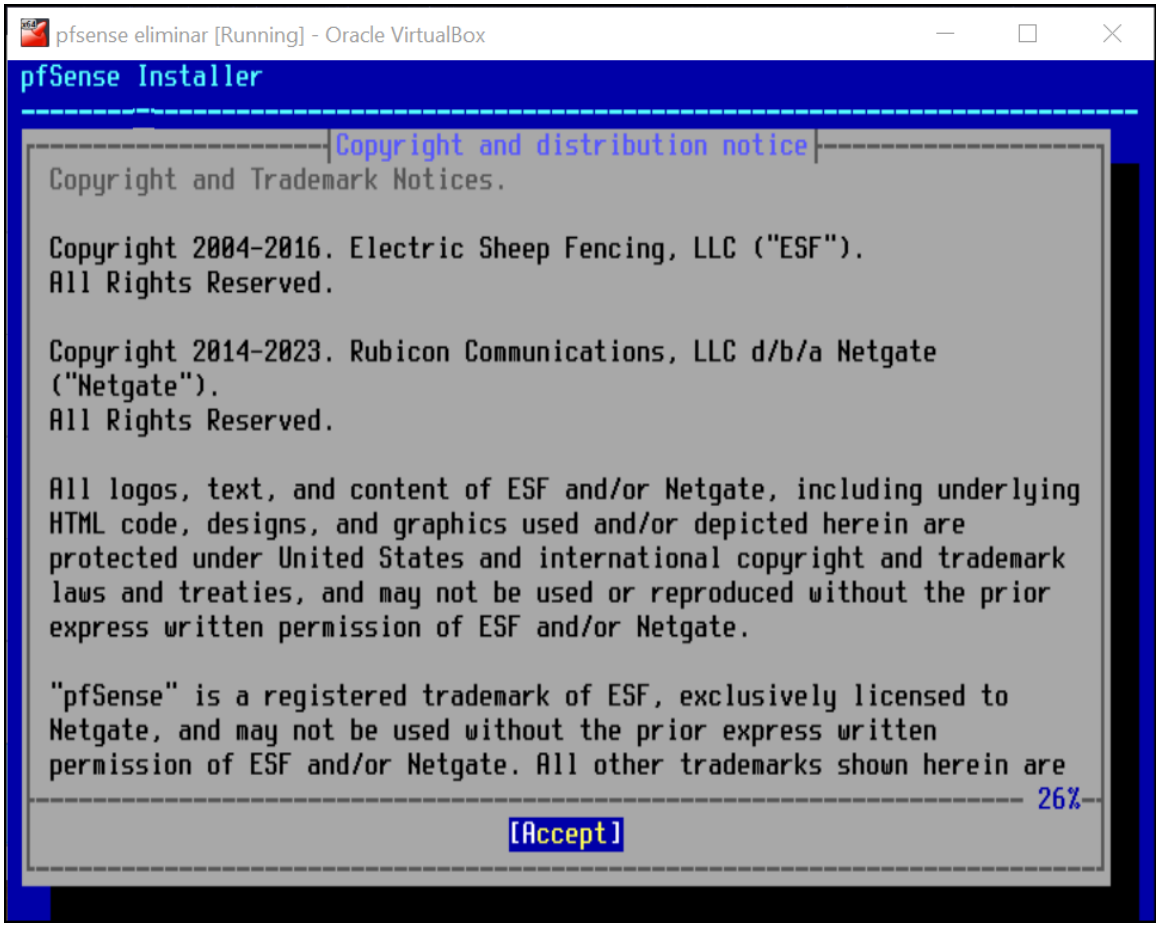
En esta primera etapa de la práctica, se realizó la instalación y configuración inicial de **Pfsense**, un sistema UTM (Unified Threat Management) utilizado para gestionar y controlar el tráfico de red de los equipos conectados. Inicialmente, se procedió con la instalación del sistema y la configuración básica, asignando las interfaces correspondientes para las redes internas (**LAN**) y externas (**WAN**). Este proceso permitió establecer los parámetros iniciales para obtener conexión en red.

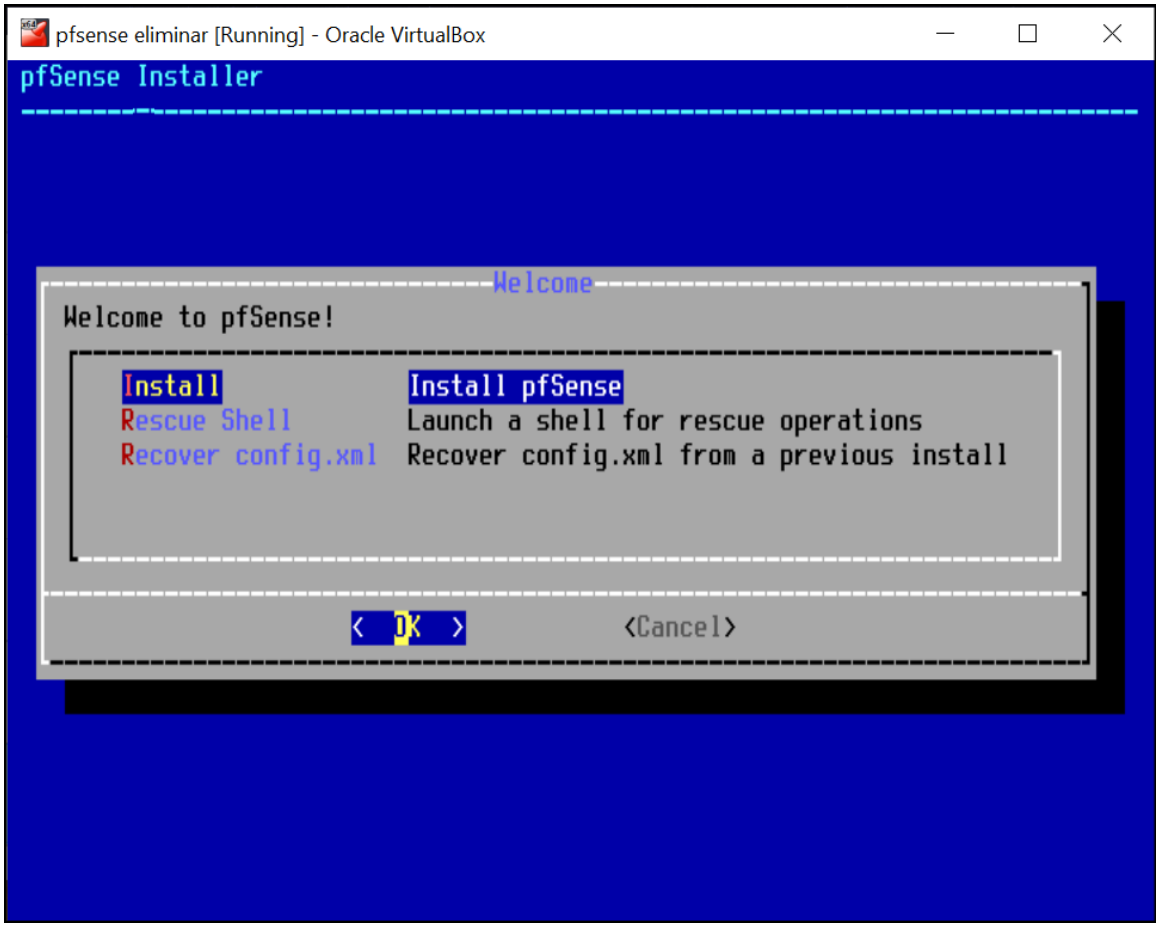
Finalmente, se verificó el correcto funcionamiento de la máquina, comprobando que las interfaces asignadas operan según lo esperado. Se obtuvo con éxito el dato de las direcciones asignadas a la **WAN** y la **LAN**, confirmando que el sistema está preparado para proceder a gestionar las diferentes reglas del Pfsense.

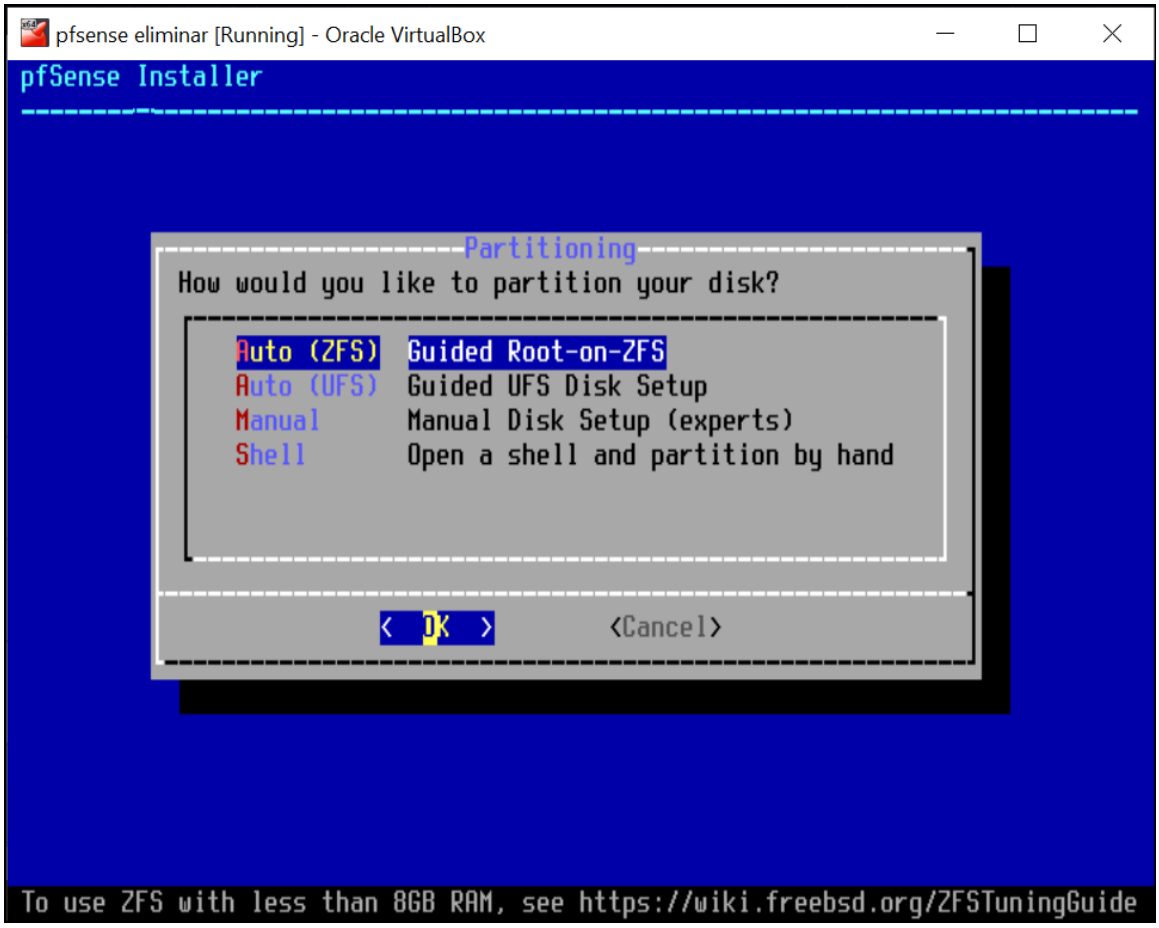


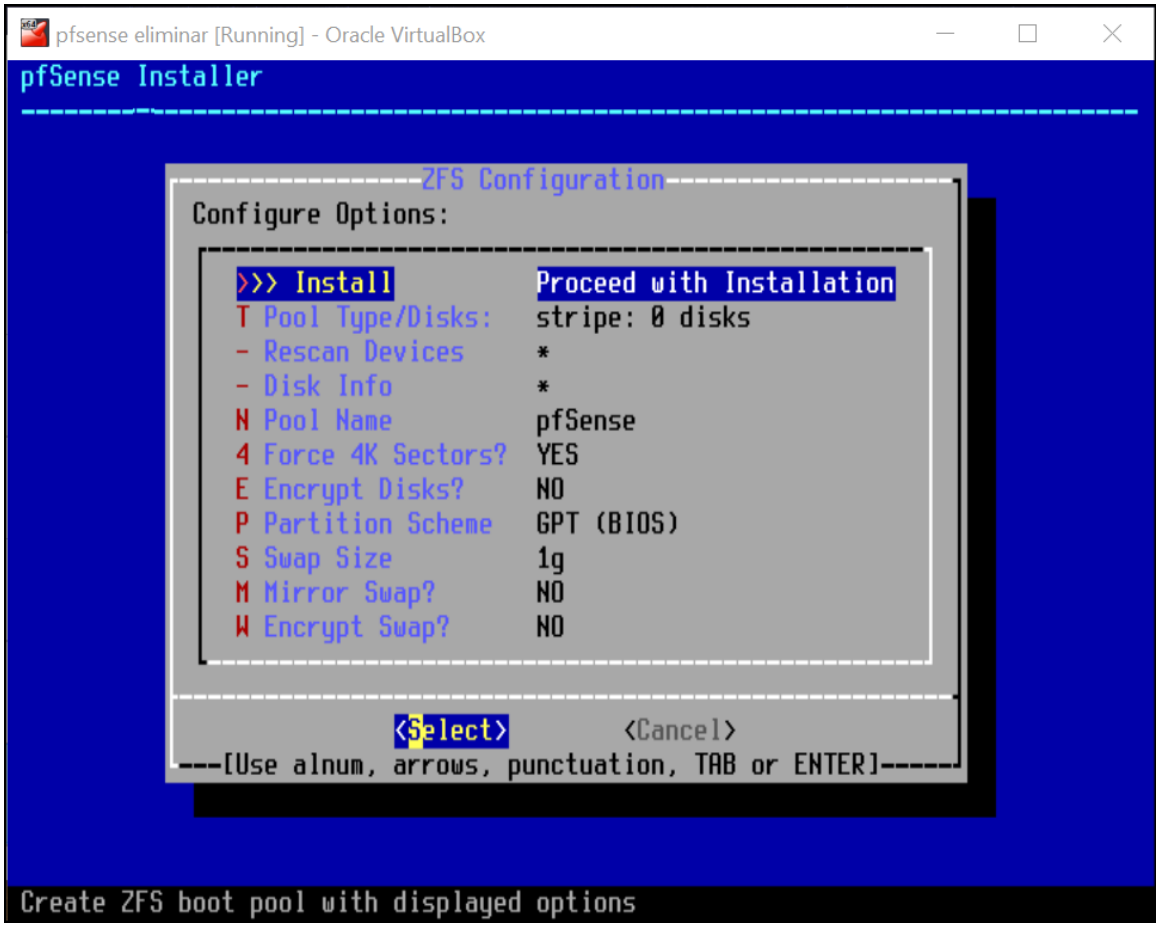

UTM Psense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Processors:
1
1 CPU
8 CPUs
Execution Cap:
100%
1%
100%
Extended Features:
Enable PAE/NX
Enable Nested VT-x/AMD-V
OK
Cancel
Help

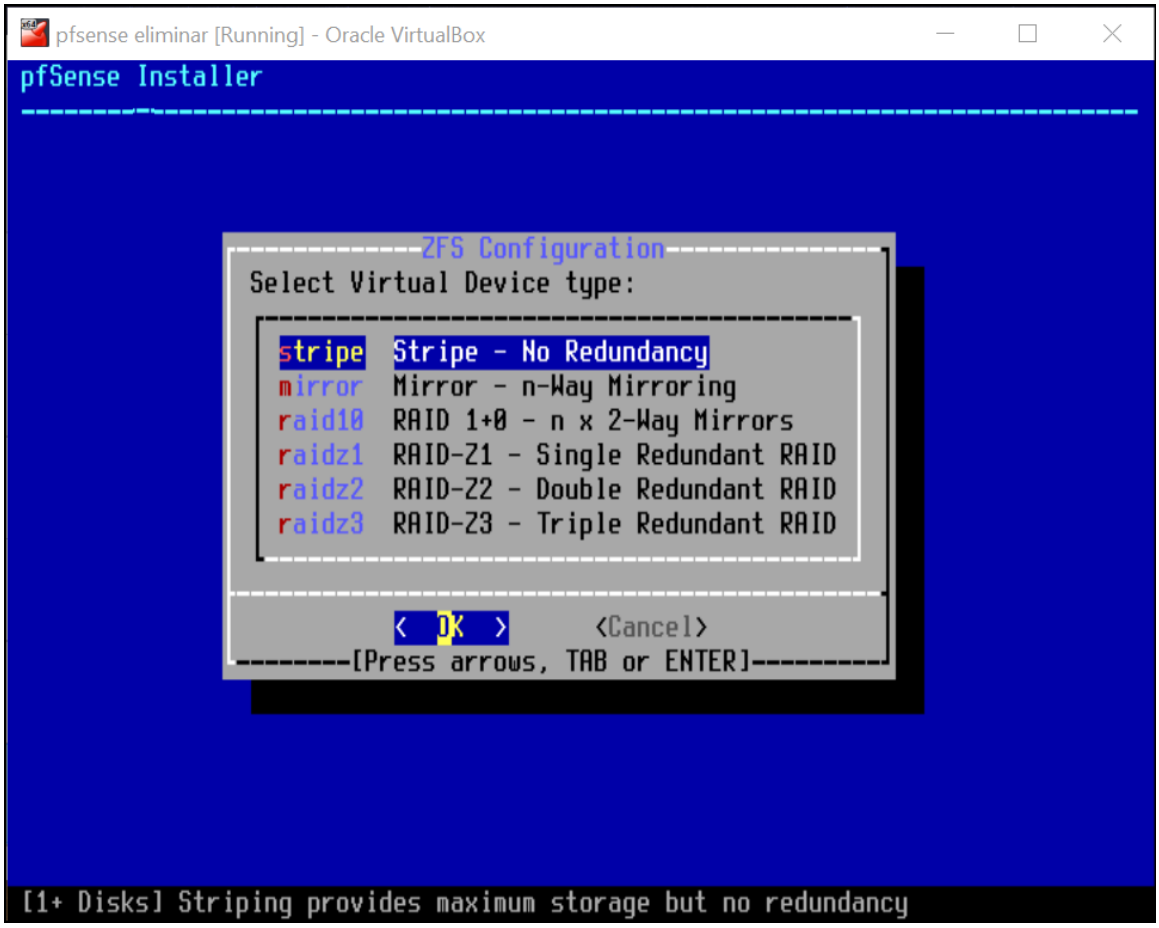

UTM Psense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Display
Screen
Remote Display
Recording
Video Memory:
16 MB
0 MB
128 MB
Monitor Count:
1
1
8
Scale Factor:
All Monitors
100%
100%
250%
Graphics Controller:
VMSVGA
Extended Features:
Enable 3D Acceleration
OK
Cancel
Help

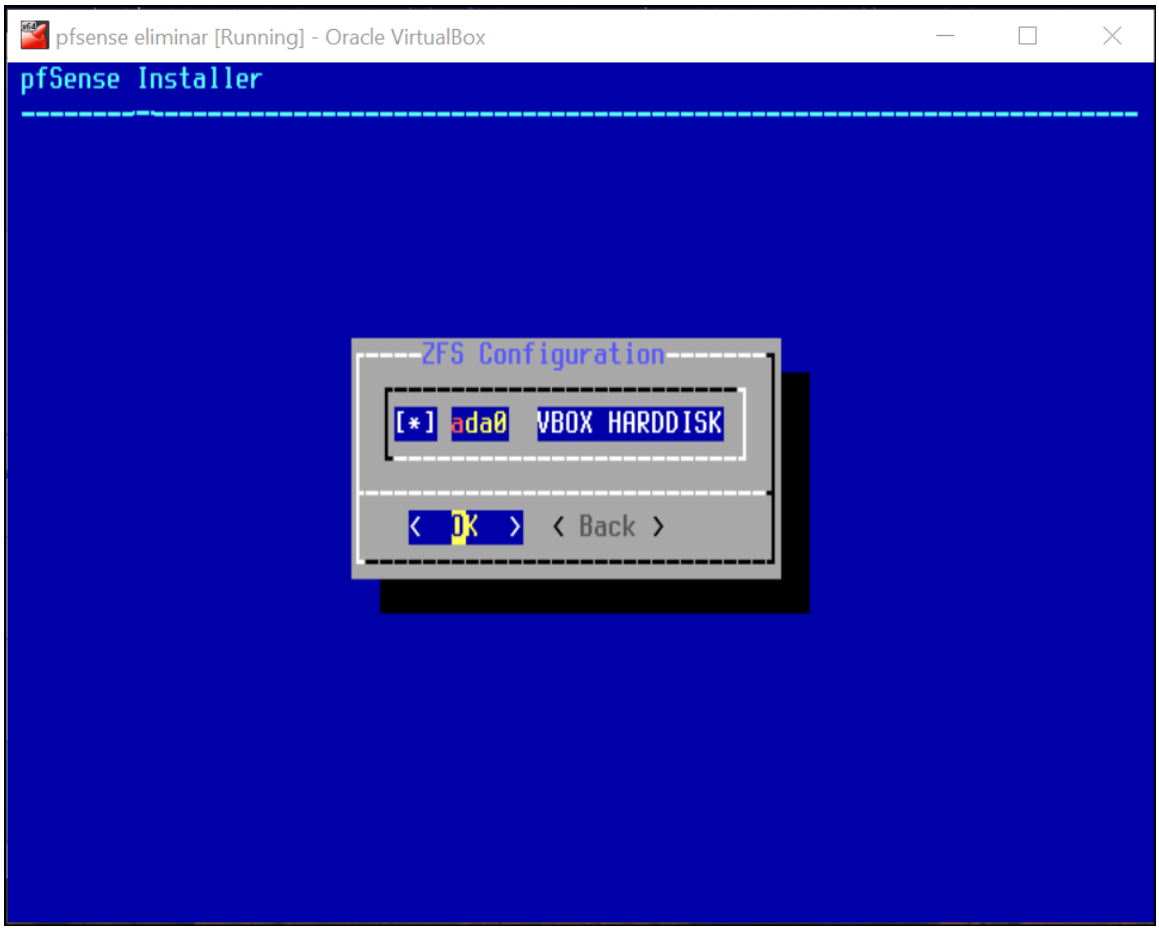

pfsense eliminar [Running] - Oracle VirtualBox
pfSense Installer
Copyright and distribution notice
Copyright and Trademark Notices.
Copyright 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.
Copyright 2014-2023. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.
All logos, text, and content of ESF and/or Netgate, including underlying
HTML code, designs, and graphics used and/or depicted herein are
protected under United States and international copyright and trademark
laws and treaties, and may not be used or reproduced without the prior
express written permission of ESF and/or Netgate.
"pfSense" is a registered trademark of ESF, exclusively licensed to
Netgate, and may not be used without the prior express written
permission of ESF and/or Netgate. All other trademarks shown herein are
26%
[Accept]

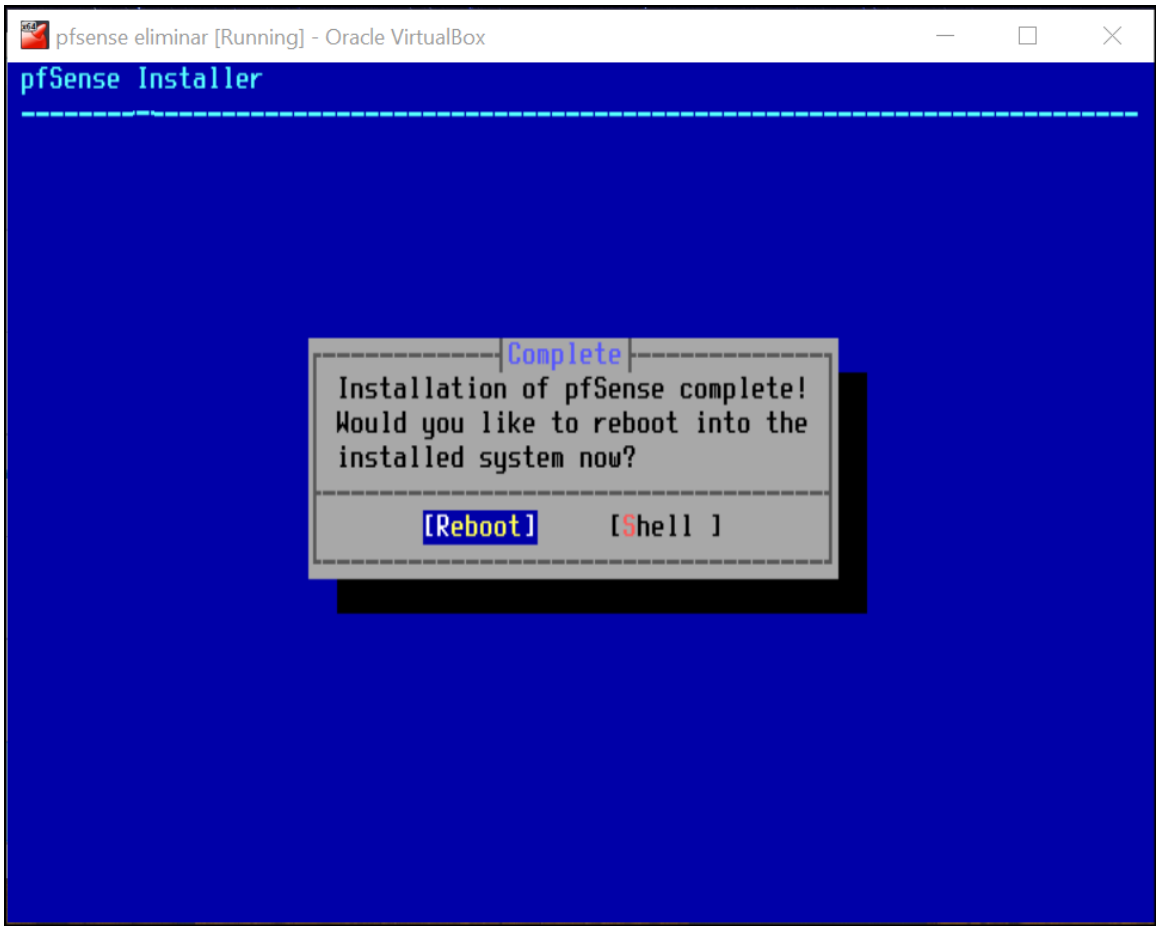

pfsense eliminar [Running] - Oracle VirtualBox
pfSense Installer
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
Recover config.xml
Recover config.xml from a previous install
OK
Cancel

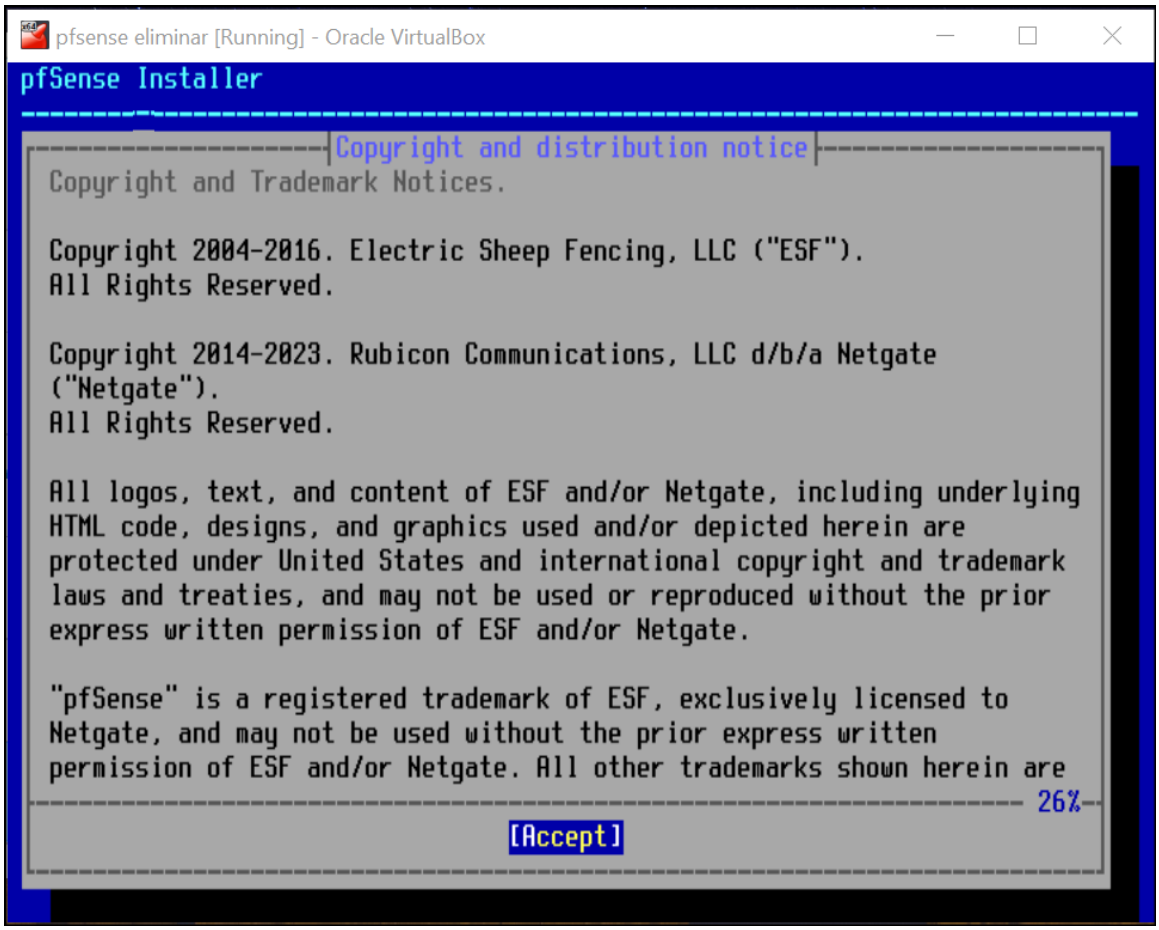

pfsense eliminar [Running] - Oracle VirtualBox
pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) Guided UFS Disk Setup
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>
To use ZFS with less than 8GB RAM, see https://wiki.freebsd.org/ZFSTuningGuide

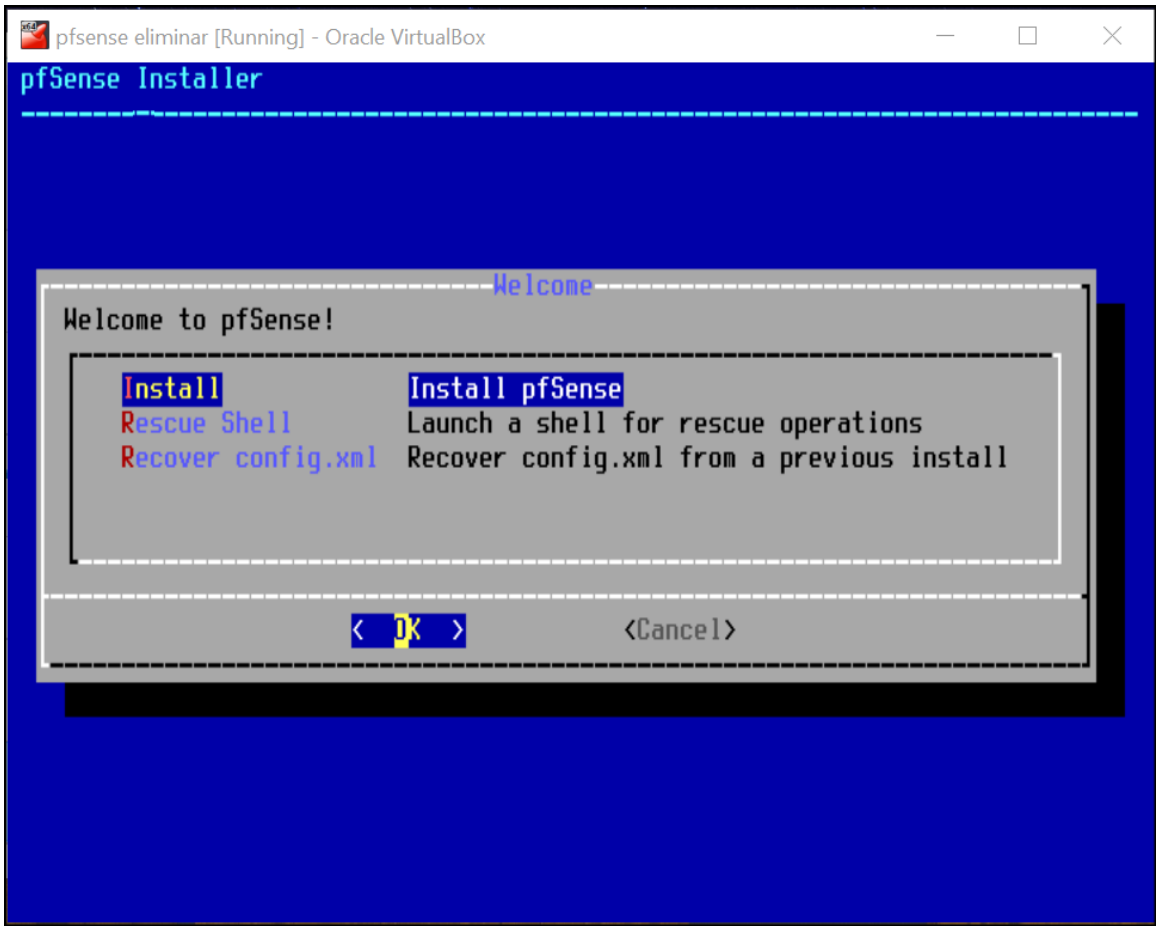

pfsense eliminar [Running] - Oracle VirtualBox
pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select> <Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]
Create ZFS boot pool with displayed options

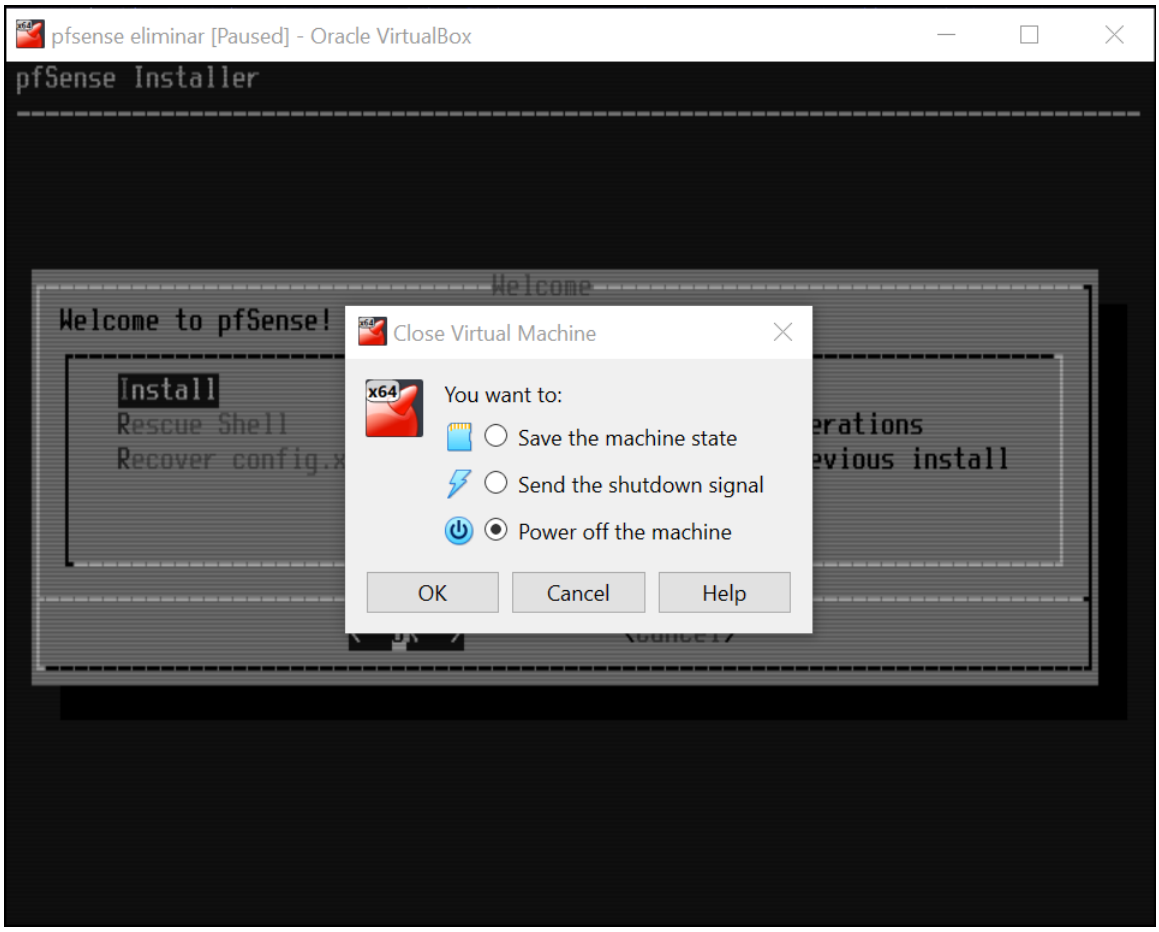

pfsense eliminar [Running] - Oracle VirtualBox
pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK >
<Cancel>
[Press arrows, TAB or ENTER]
[1+ Disks] Striping provides maximum storage but no redundancy

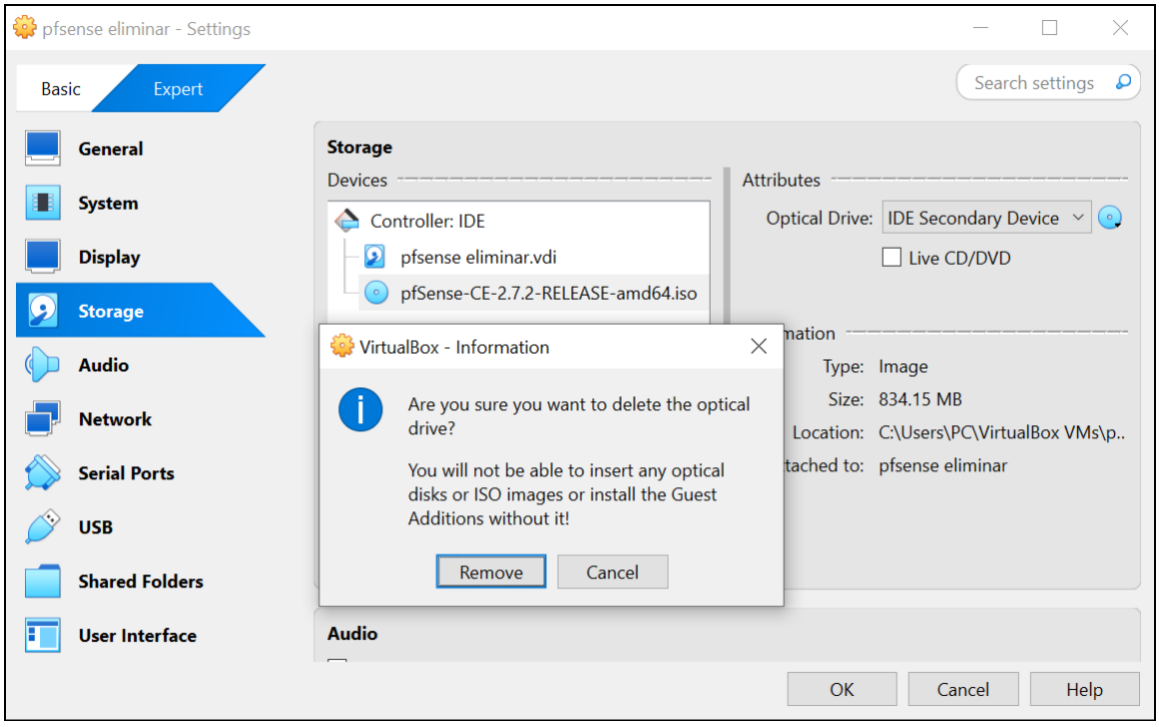

pfsense eliminar [Running] - Oracle VirtualBox
pfSense Installer
ZFS Configuration
[*] ada0 VBOX HARDDISK
< OK >
< Back >

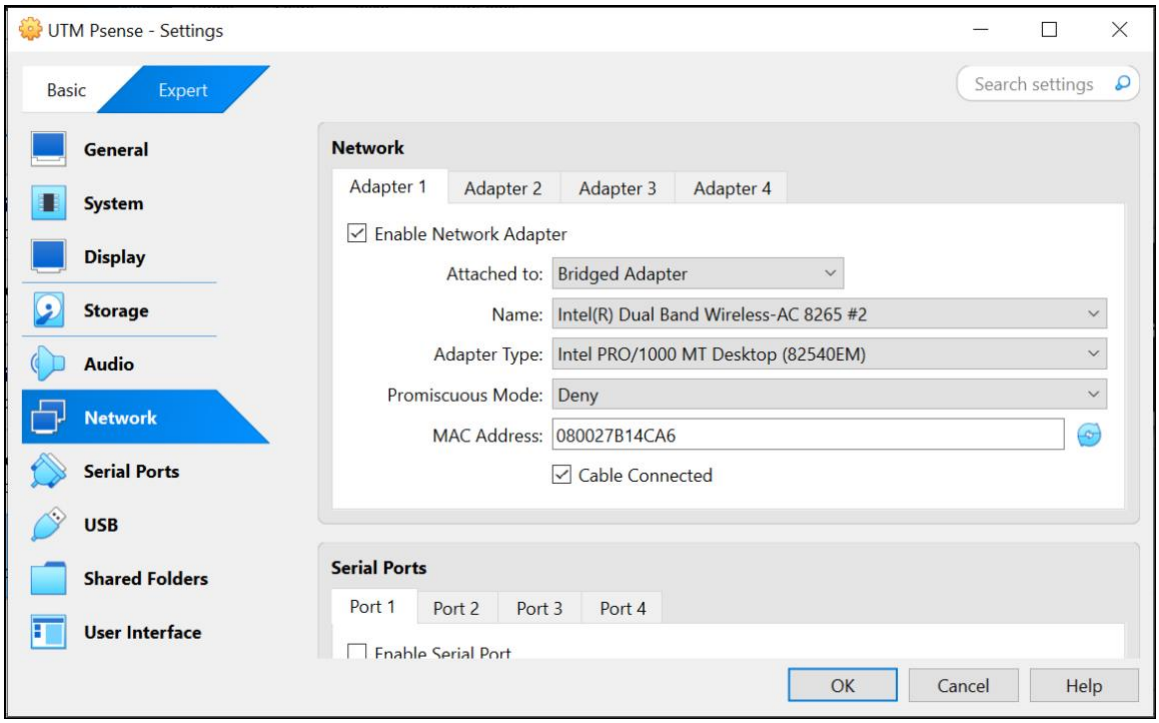

pfsense eliminar [Running] - Oracle VirtualBox
pfSense Installer
Complete
Installation of pfSense complete!
Would you like to reboot into the
installed system now?
[Reboot]
[Shell]

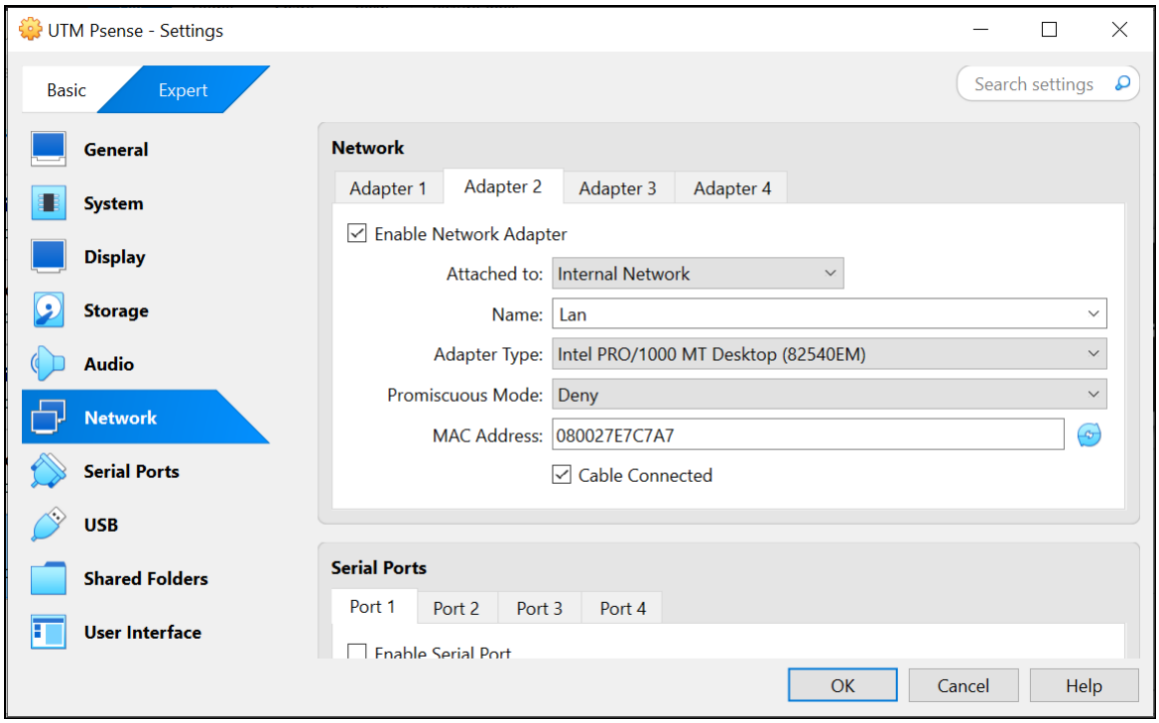

pfsense eliminar [Running] - Oracle VirtualBox
pfSense Installer
Copyright and distribution notice
Copyright and Trademark Notices.
Copyright 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.
Copyright 2014-2023. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.
All logos, text, and content of ESF and/or Netgate, including underlying
HTML code, designs, and graphics used and/or depicted herein are
protected under United States and international copyright and trademark
laws and treaties, and may not be used or reproduced without the prior
express written permission of ESF and/or Netgate.
"pfSense" is a registered trademark of ESF, exclusively licensed to
Netgate, and may not be used without the prior express written
permission of ESF and/or Netgate. All other trademarks shown herein are
26%
[Accept]

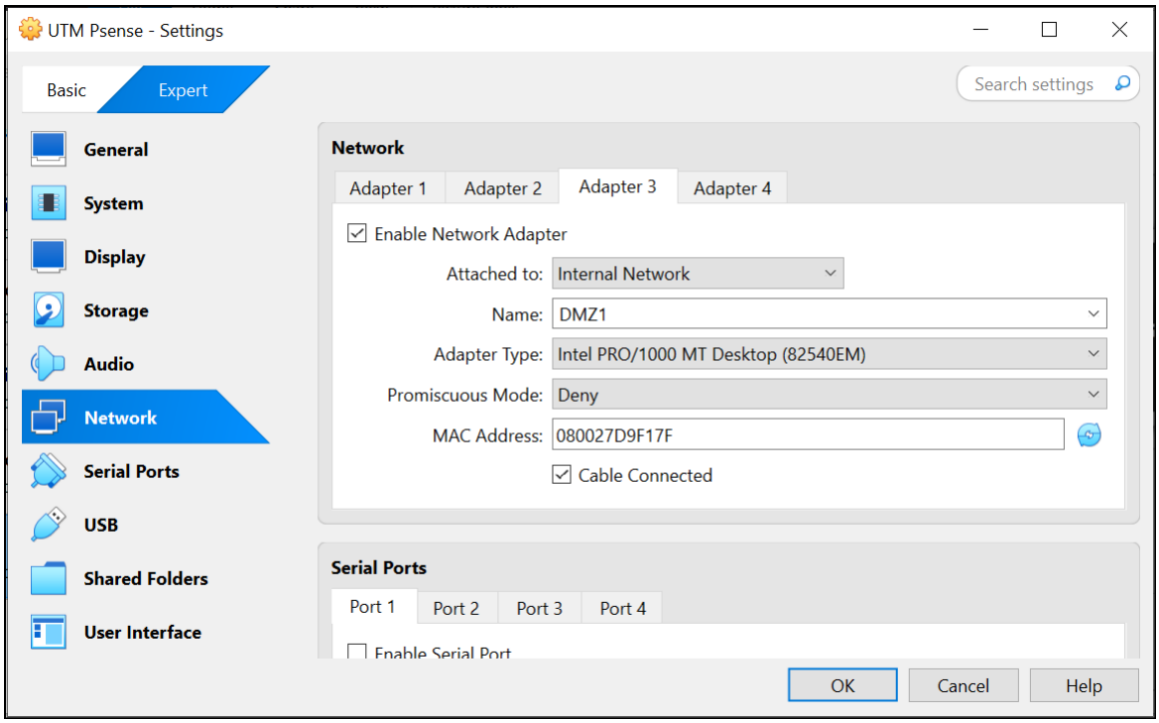

pfsense eliminar [Running] - Oracle VirtualBox
pfSense Installer
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
Recover config.xml
Recover config.xml from a previous install
OK
Cancel

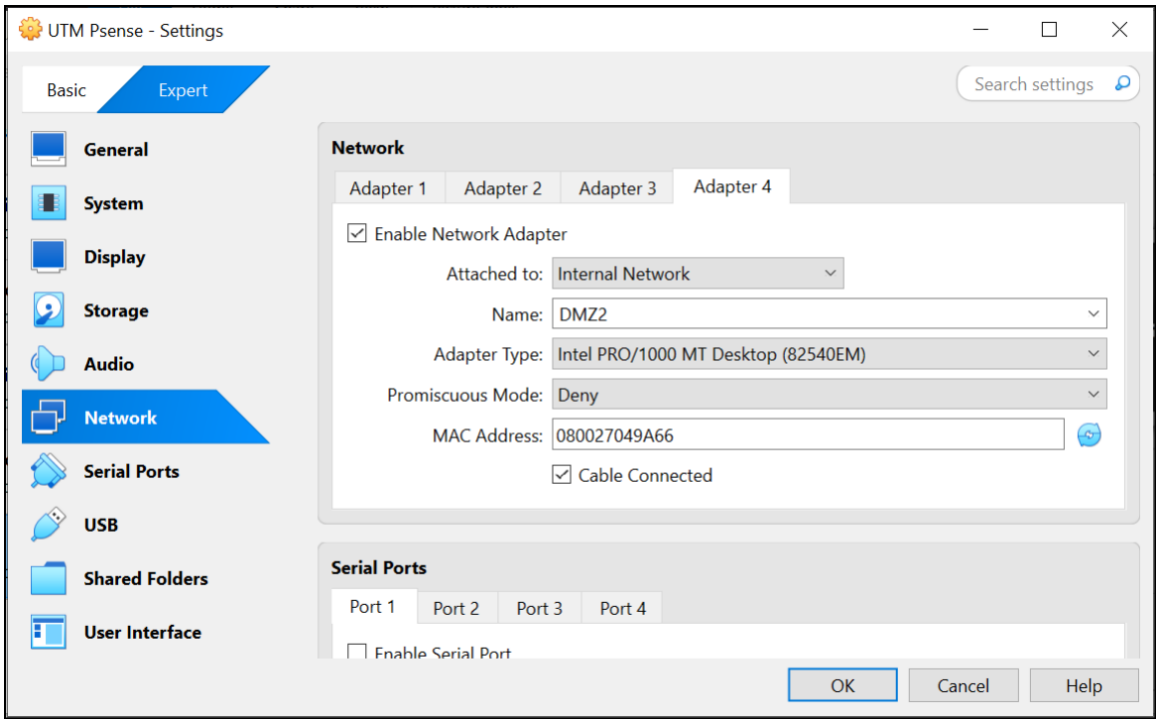

pfsense eliminar [Paused] - Oracle VirtualBox
pfSense Installer
Welcome
Welcome to pfSense!
Install
Rescue Shell
Recover config.x
erations
evious install
Close Virtual Machine
You want to:
Save the machine state
Send the shutdown signal
Power off the machine
OK
Cancel
Help

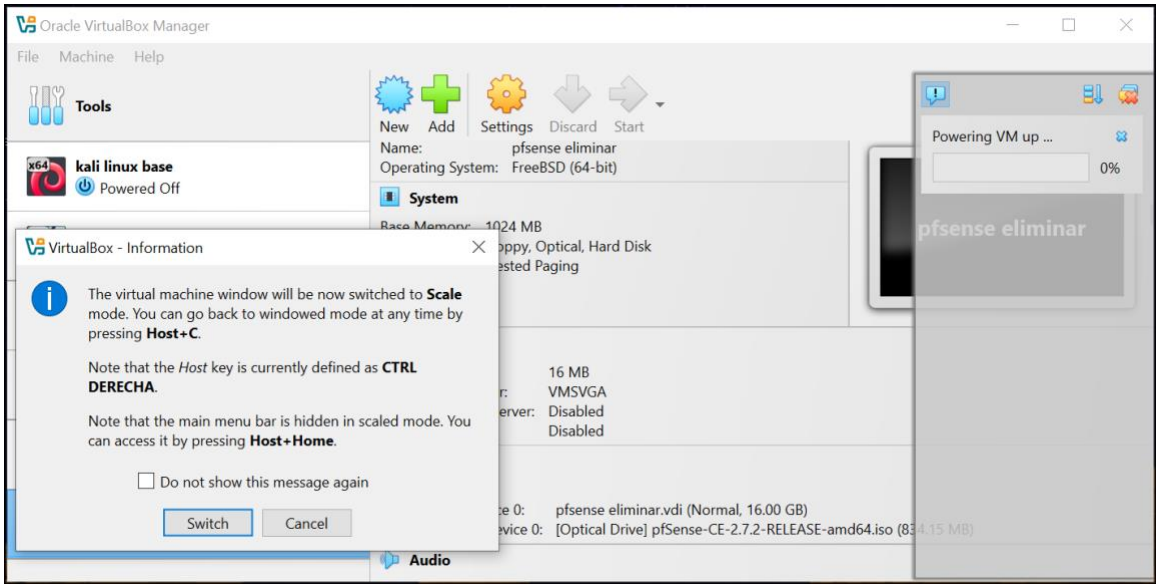

pfsense eliminar - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Devices
Controller: IDE
pfsense eliminar.vdi
pfSense-CE-2.7.2-RELEASE-amd64.iso
Attributes
Optical Drive: IDE Secondary Device
Live CD/DVD
Type: Image
Size: 834.15 MB
Location: C:\Users\PC\VirtualBox VMs\p..
tached to: pfsense eliminar
VirtualBox - Information
Are you sure you want to delete the optical drive?
You will not be able to insert any optical disks or ISO images or install the Guest Additions without it!
Remove
Cancel
Audio
OK
Cancel
Help

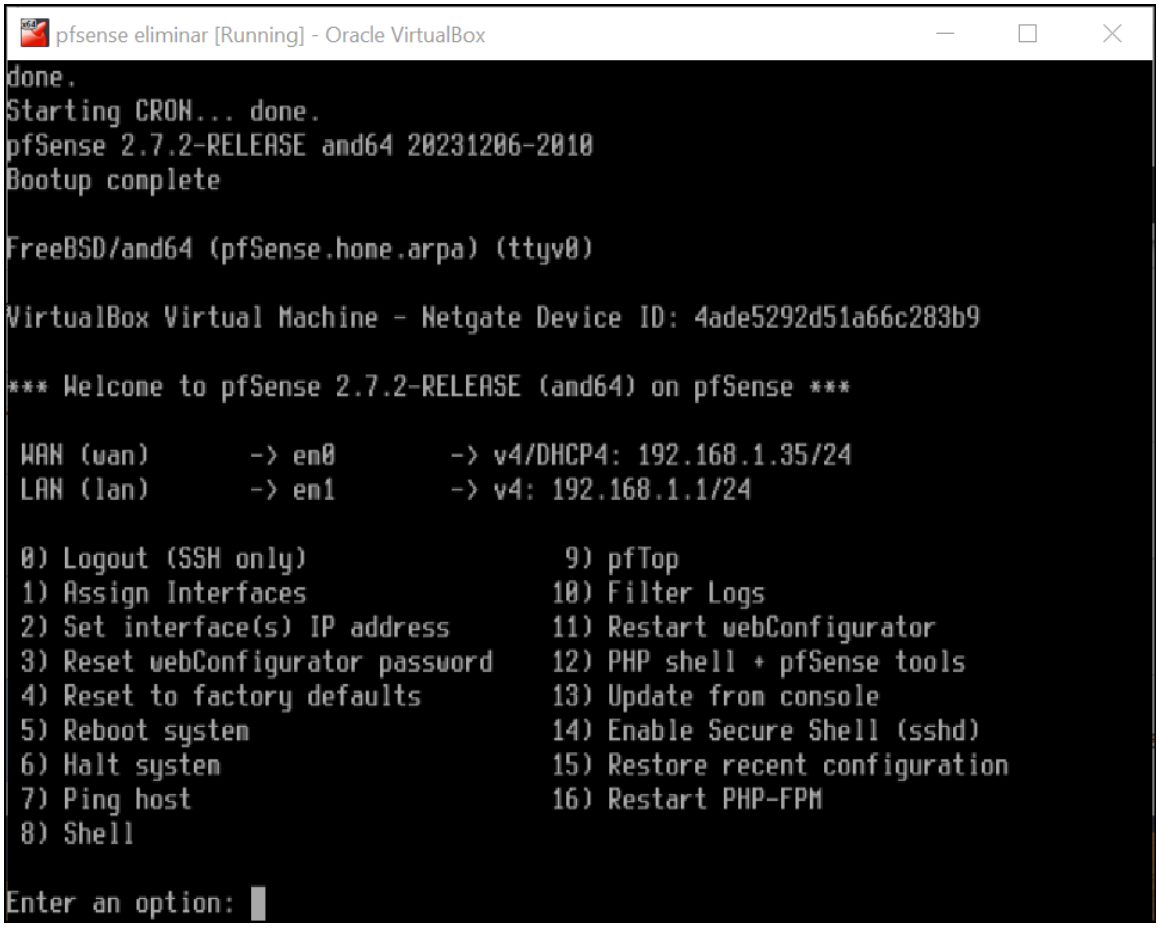

UTM Psense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: Intel(R) Dual Band Wireless-AC 8265 #2
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027B14CA6
Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
Enable Serial Port
OK
Cancel
Help


UTM Psense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Internal Network
Name: Lan
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027E7C7A7
Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
Enable Serial Port
OK
Cancel
Help


UTM Psense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Internal Network
Name: DMZ1
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027D9F17F
Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
Enable Serial Port
OK
Cancel
Help


UTM Psense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Internal Network
Name: DMZ2
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027049A66
Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
Enable Serial Port
OK
Cancel
Help

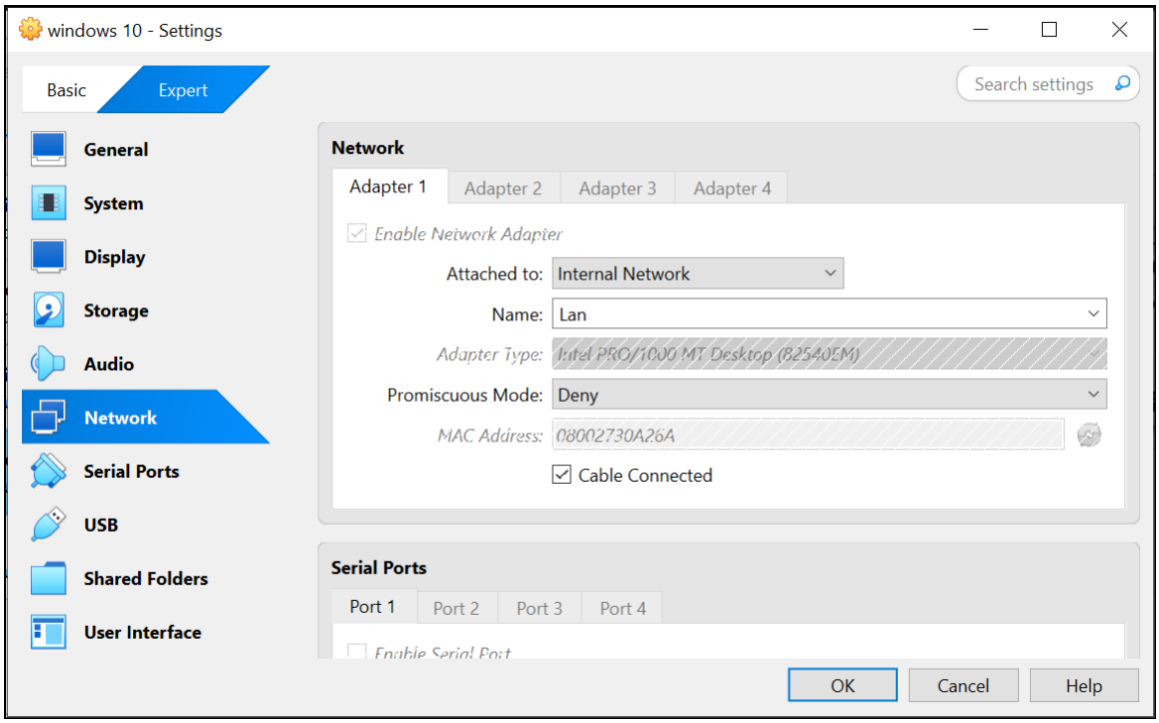

Oracle VirtualBox Manager
File Machine Help
Tools
kali linux base
Powered Off
New Add Settings Discard Start
Name: pfsense eliminar
Operating System: FreeBSD (64-bit)
System
VirtualBox - Information
The virtual machine window will be now switched to Scale mode. You can go back to windowed mode at any time by pressing Host+C.
Note that the Host key is currently defined as CTRL DERECHA.
Note that the main menu bar is hidden in scaled mode. You can access it by pressing Host+Home.
Do not show this message again
Switch
Cancel
16 MB
VMSVGA
Disabled
Disabled
pfsense eliminar.vdi (Normal, 16.00 GB)
[Optical Drive] pfSense-CE-2.7.2-RELEASE-amd64.iso
Audio
Powering VM up ...
0%
pfsense eliminar

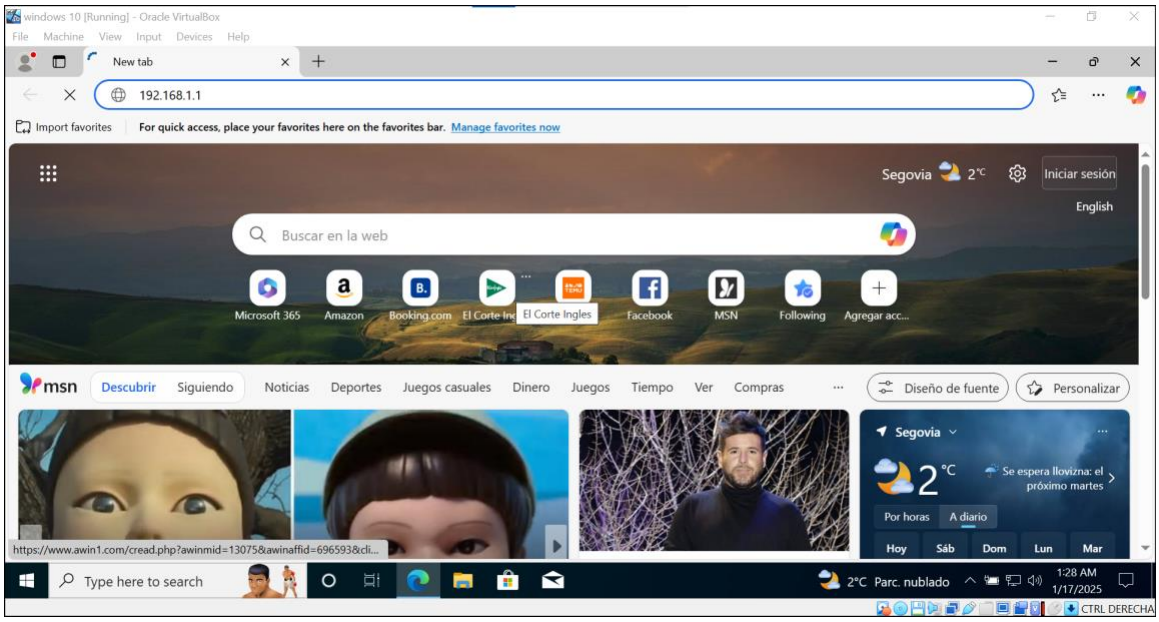

pfsense eliminar [Running] - Oracle VirtualBox
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 4ade5292d51a66c283b9
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.35/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

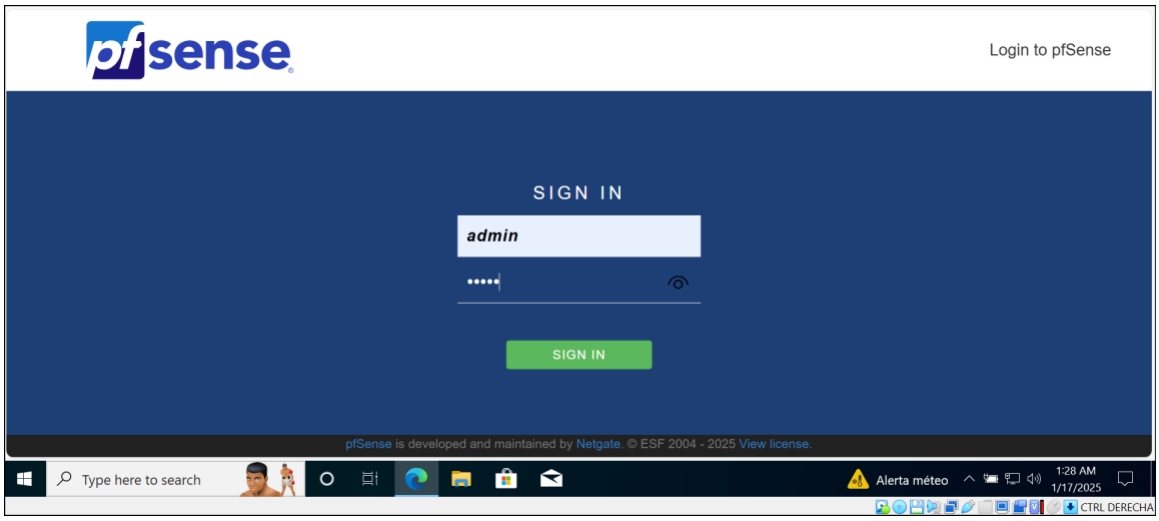
1.2. Configuración

En esta etapa de la práctica, se inició la máquina virtual con Windows y se estableció conexión con **Pfsense** a través del navegador. Durante este proceso, se llevó a cabo la configuración inicial del sistema.

Además, se ha asignado ya la red LAN a esta máquina.







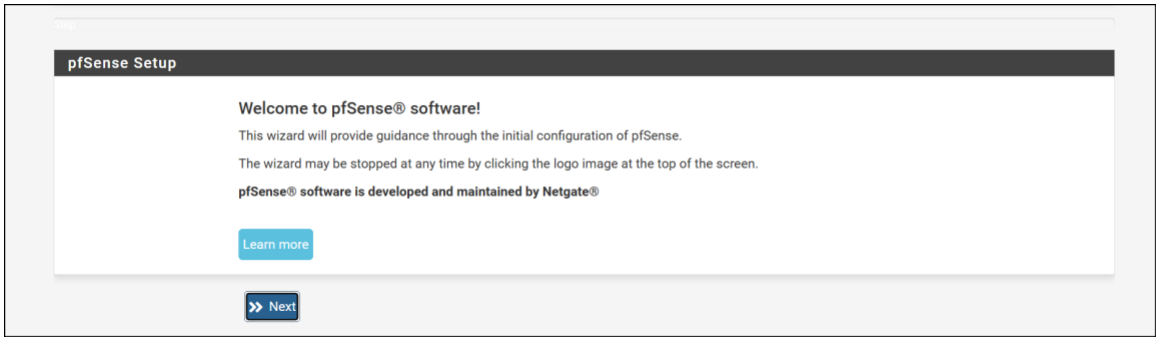
No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.

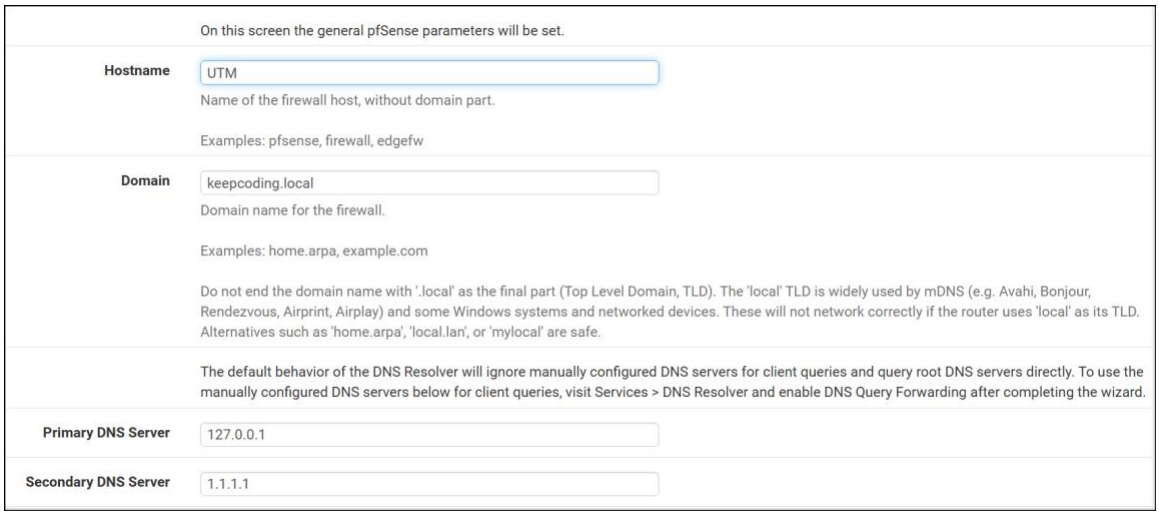
Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance.

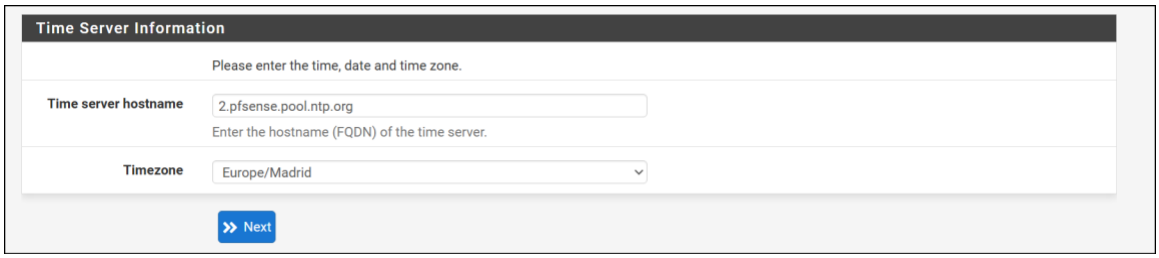
The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

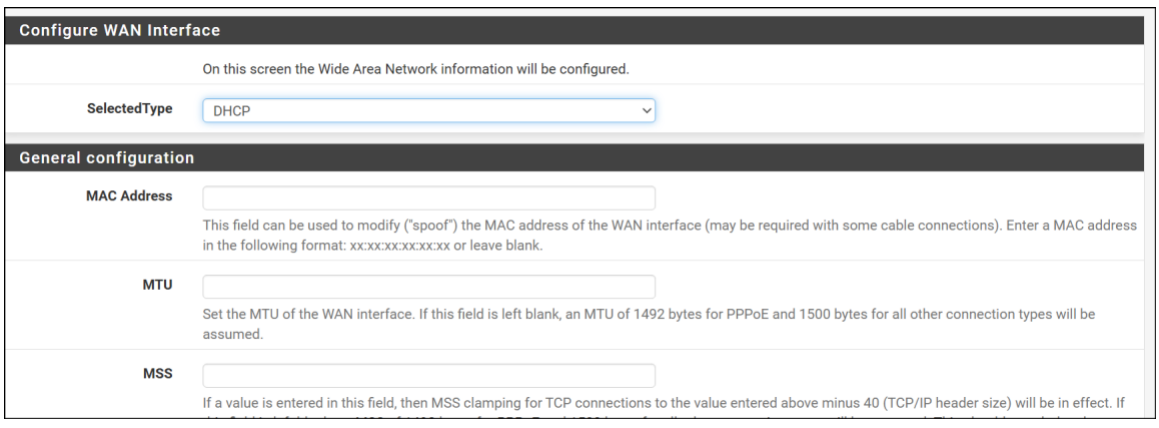
Accept

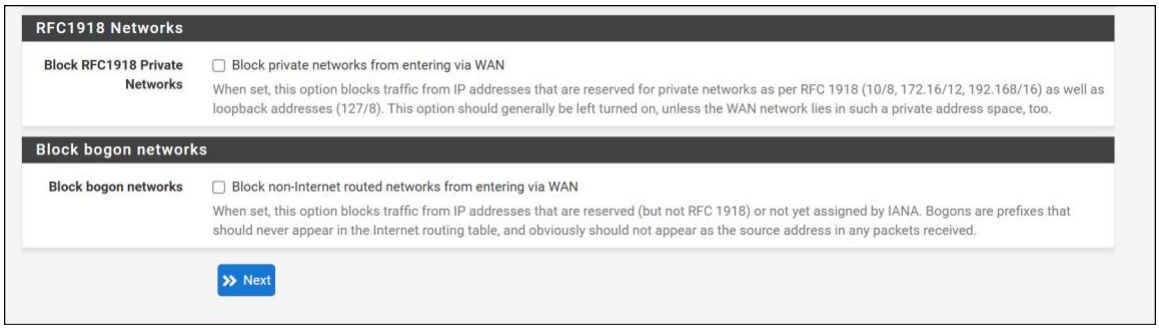


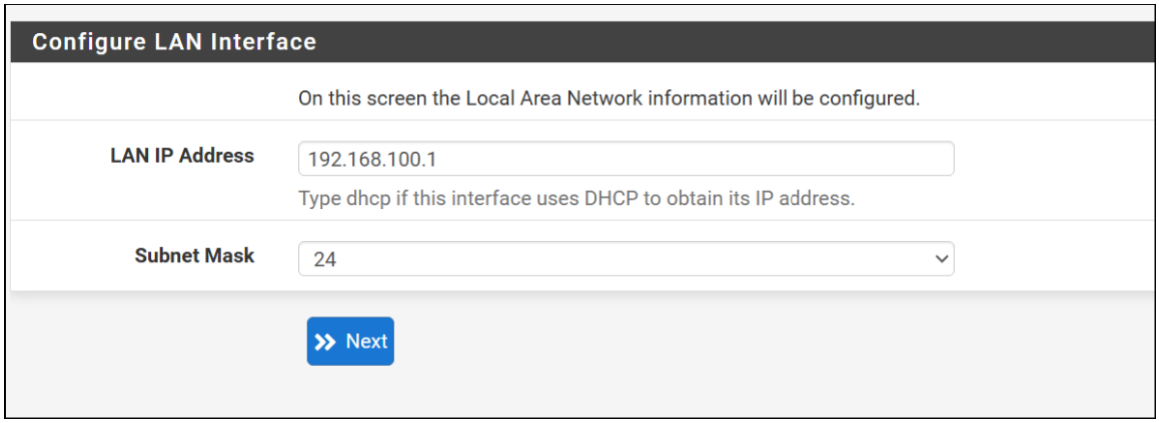

On this screen the general pfSense parameters will be set.
Hostname
UTM
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw
Domain
keepcoding.local
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.
Primary DNS Server
127.0.0.1
Secondary DNS Server
1.1.1.1

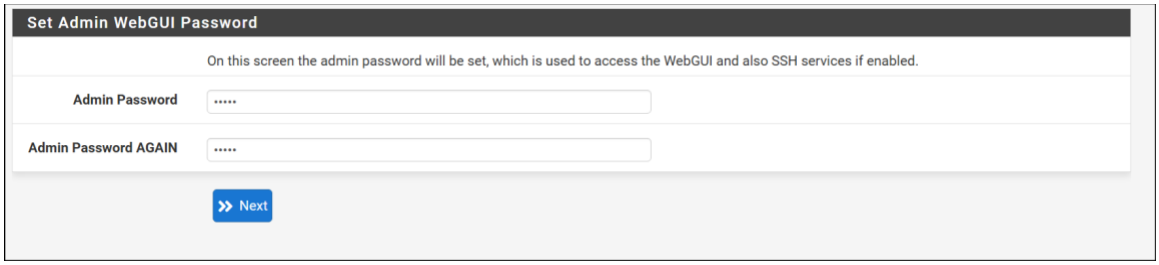

Primary DNS Server
127.0.0.1
Secondary DNS Server
1.1.1.1
Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN
Next


Time Server Information
Please enter the time, date and time zone.
Time server hostname
2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.
Timezone
Europe/Madrid
Next

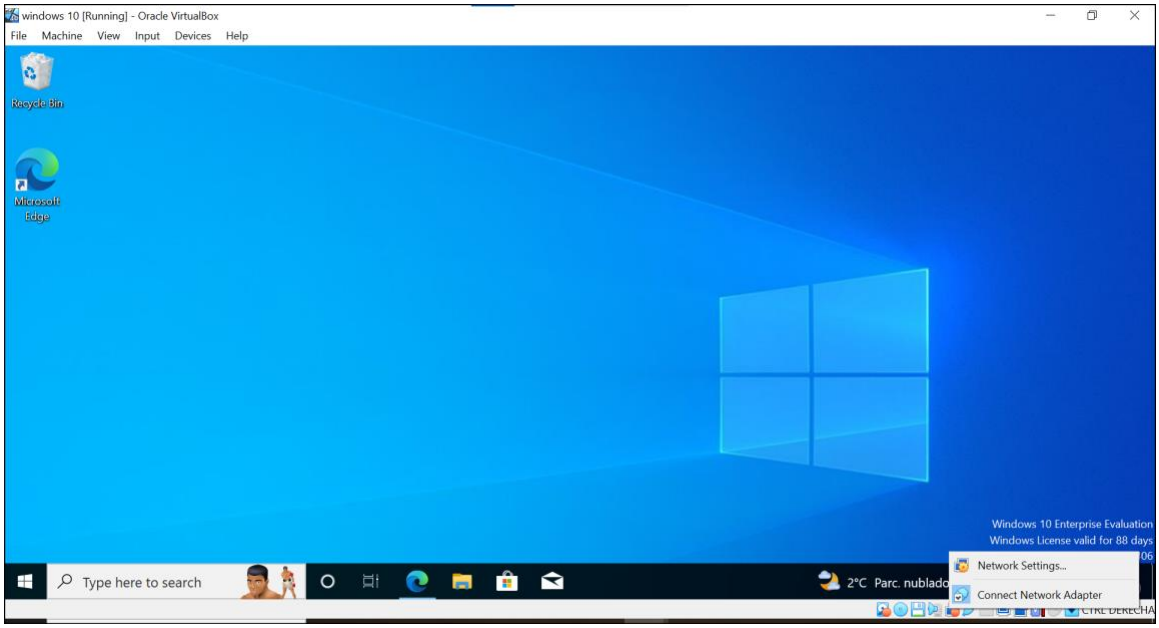

Configure WAN Interface
On this screen the Wide Area Network information will be configured.
SelectedType
DHCP
General configuration
MAC Address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If

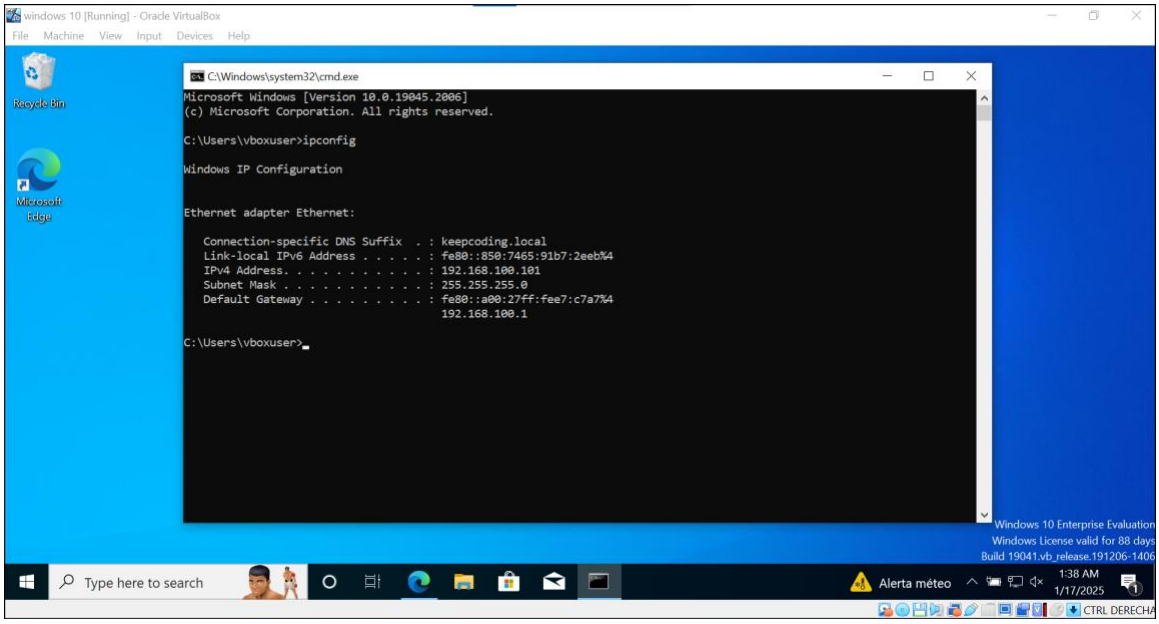

RFC1918 Networks
Block RFC1918 Private Networks
Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.
Block bogon networks
Block bogon networks
Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.
Next

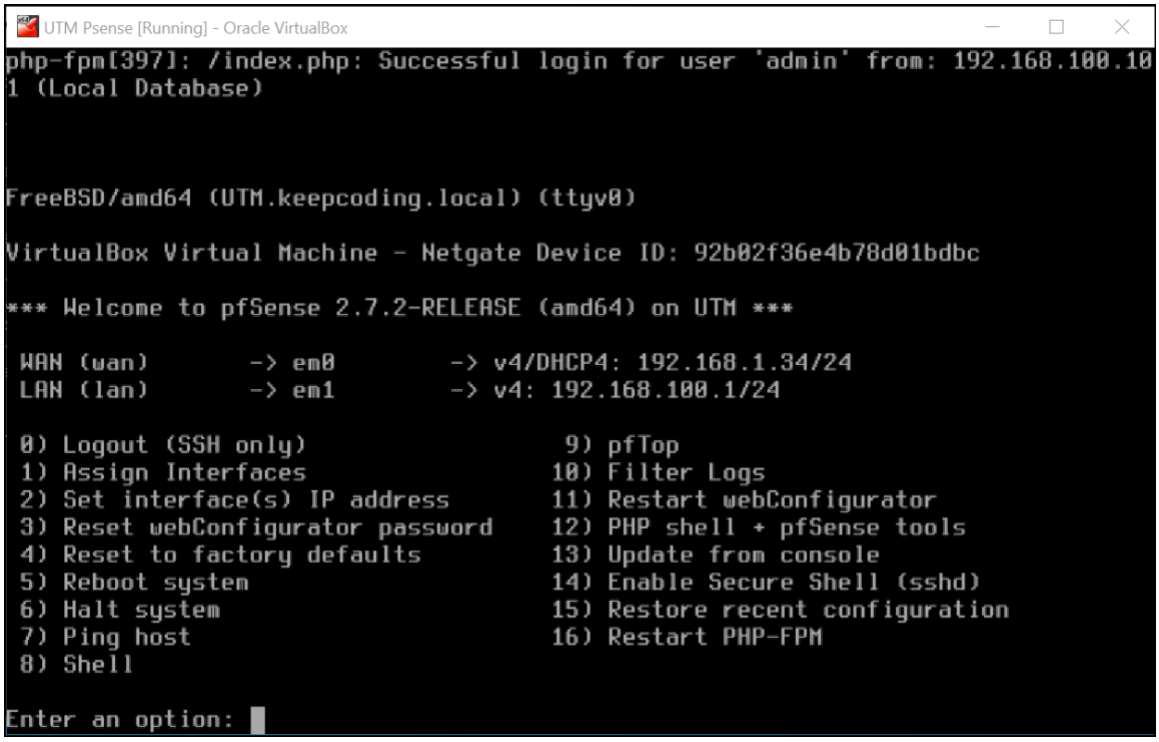

Configure LAN Interface
On this screen the Local Area Network information will be configured.
LAN IP Address
192.168.100.1
Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask
24
Next

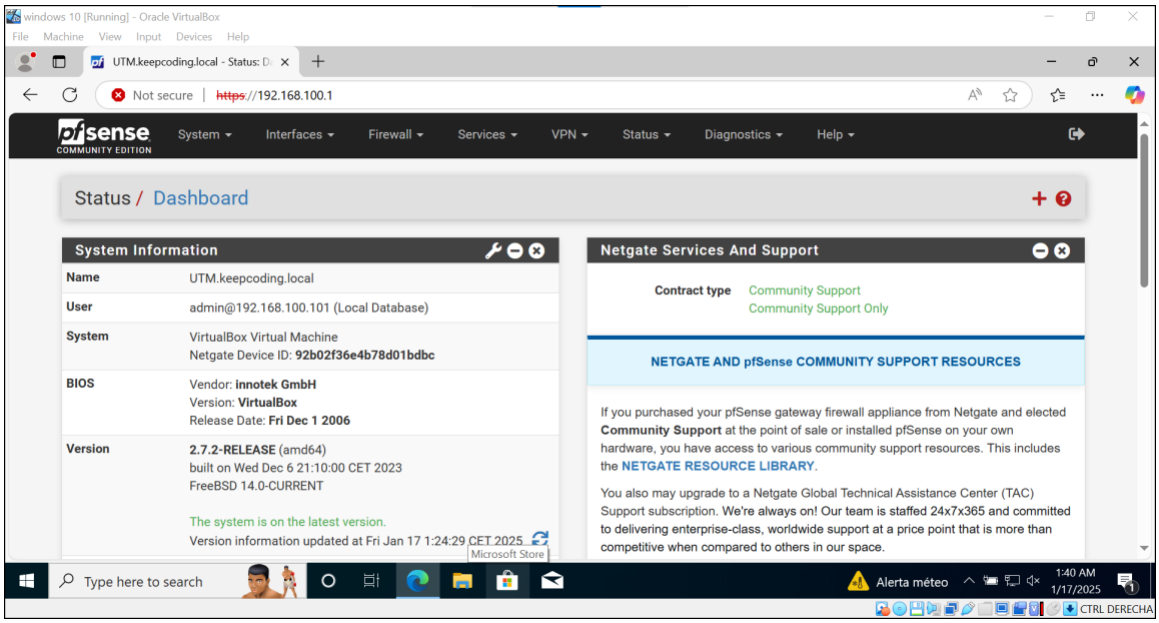

Set Admin WebGUI Password
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.
Admin Password
Admin Password AGAIN
Next


Reload configuration
Click 'Reload' to reload pfSense with new changes.
Reload


windows 10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Type here to search
2°C Parc. nublado
Network Settings...
Connect Network Adapter
Windows 10 Enterprise Evaluation
Windows License valid for 88 days


windows 10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\vboxuser>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : keepcoding.local
Link-local IPv6 Address . . . . . : fe80::850:7465:91b7:2eeb%4
IPv4 Address. . . . . : 192.168.100.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::a00:27ff:fee7:c7a7%4
192.168.100.1
C:\Users\vboxuser>
Type here to search
Alerta météo
1:38 AM
1/17/2025
Windows 10 Enterprise Evaluation
Windows License valid for 88 days
Build 19041.vb_release.191206-1406



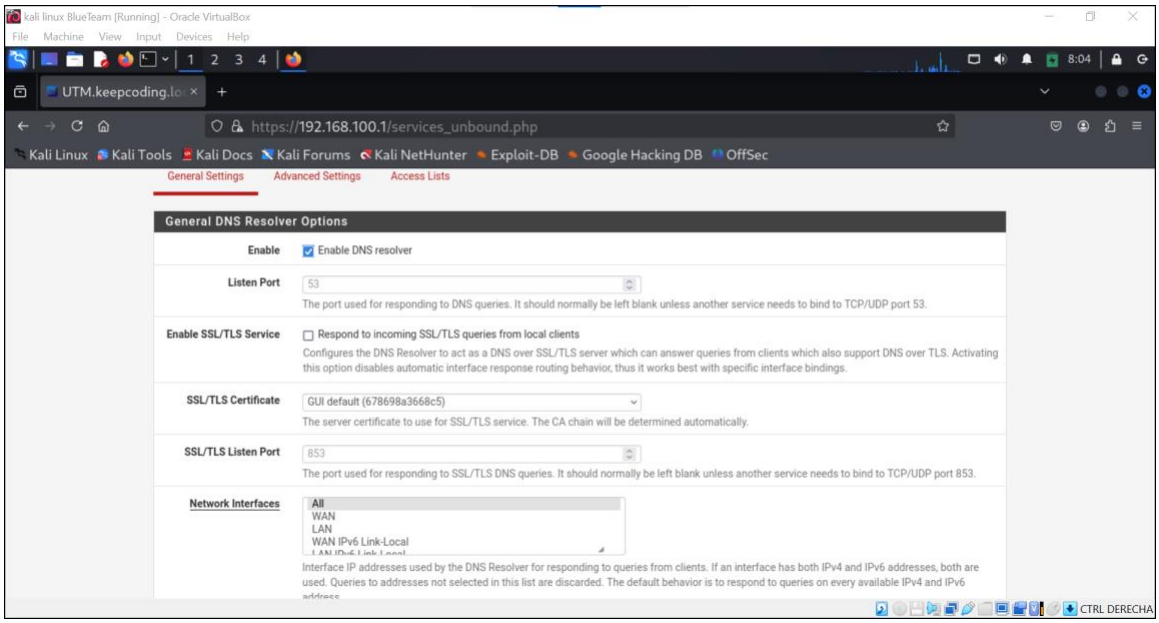


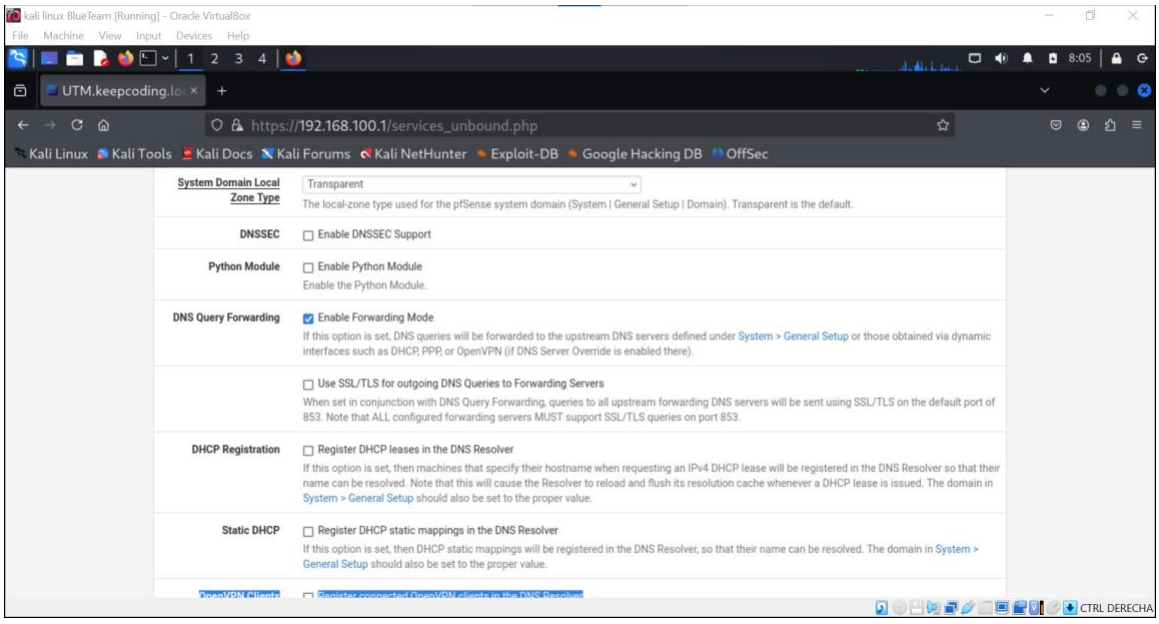
1.3. IPS y DHCP

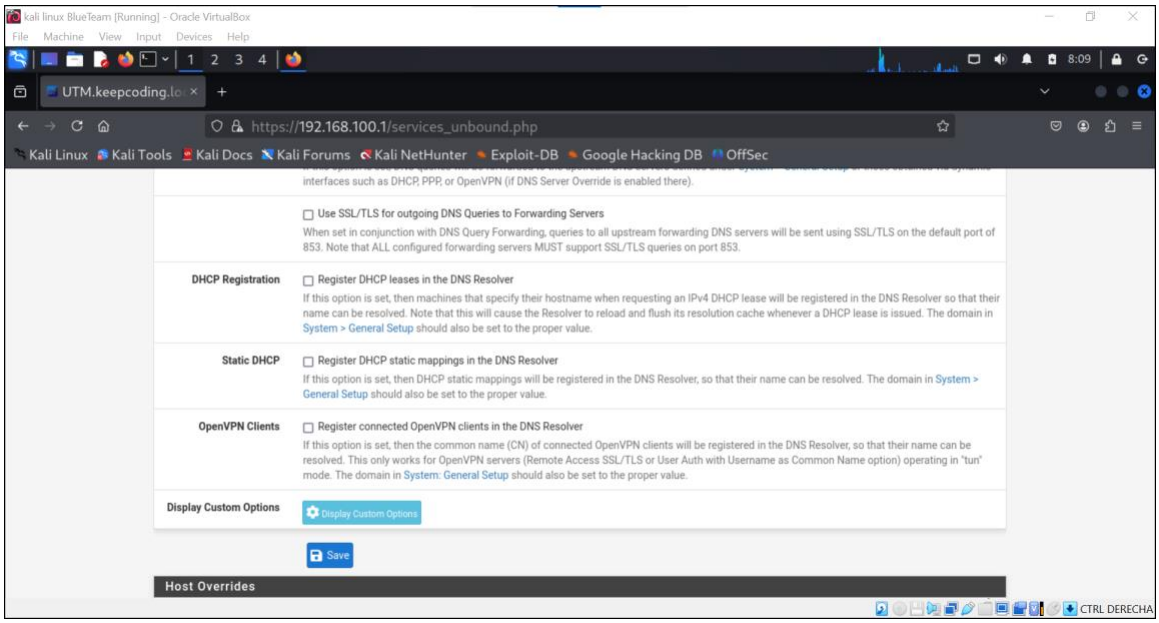
En este apartado, se procedió a asignar direcciones IP dinámicas a las redes LAN, DMZ y DMZ2, estableciendo rangos específicos de direcciones IP para cada una de ellas, con el objetivo de prevenir conflictos. Para ello, se habilitó el servicio DHCP en dichas redes, permitiendo la asignación automática de direcciones IP a los dispositivos conectados. Además, DHCP simplifica la administración de la red al proporcionar de manera

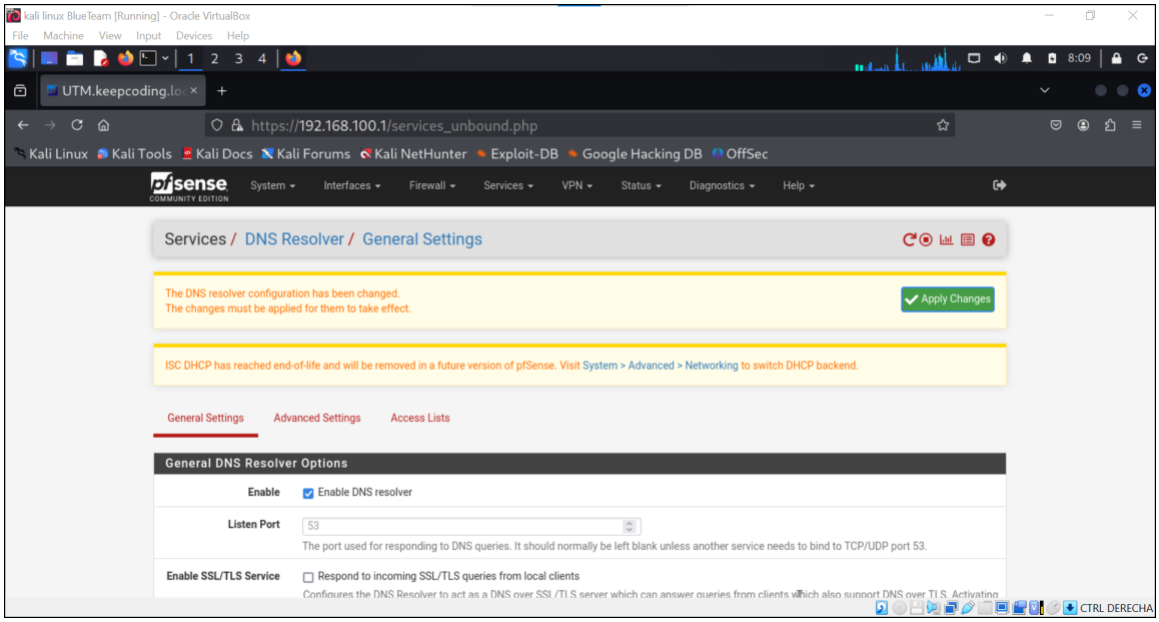
centralizada otros parámetros esenciales, como la máscara de subred, la puerta de enlace predeterminada y los servidores DNS, asegurando así una configuración correcta y eficiente en todas las conexiones.

1.3.1. DNS

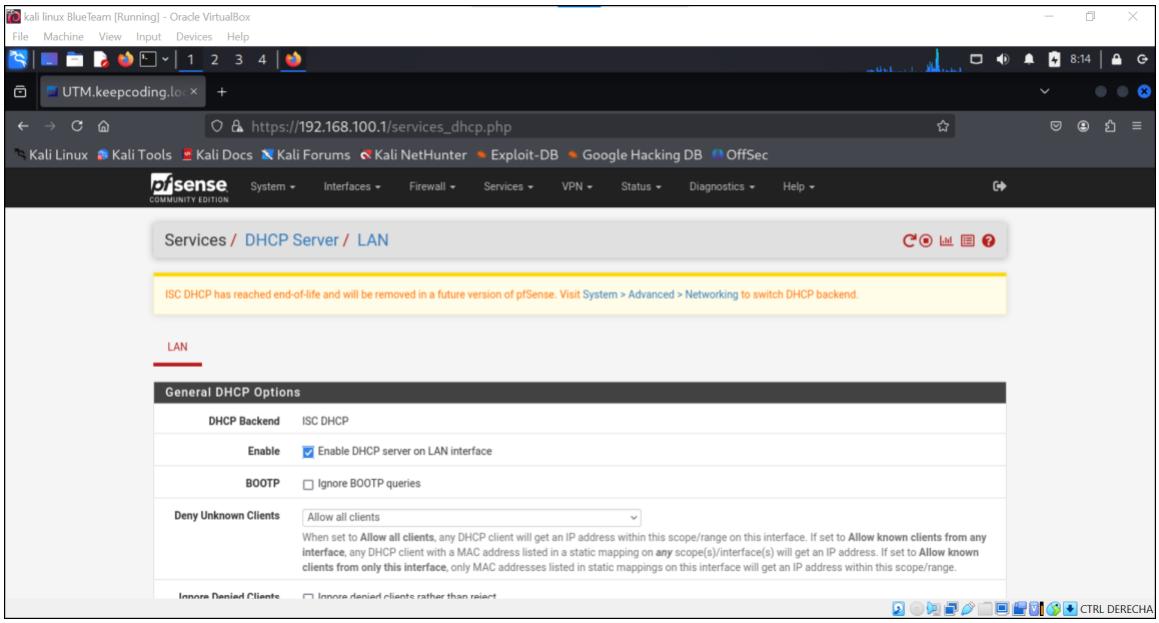


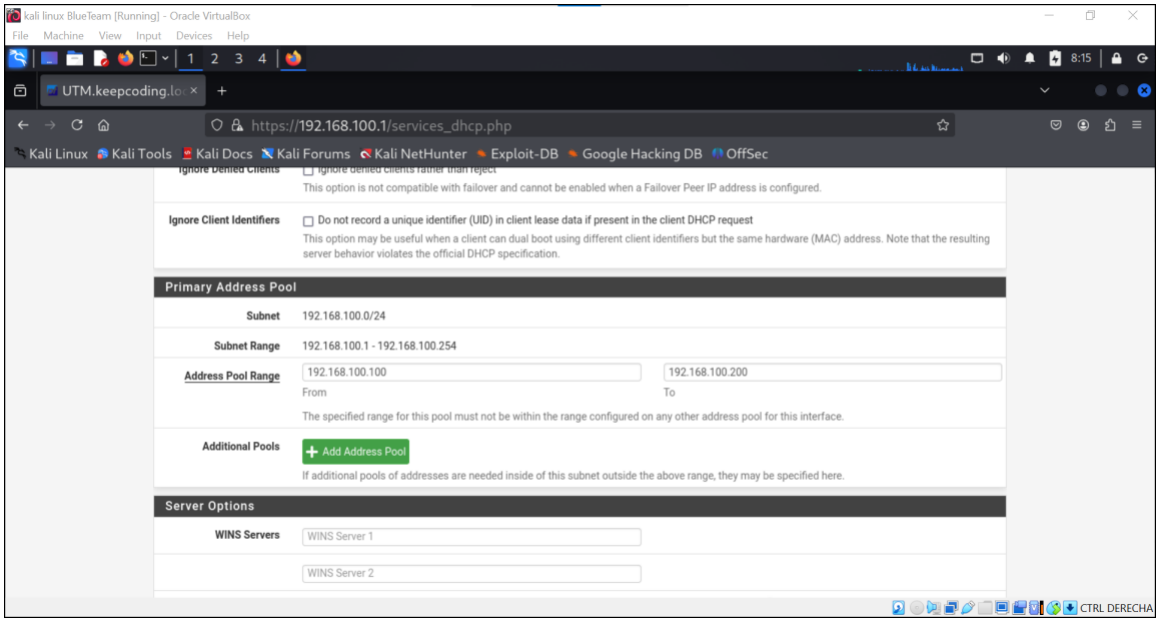


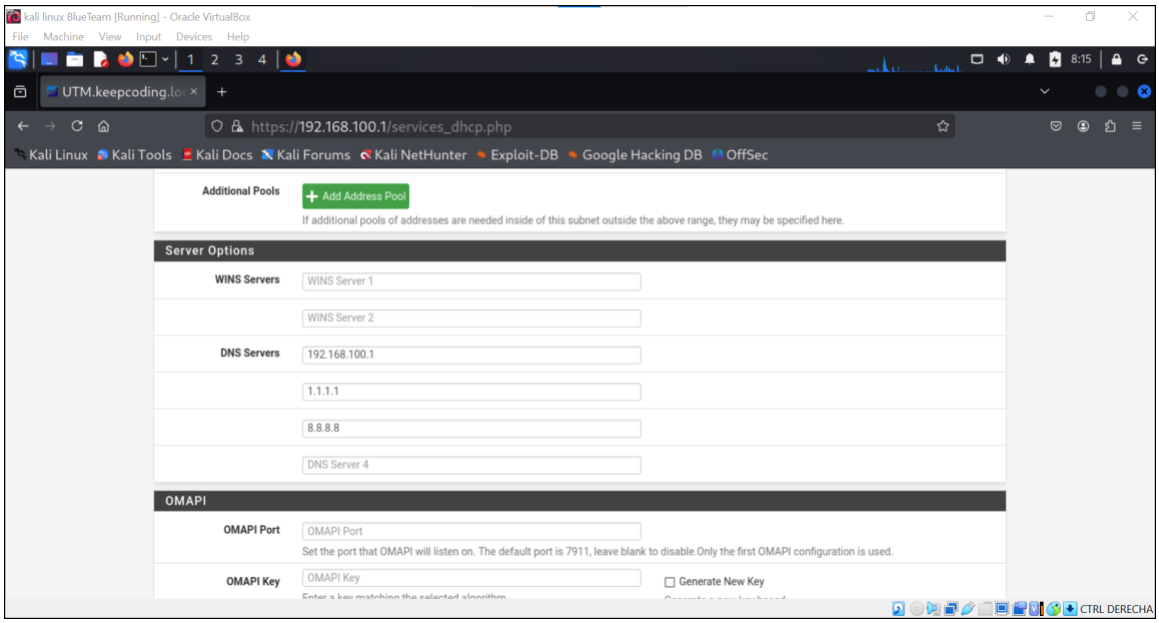

kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
UTM.keepcoding.lo
https://192.168.100.1/services_unbound.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).
Use SSL/TLS for outgoing DNS Queries to Forwarding Servers
When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.
DHCP Registration
Register DHCP leases in the DNS Resolver
If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in System > General Setup should also be set to the proper value.
Static DHCP
Register DHCP static mappings in the DNS Resolver
If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.
OpenVPN Clients
Register connected OpenVPN clients in the DNS Resolver
If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in System: General Setup should also be set to the proper value.
Display Custom Options
Display Custom Options
Save
Host Overrides
CTRL DERECHA

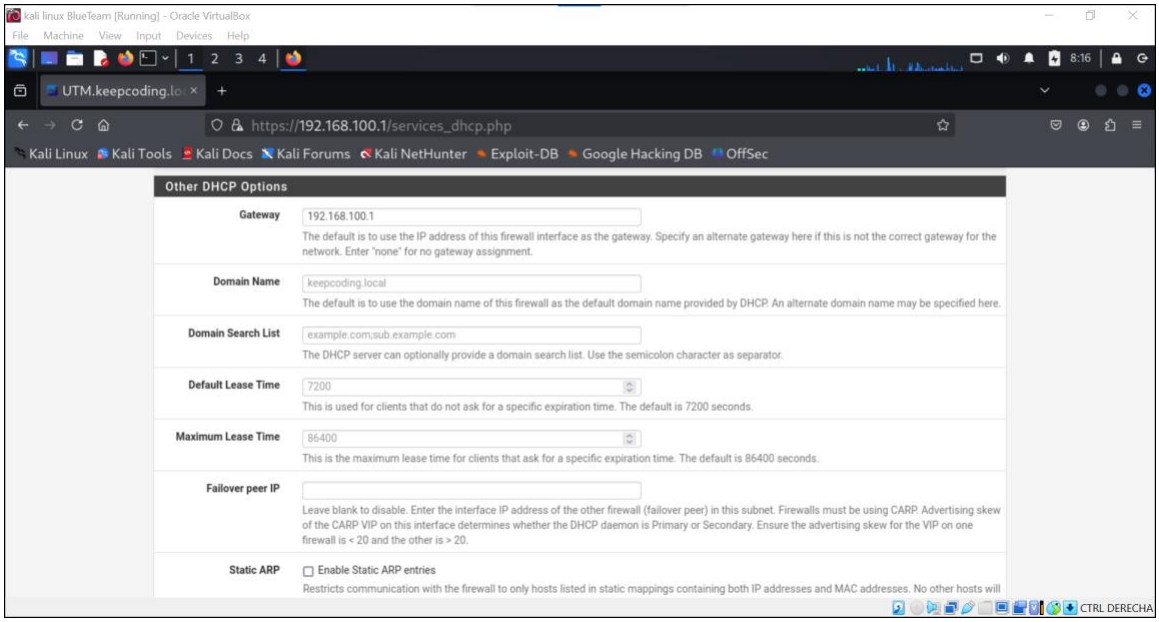

kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
UTM.keepcoding.lo
https://192.168.100.1/services_unbound.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Services / DNS Resolver / General Settings
The DNS resolver configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
General Settings
Advanced Settings
Access Lists
General DNS Resolver Options
Enable
Enable DNS resolver
Listen Port
53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.
Enable SSL/TLS Service
Respond to incoming SSL/TLS queries from local clients
CTRL DERECHA

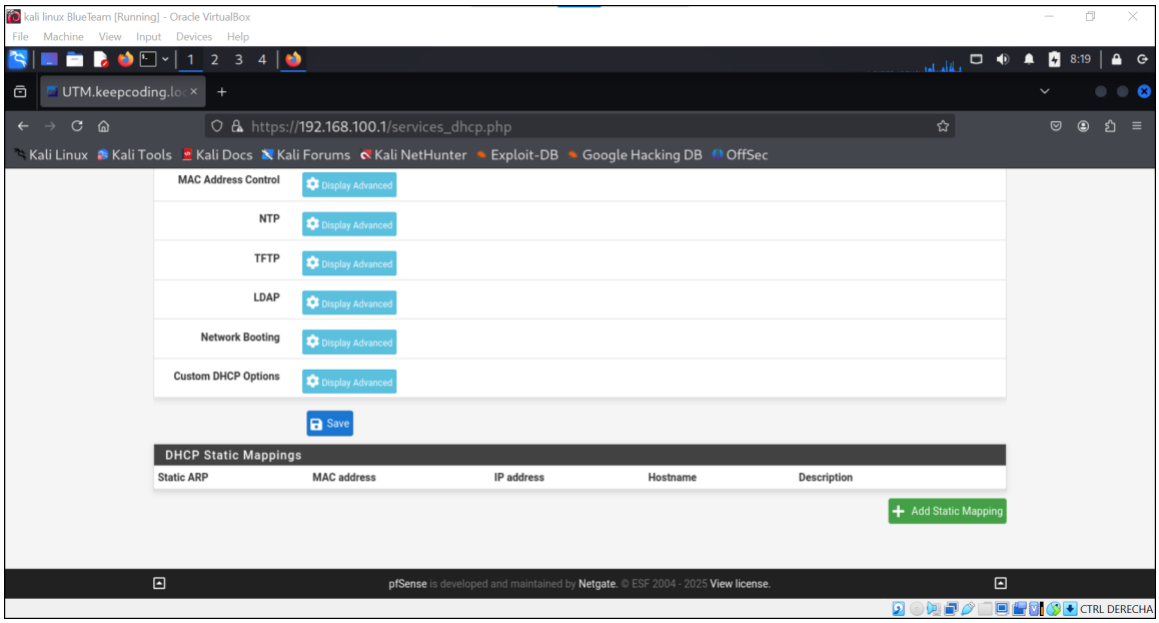
1.3.2. DHCP de la red LAN

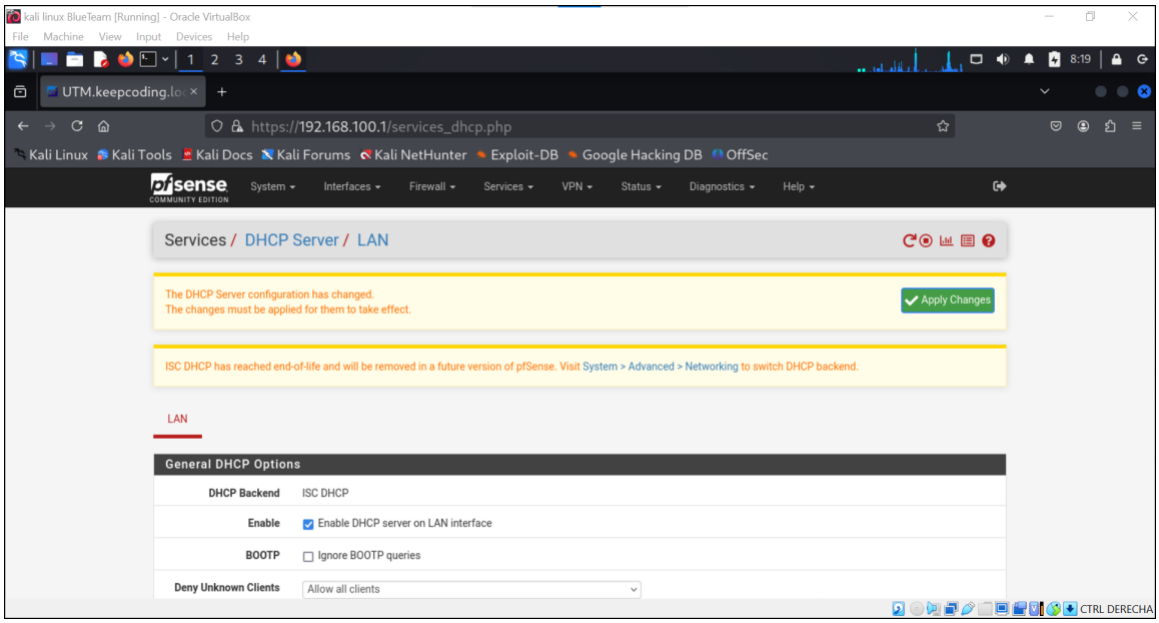





kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
UTM.keepcoding.lo
https://192.168.100.1/services_dhcp.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Additional Pools
Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.
Server Options
WINS Servers
WINS Server 1
WINS Server 2
DNS Servers
192.168.100.1
1.1.1.1
8.8.8.8
DNS Server 4
OMAPI
OMAPI Port
OMAPI Port
Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable.Only the first OMAPI configuration is used.
OMAPI Key
OMAPI Key
Generate New Key
CTRL DERECHA

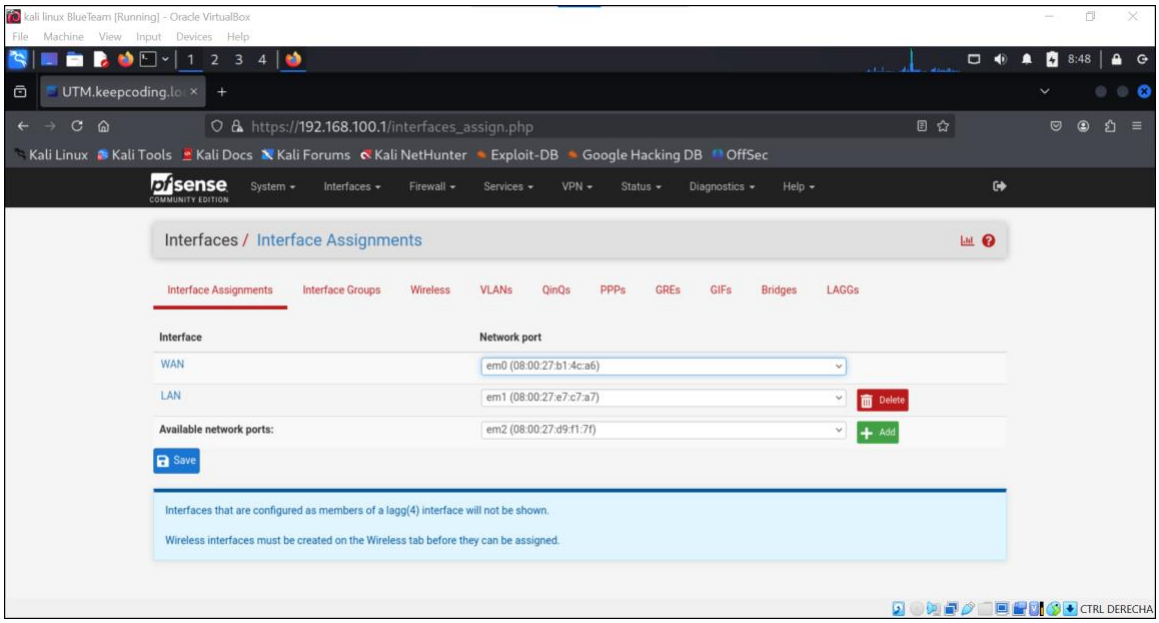

kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
UTM.keepcoding.lo
https://192.168.100.1/services_dhcp.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Other DHCP Options
Gateway
192.168.100.1
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.
Domain Name
keepcoding.local
The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain Search List
example.com;sub.example.com
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default Lease Time
7200
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum Lease Time
86400
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP
Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primary or Secondary. Ensure the advertising skew for the VIP on one firewall is < 20 and the other is > 20.
Static ARP
Enable Static ARP entries
Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will
CTRL DERECHA

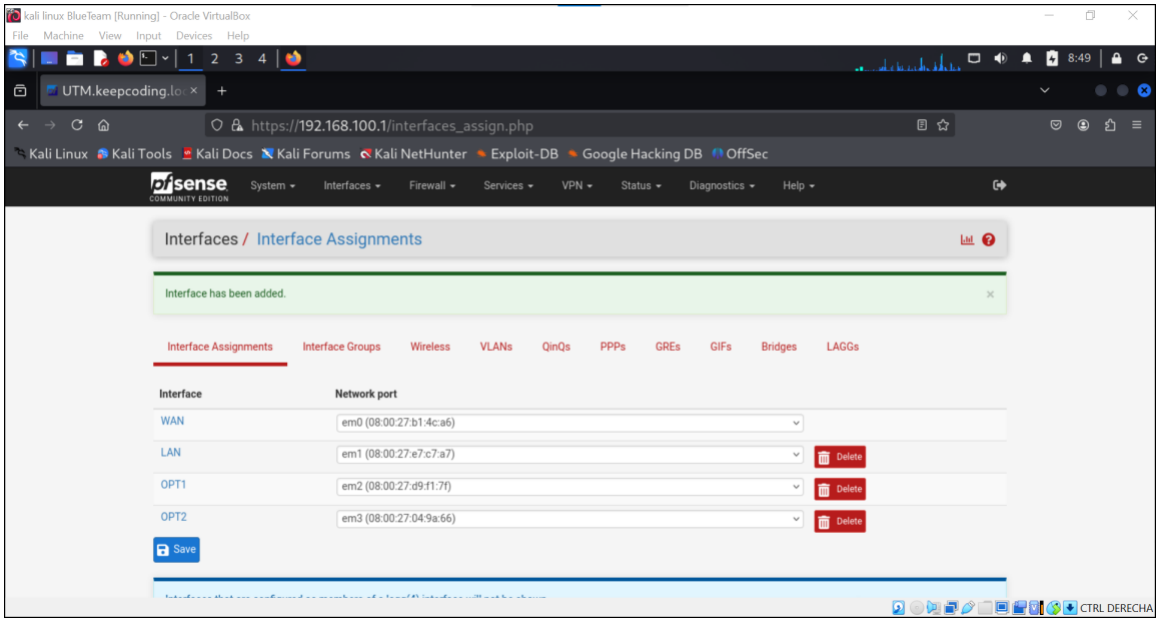


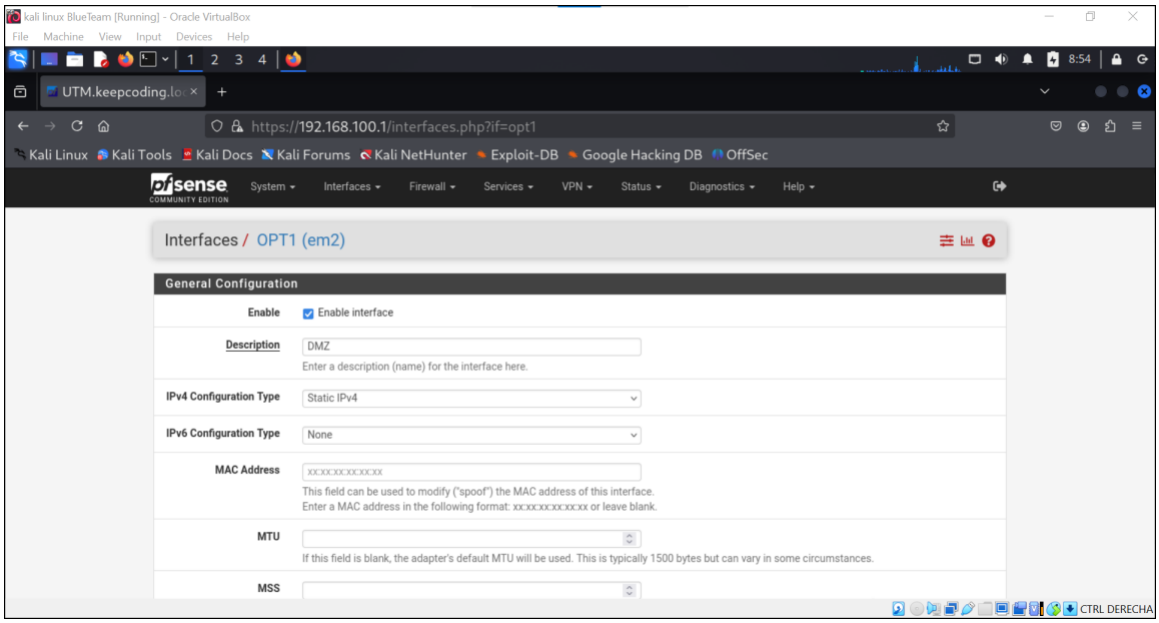


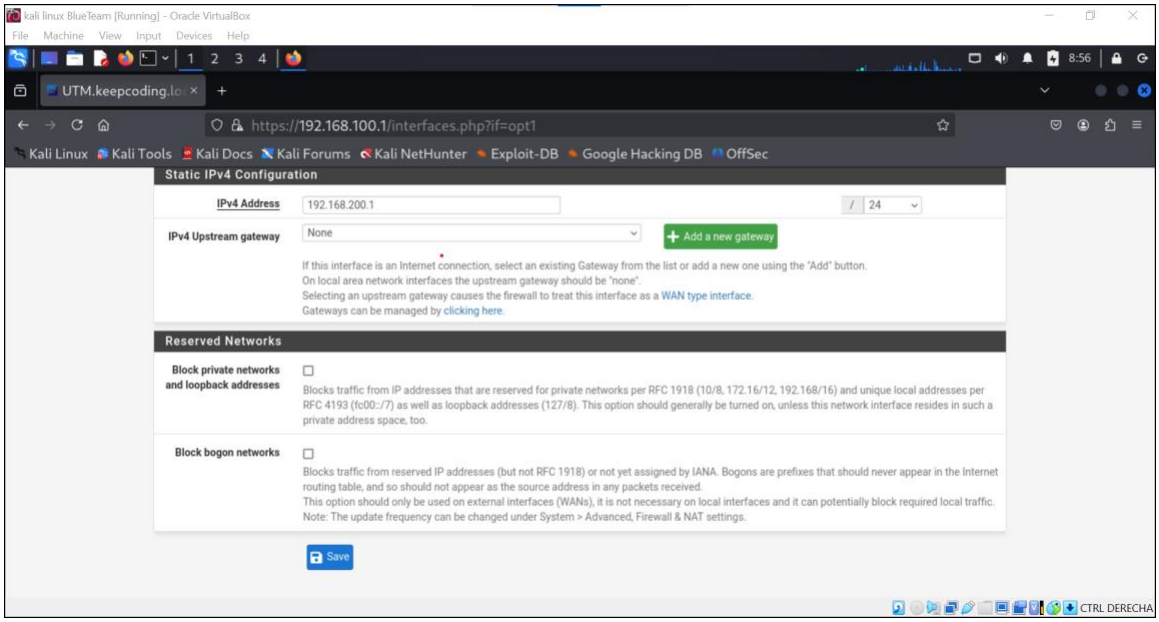
1.3.2. Añadir red DMZ

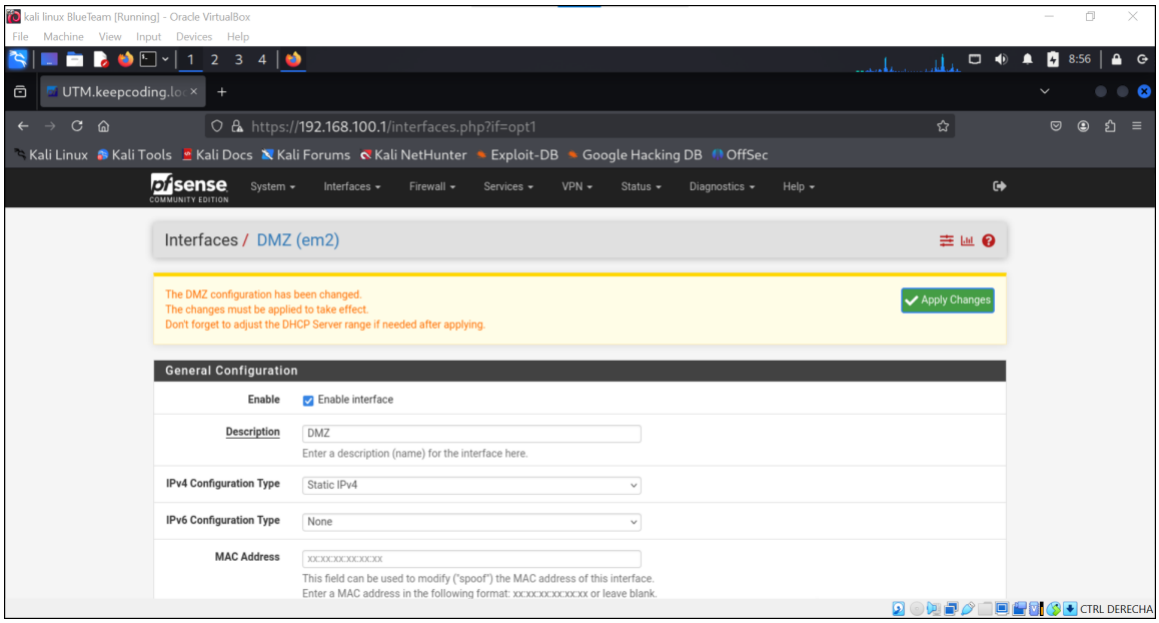
A la DMZ le vamos a aplicar una puerta de enlace estática.


kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
8:48
UTM.keepcoding.lo
https://192.168.100.1/interfaces_assign.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Interfaces / Interface Assignments
Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs
Interface
Network port
WAN
em0 (08:00:27:b1:4c:a6)
LAN
em1 (08:00:27:e7:c7:a7)
Delete
Available network ports:
em2 (08:00:27:d9:f1:7f)
Add
Save
Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.
CTRL DERECHA


kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
8:49
UTM.keepcoding.lo
https://192.168.100.1/interfaces_assign.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Interfaces / Interface Assignments
Interface has been added.
Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs
Interface
Network port
WAN
em0 (08:00:27:b1:4c:a6)
LAN
em1 (08:00:27:e7:c7:a7)
Delete
OPT1
em2 (08:00:27:d9:f1:7f)
Delete
OPT2
em3 (08:00:27:04:9a:66)
Delete
Save
CTRL DERECHA

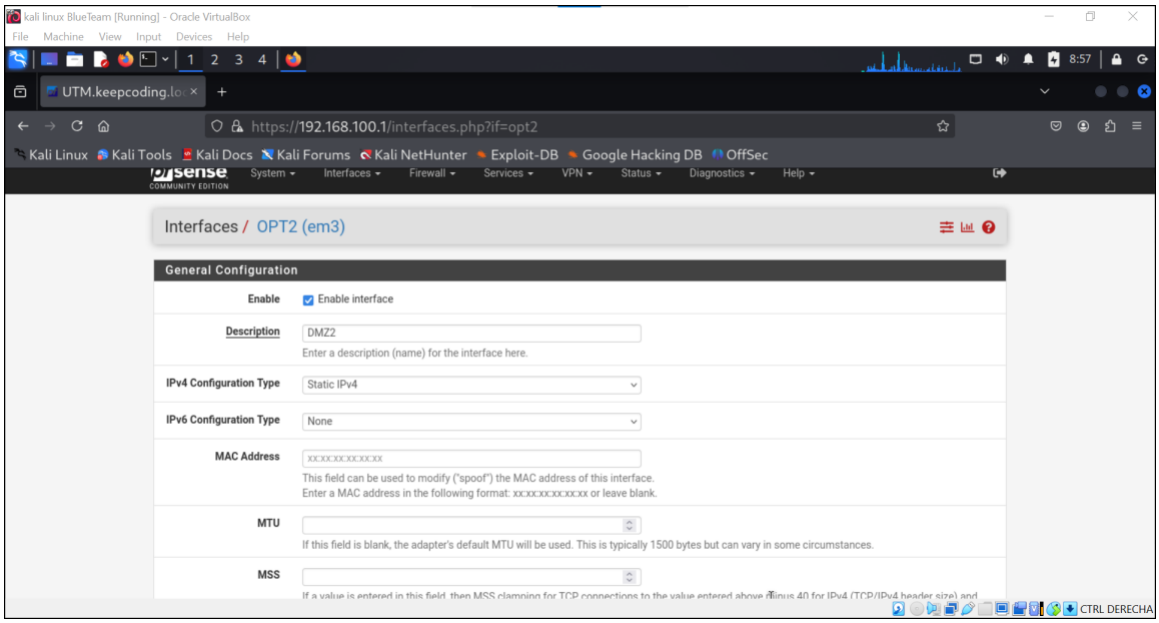

kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
8:54
UTM.keepcoding.lo
https://192.168.100.1/interfaces.php?if=opt1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Interfaces / OPT1 (em2)
General Configuration
Enable
Enable interface
Description
DMZ
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xxxxxxxxxxxx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
CTRL DERECHA

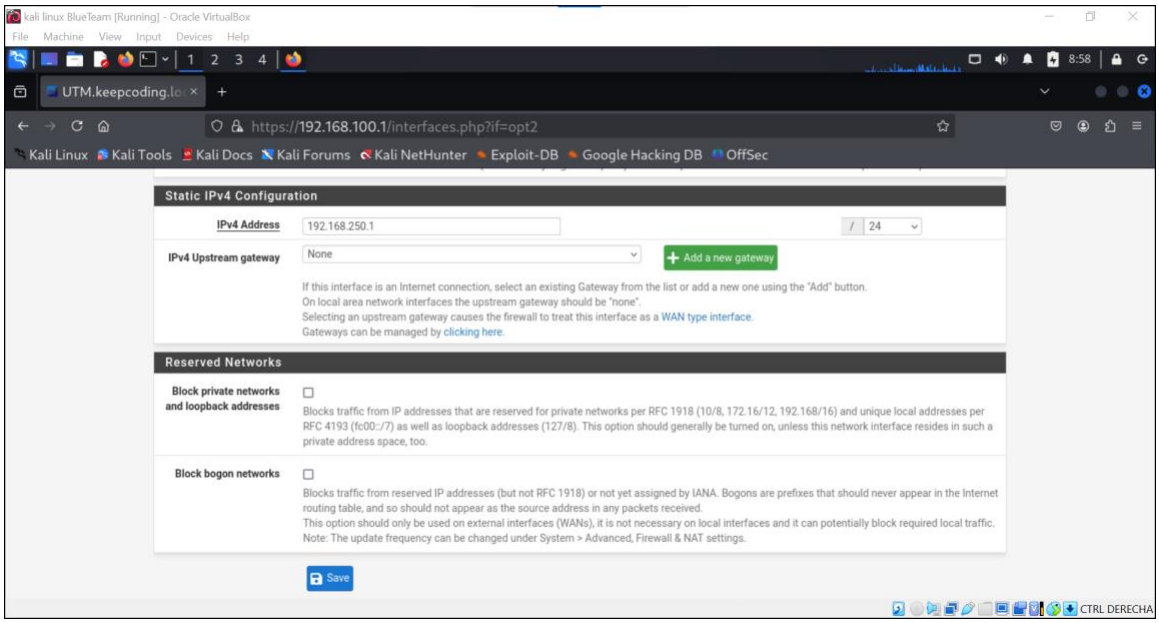

kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
8:56
UTM.keepcoding.lo
https://192.168.100.1/interfaces.php?if=opt1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Static IPv4 Configuration
IPv4 Address
192.168.200.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.
Reserved Networks
Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.
Save
CTRL DERECHA

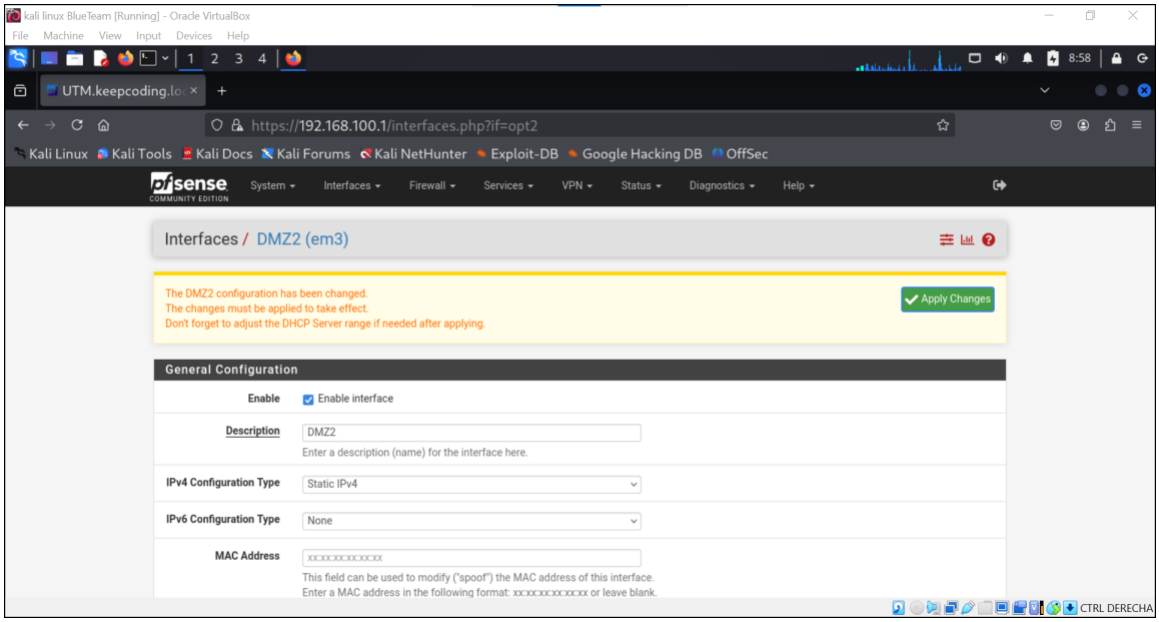


1.3.3 Añadir red DMZ2

A la DMZ2 le vamos a aplicar una puerta de enlace estática.

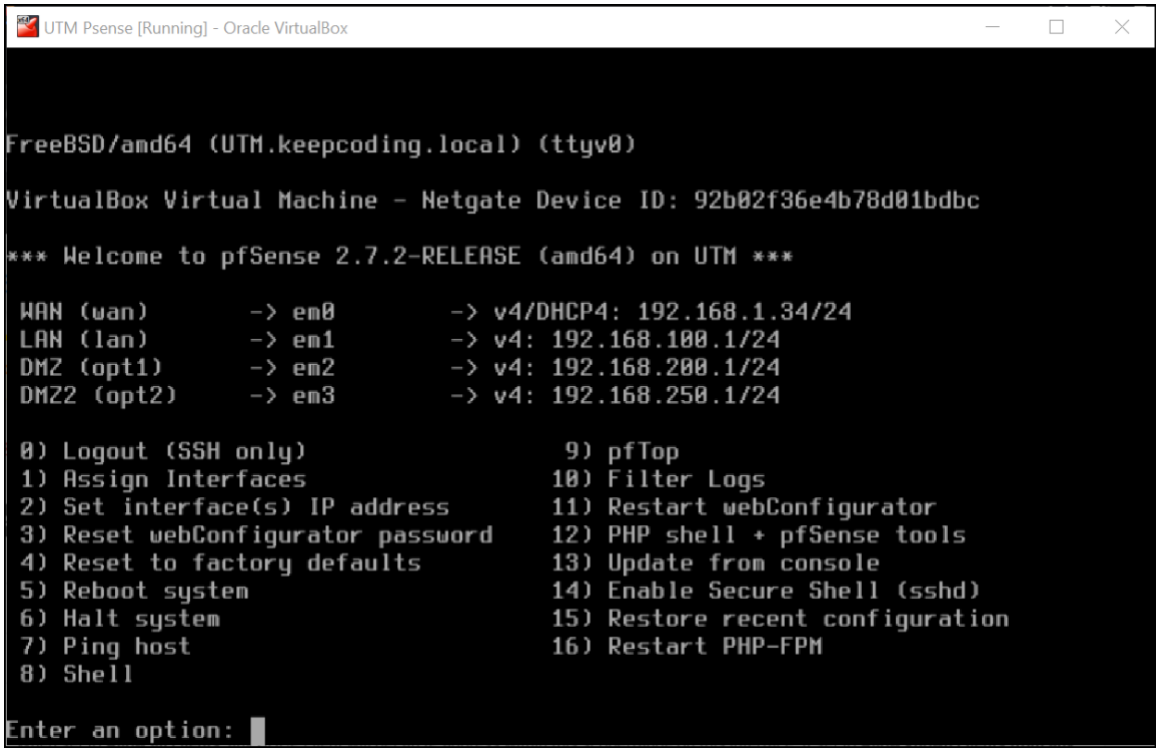




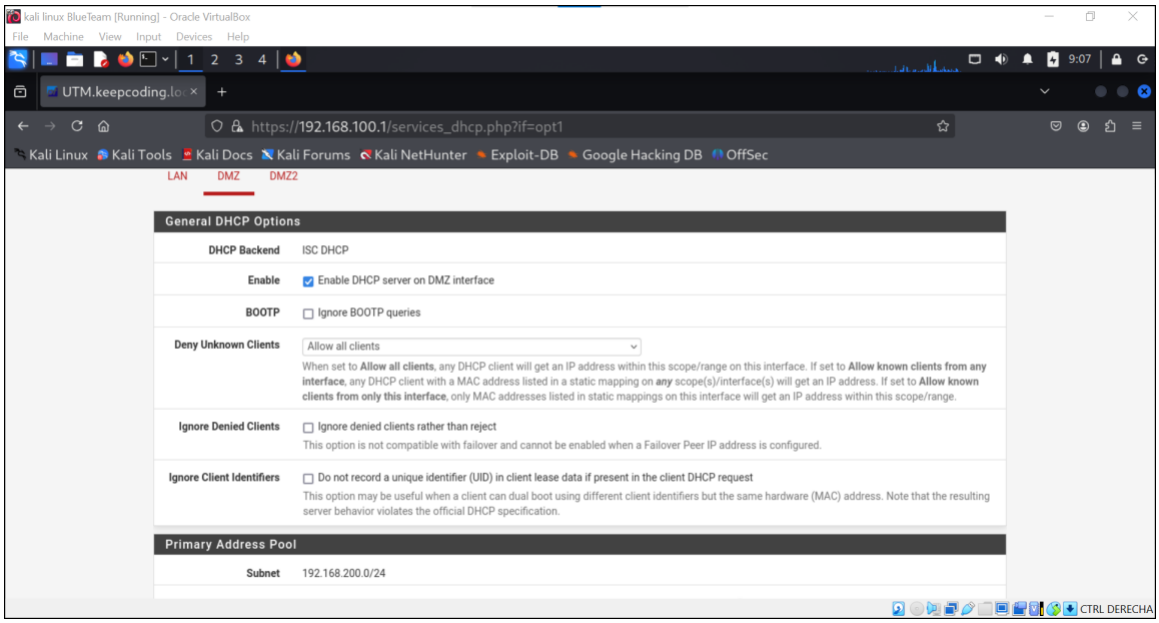


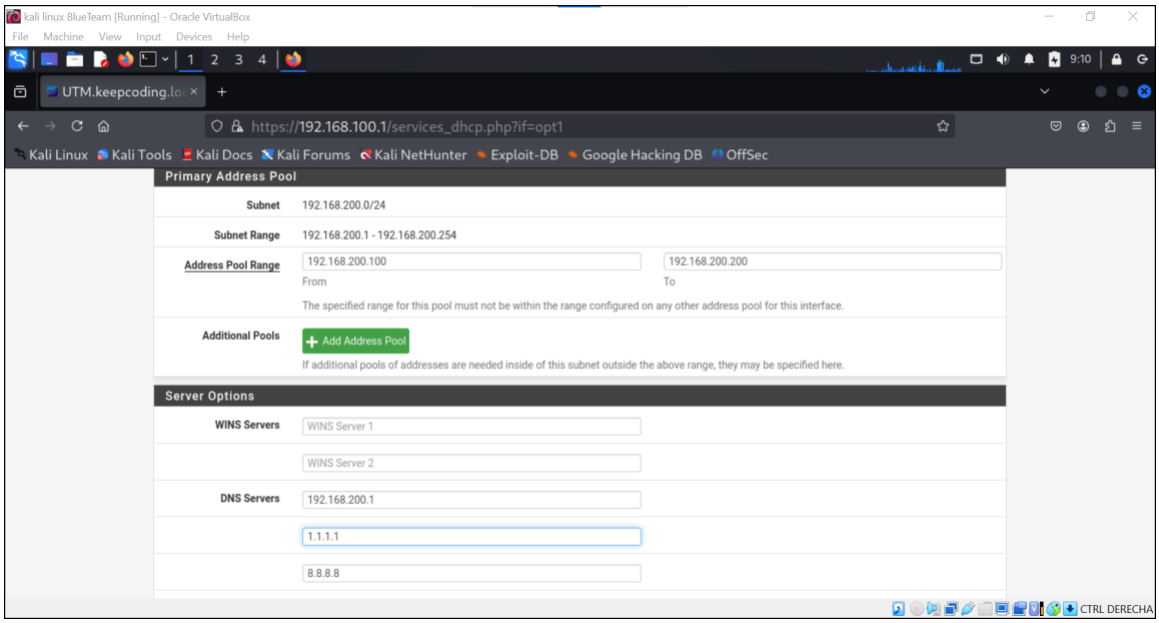
1.3.4 Comprobar redes añadidas

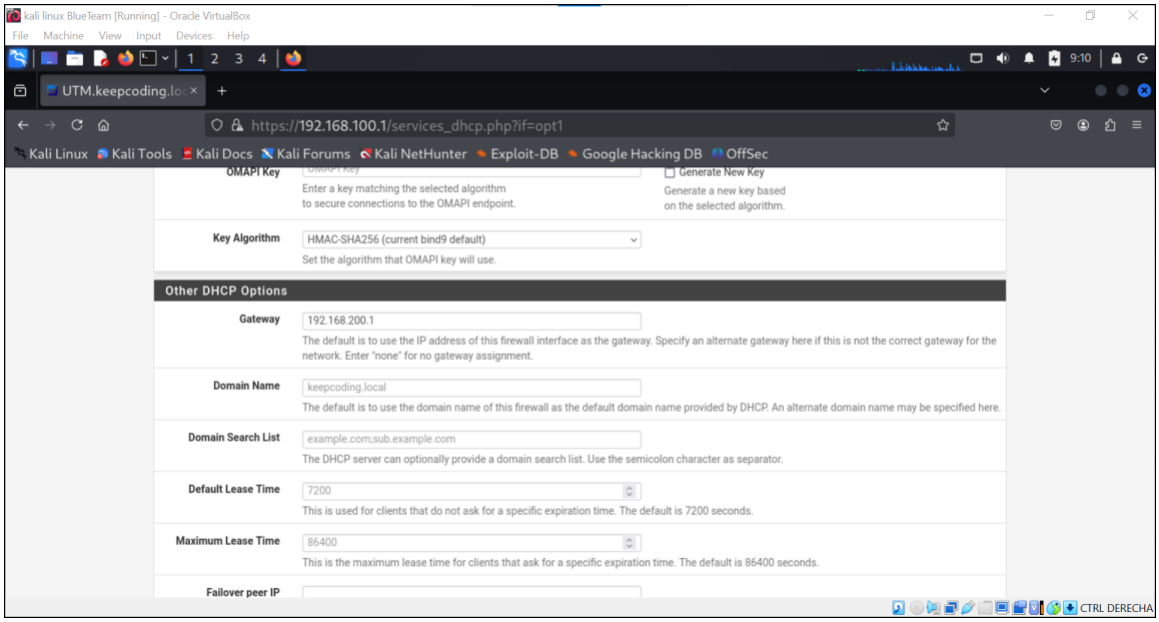
Lo que vamos a comprobar en Pfsense es si las redes se han añadido correctamente.

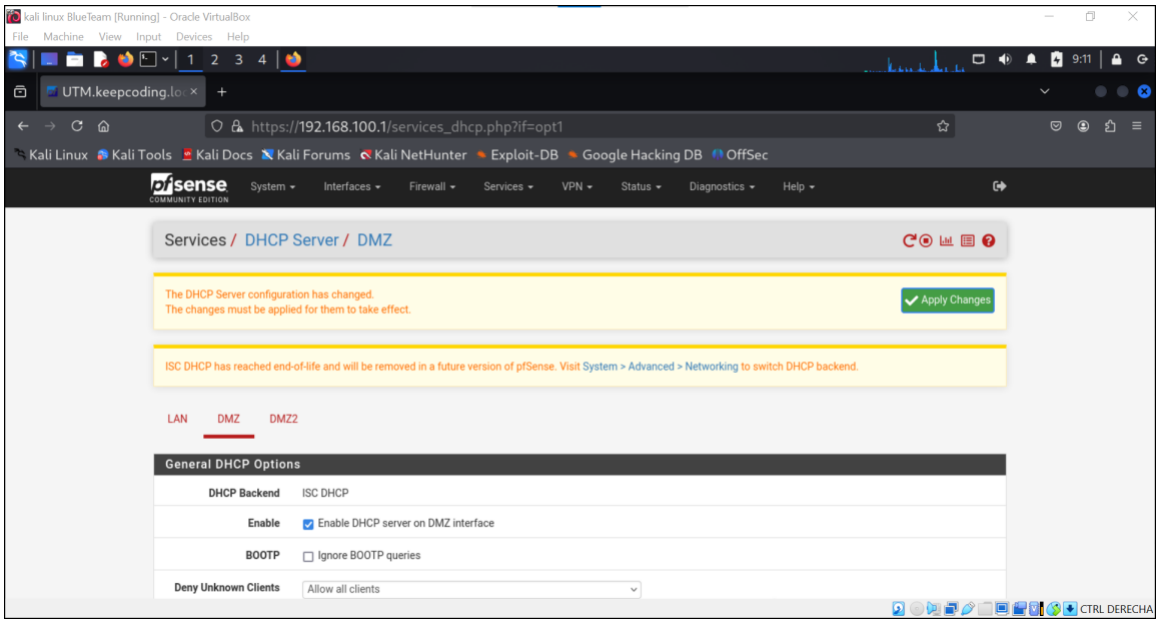


1.3.5 Rango DMZ

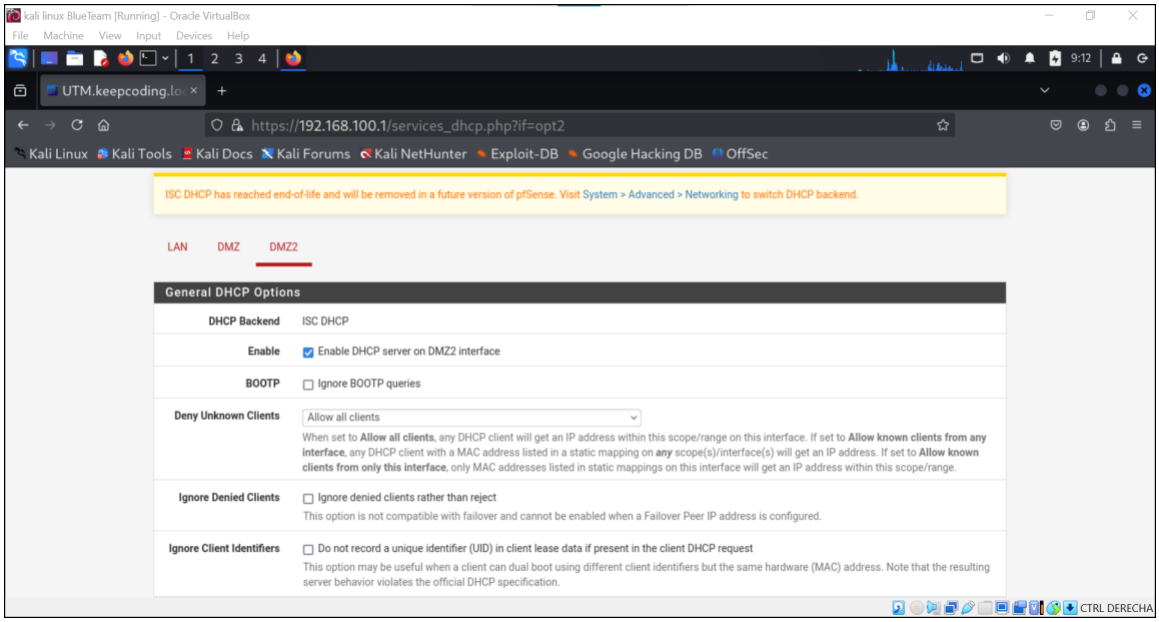


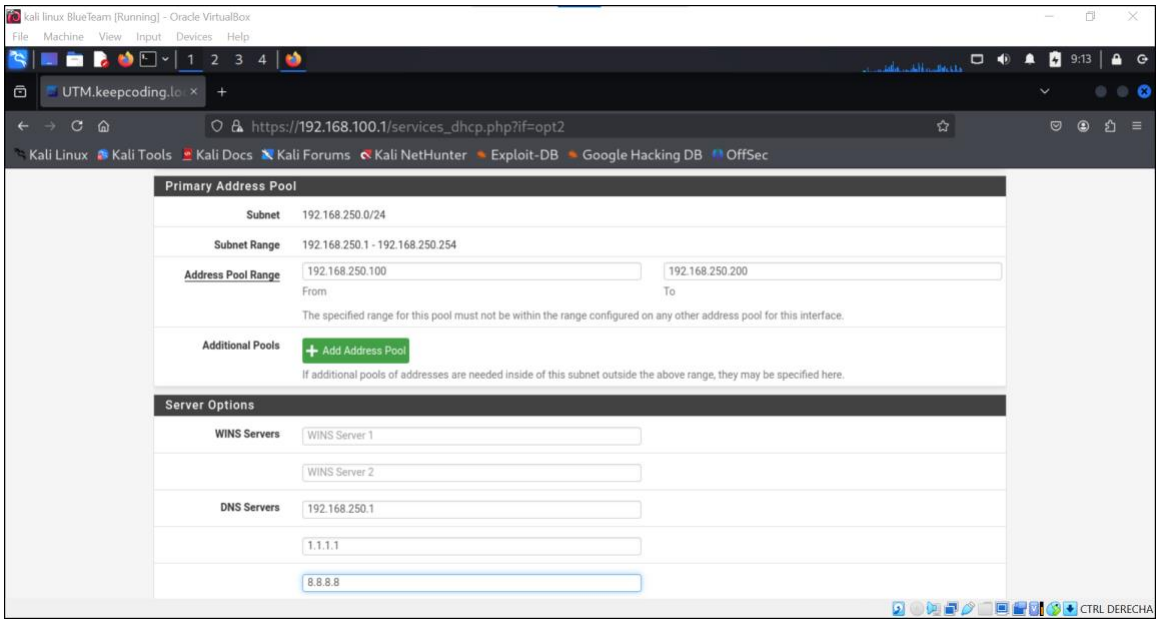

kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
UTM.keepcoding.lo
https://192.168.100.1/services_dhcp.php?if=opt1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Primary Address Pool
Subnet
192.168.200.0/24
Subnet Range
192.168.200.1 - 192.168.200.254
Address Pool Range
192.168.200.100
From
192.168.200.200
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.
Server Options
WINS Servers
WINS Server 1
WINS Server 2
DNS Servers
192.168.200.1
1.1.1.1
8.8.8.8
CTRL DERECHA

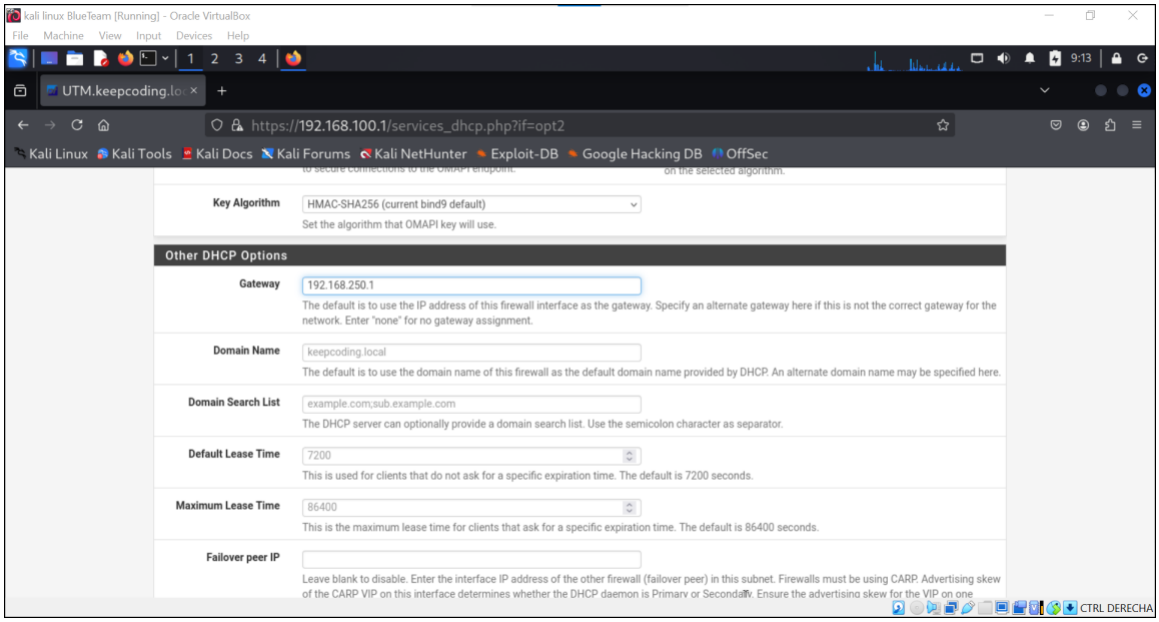

kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
UTM.keepcoding.lo
https://192.168.100.1/services_dhcp.php?if=opt1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OMAPI Key
Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.
Generate New Key
Generate a new key based on the selected algorithm.
Key Algorithm
HMAC-SHA256 (current bind9 default)
Set the algorithm that OMAPI key will use.
Other DHCP Options
Gateway
192.168.200.1
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.
Domain Name
keepcoding.local
The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain Search List
example.com;sub.example.com
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default Lease Time
7200
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum Lease Time
86400
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP
CTRL DERECHA

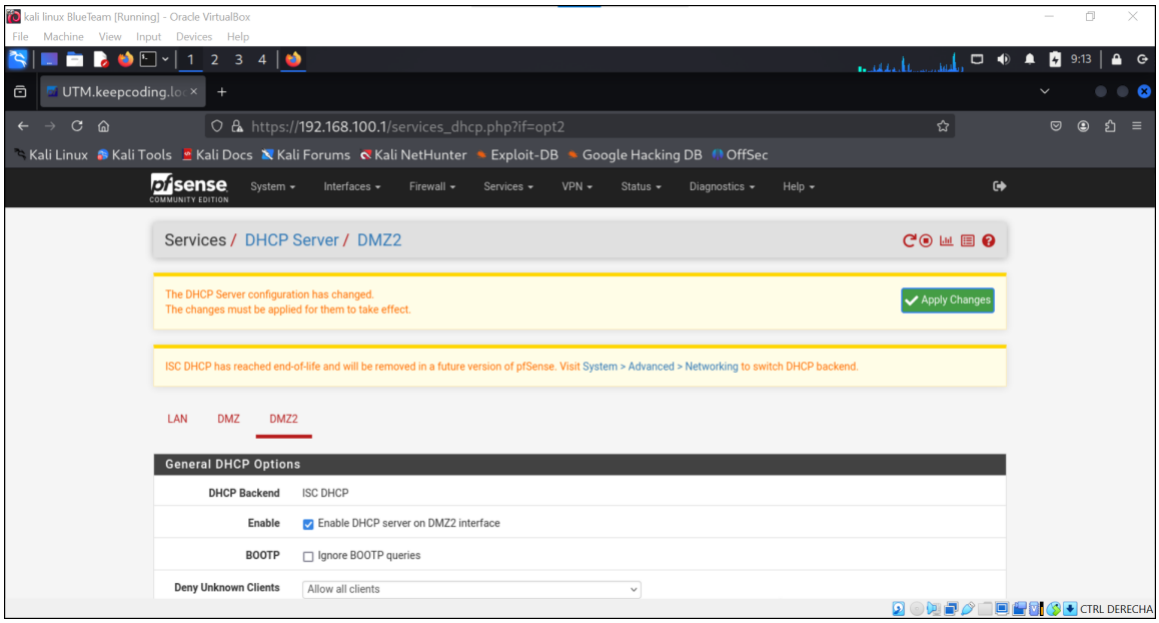


1.3.6 Rango DMZ2




kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
UTM.keepcoding.lo
https://192.168.100.1/services_dhcp.php?if=opt2
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Primary Address Pool
Subnet
192.168.250.0/24
Subnet Range
192.168.250.1 - 192.168.250.254
Address Pool Range
192.168.250.100
From
192.168.250.200
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.
Server Options
WINS Servers
WINS Server 1
WINS Server 2
DNS Servers
192.168.250.1
1.1.1.1
8.8.8.8
CTRL DERECHA


kali linux BlueTeam [Running] - Oracle VirtualBox
File Machine View Input Devices Help
UTM.keepcoding.lo
https://192.168.100.1/services_dhcp.php?if=opt2
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Key Algorithm
HMAC-SHA256 (current bind9 default)
Set the algorithm that OMAPI key will use.
Other DHCP Options
Gateway
192.168.250.1
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.
Domain Name
keepcoding.local
The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain Search List
example.com;sub.example.com
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default Lease Time
7200
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum Lease Time
86400
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP
Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primary or Secondary. Ensure the advertising skew for the VIP on one
CTRL DERECHA



1.4. Firewall

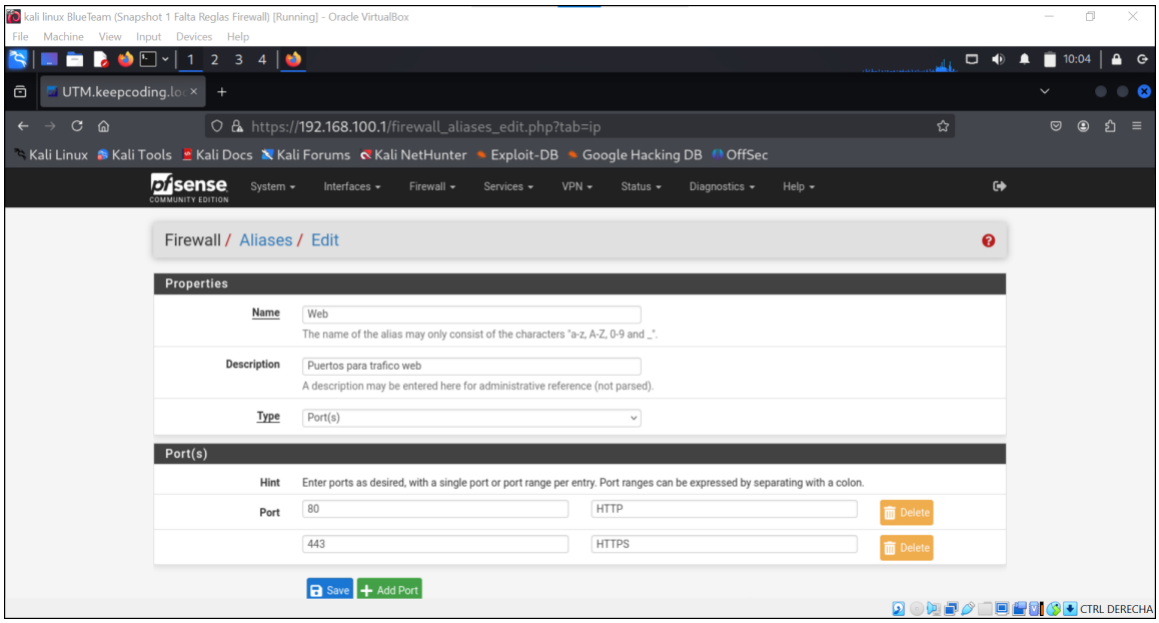
En esta sección se detallan las reglas principales implementadas en el firewall, junto con la validación del correcto funcionamiento del servicio DNS y la definición de políticas específicas para la gestión de las comunicaciones entre las diferentes redes configuradas.

Se establece que la red DMZ estará completamente aislada de las redes internas LAN y DMZ2, sin posibilidad de comunicación en ningún sentido. No obstante, se permitirá acceso bidireccional entre la red DMZ y la red externa WAN, cumpliendo con los requisitos de segmentación y control. Asimismo, se asigna esta red al Honeypot, como parte de la estrategia de detección y análisis de posibles amenazas externas.

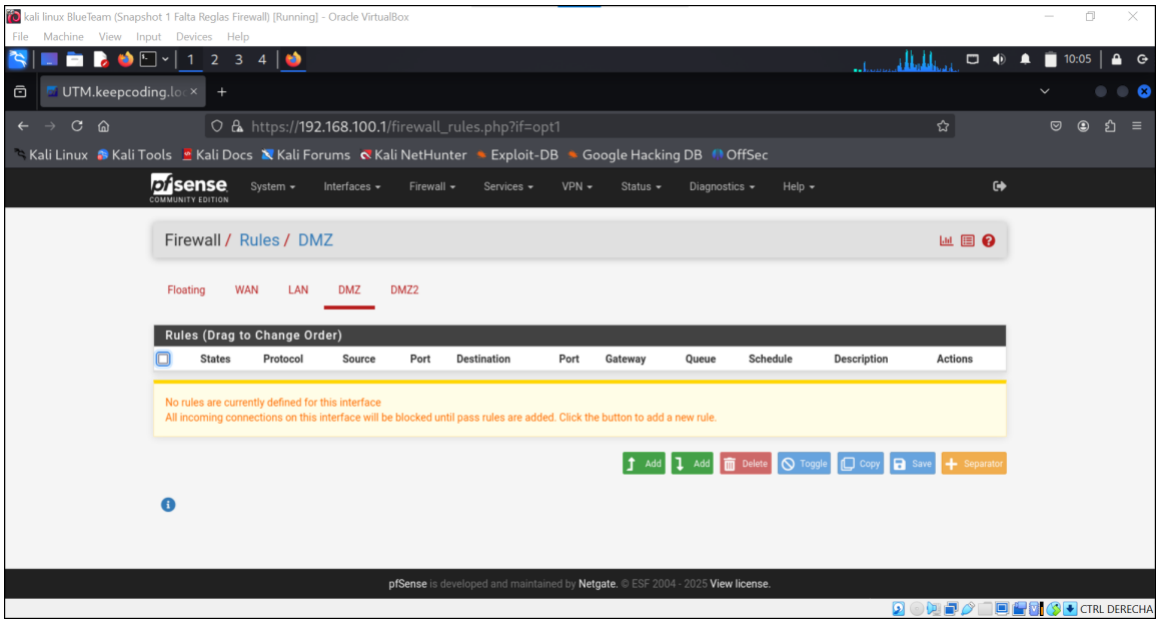
Esta configuración refuerza los principios de seguridad perimetral y minimiza los riesgos asociados a accesos no autorizados desde redes externas hacia la infraestructura interna.

1.4.1 Alias a puertos

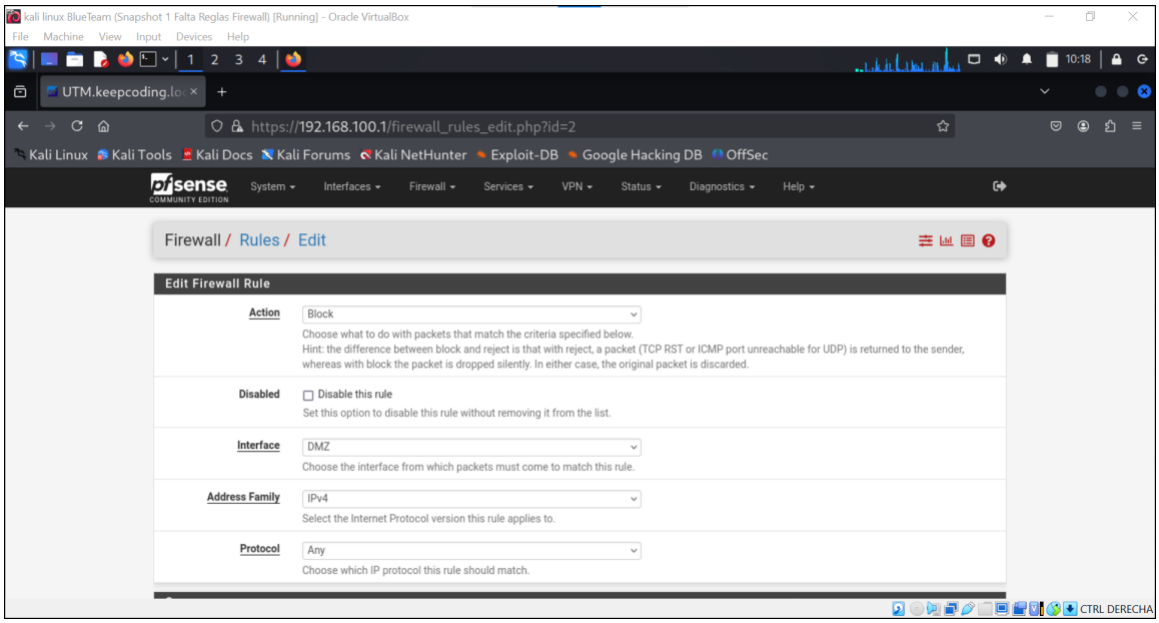
Vamos a otorgar el alias "Web" a los puertos 80 (HTTP) y 443 (HTTPS), ya que ambos están comúnmente asociados a la transmisión de datos a través de páginas web. El puerto 80 (HTTP) se utiliza para establecer conexiones no cifradas, lo que significa que los datos transmitidos entre el cliente y el servidor pueden ser interceptados y leídos fácilmente por terceros. Por otro lado, el puerto 443 (HTTPS) opera con un nivel de seguridad superior, ya que emplea protocolos de cifrado como TLS (Transport Layer Security), lo que garantiza la confidencialidad e integridad de los datos transmitidos.

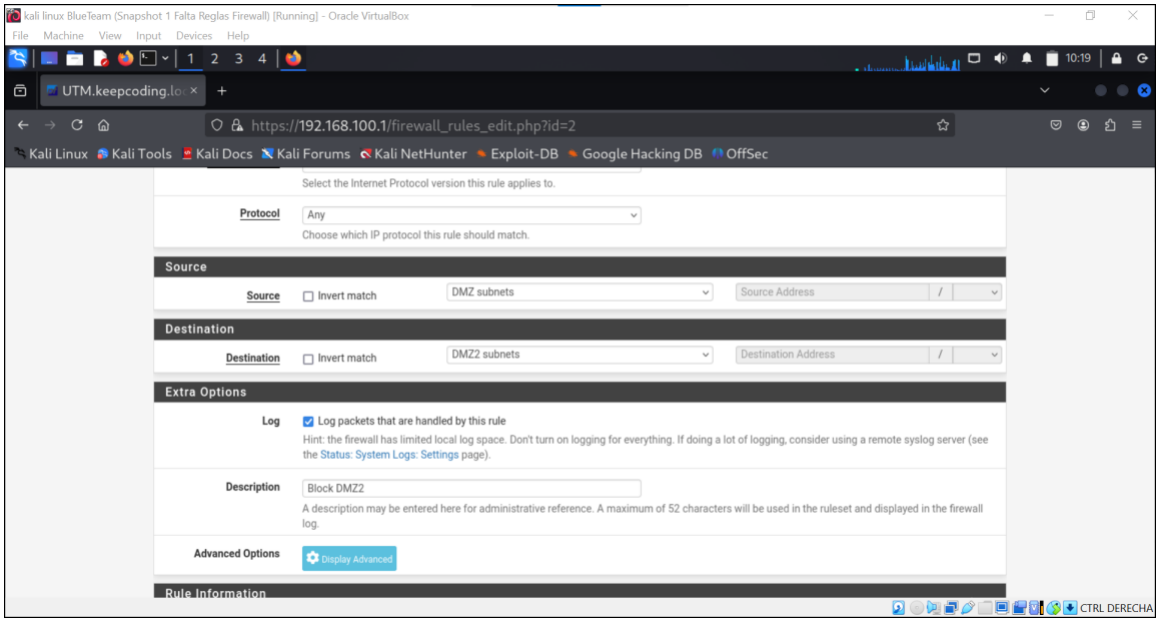


1.4.2. Reglas Firewall DMZ

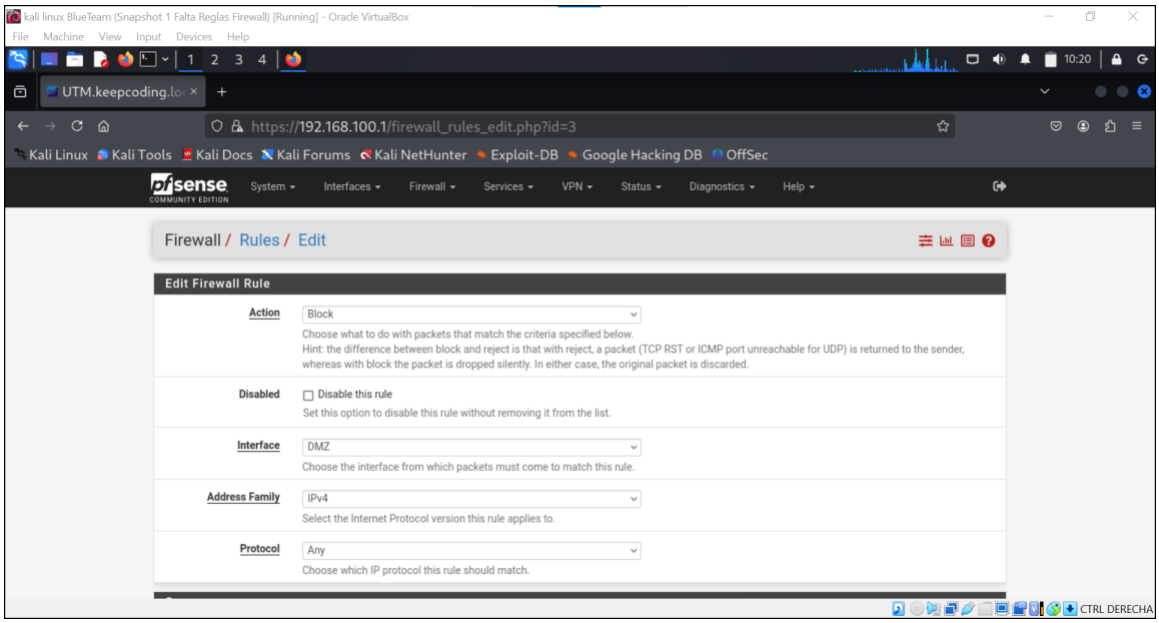


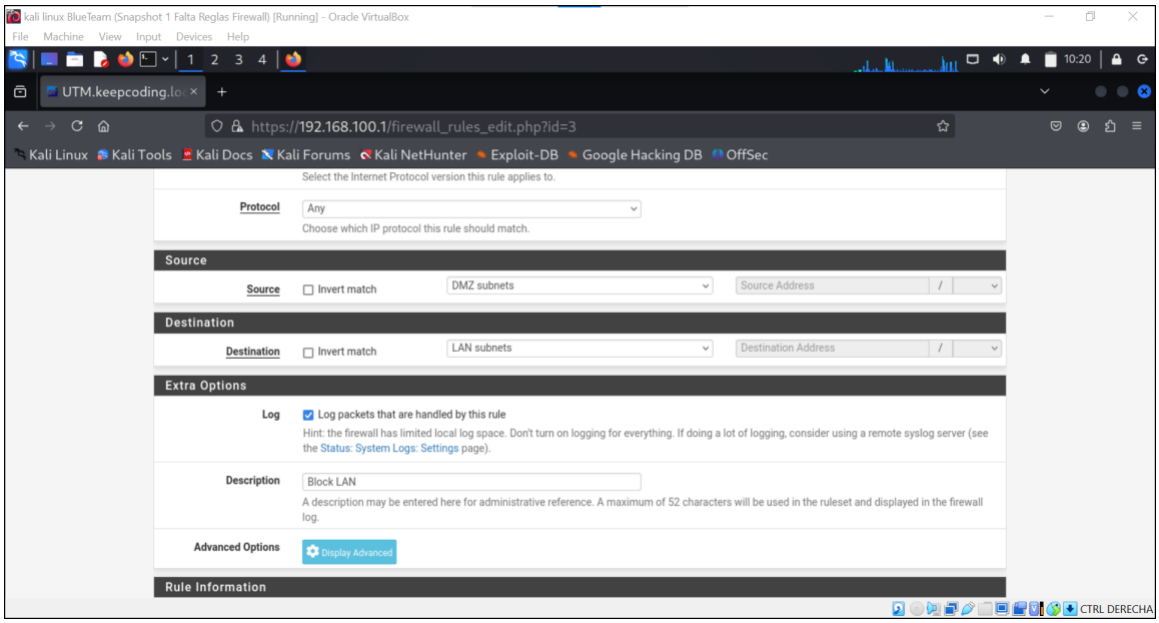
Primero vamos a bloquear la comunicación entre DMZ y DMZ2.



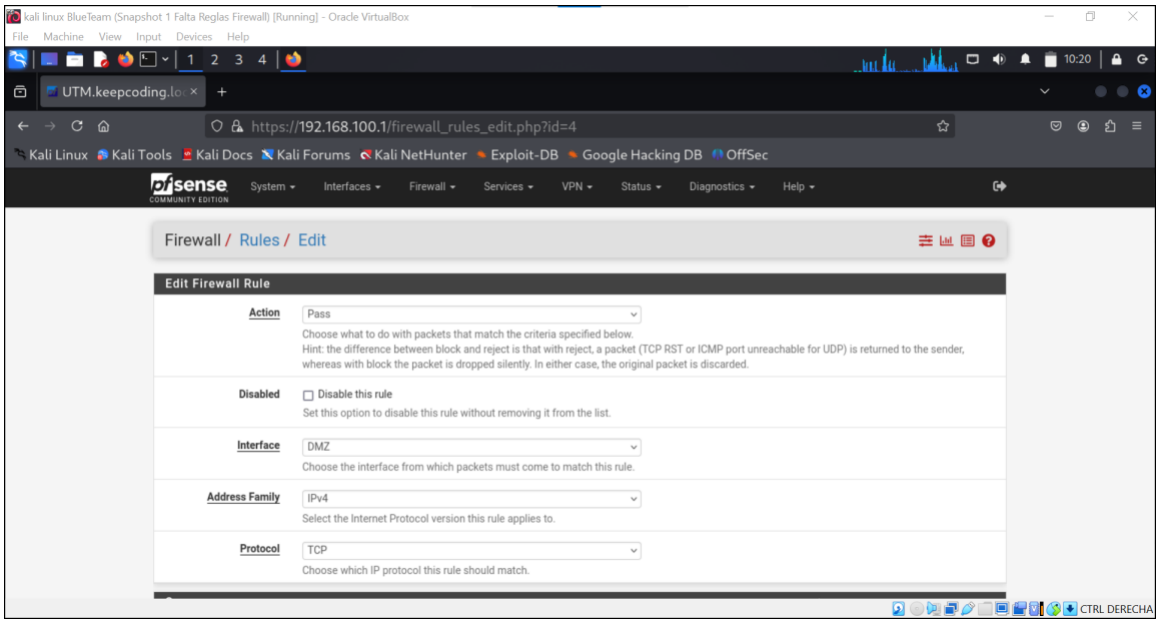


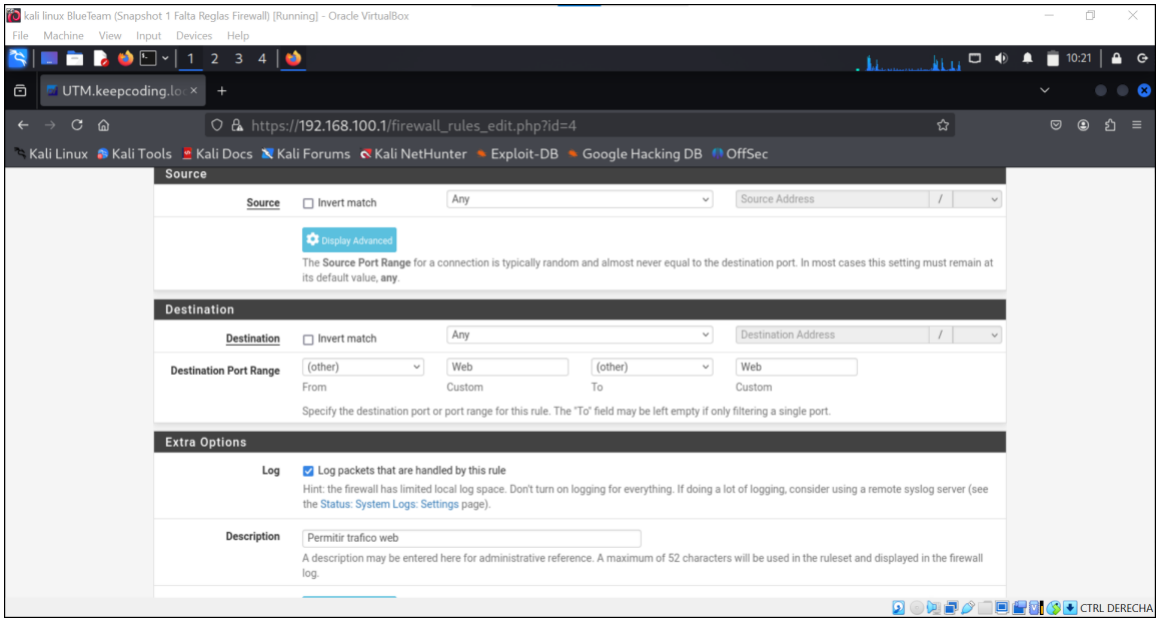
A continuación, bloquearemos también la comunicación entre la red DMZ y LAN.



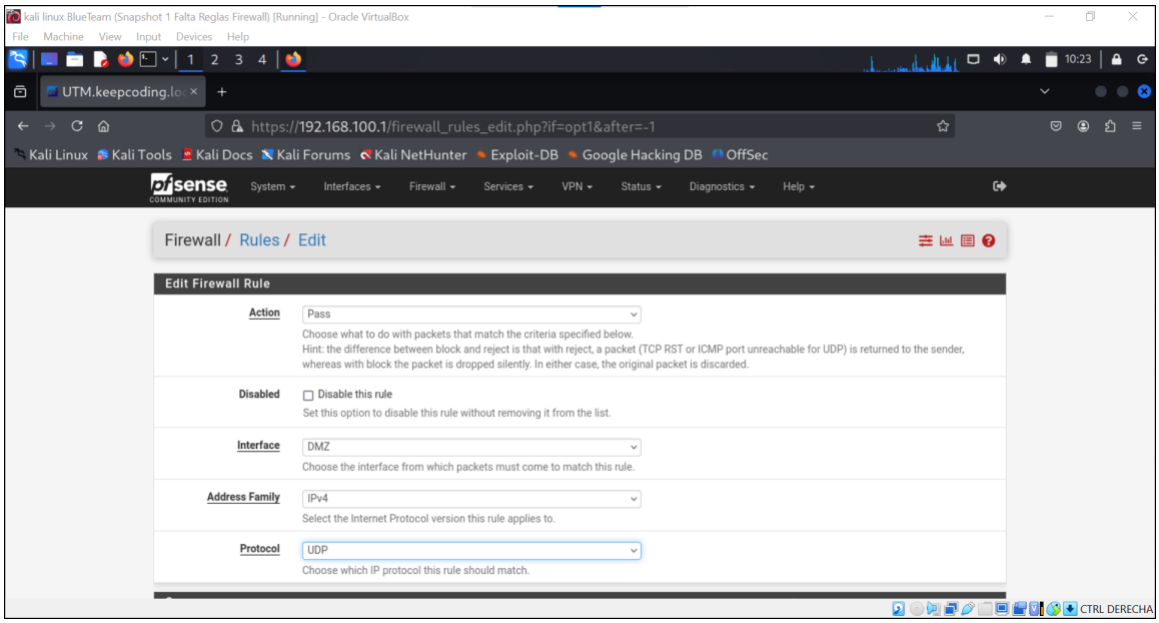


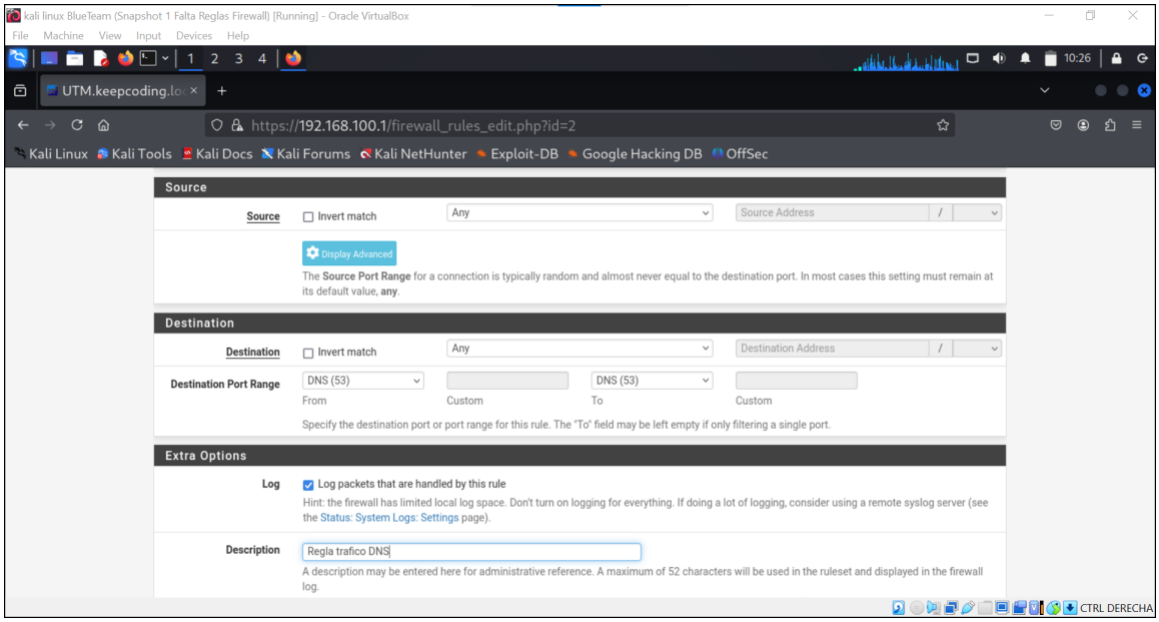
Después, vamos a permitir el tráfico web a la red de DMZ. Para ello se ha utilizado el protocolo UTP, que garantiza la importación de los paquetes enteros. Es el típico que se utiliza para conexiones HTTPS.



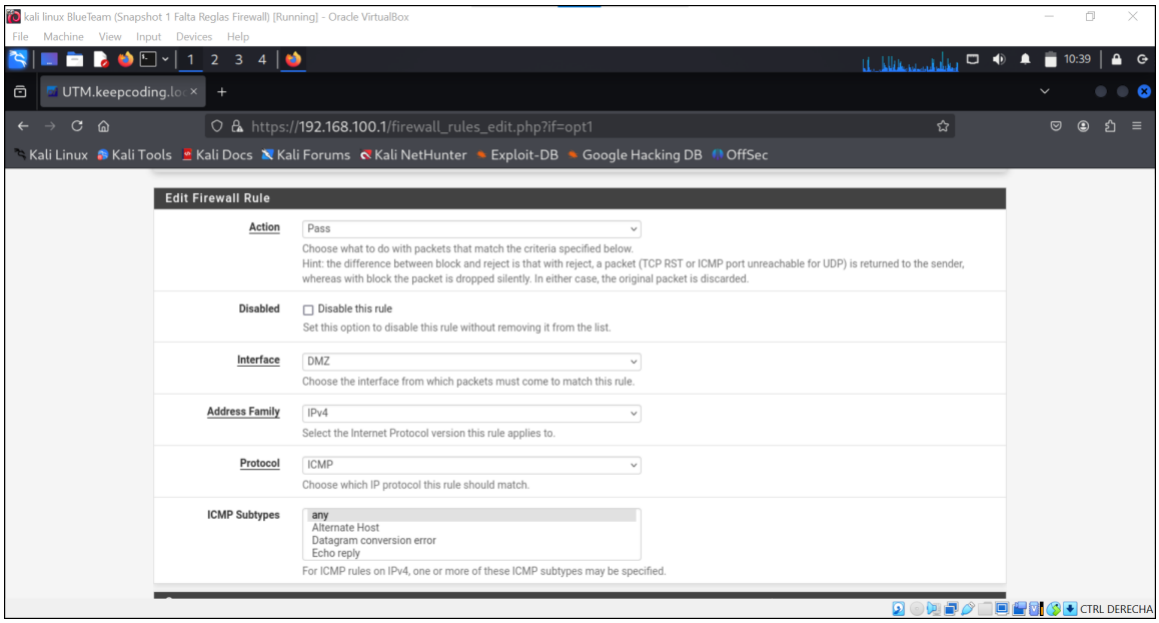


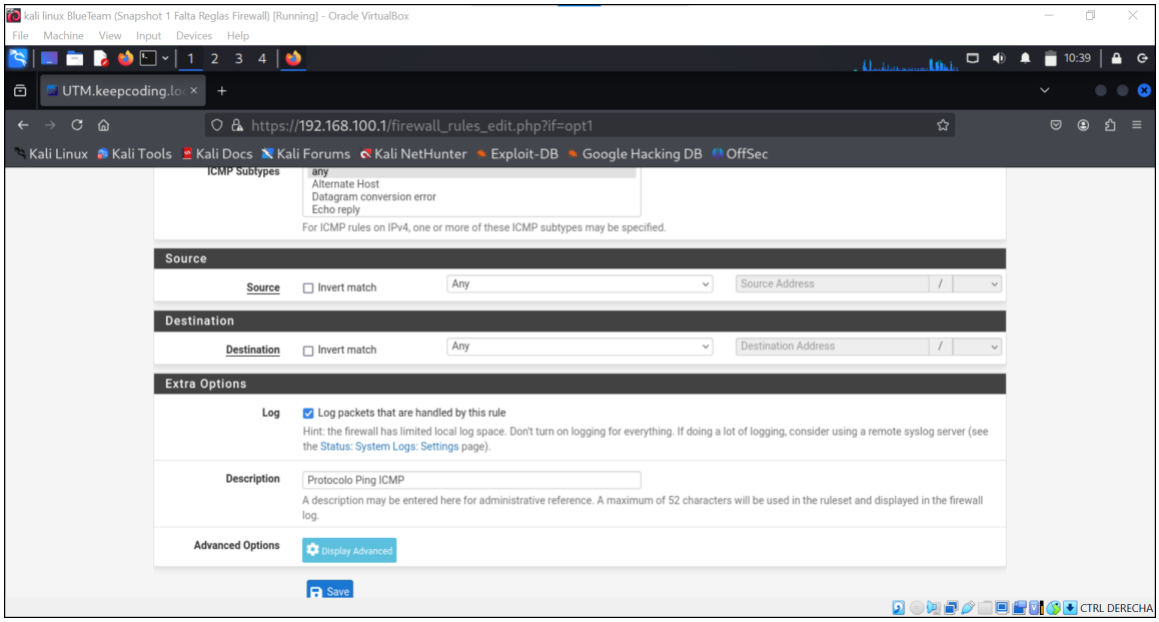
Ahora vamos a habilitar las reglas de DNS en la red de DMZ. Para ello se va a utilizar el protocolo UDP, que no garantiza importar los paquetes completos en diferencia al protocolo UTP.



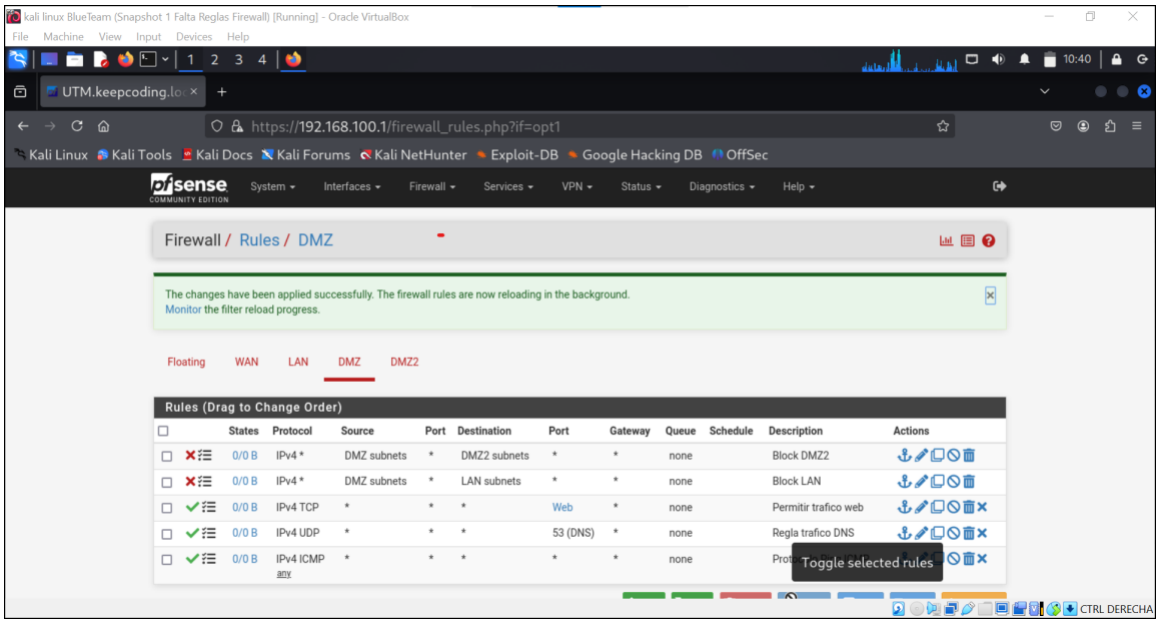


Ahora vamos a habilitar el ping utilizando el protocolo ICMP, que es un protocolo de red perteneciente a la familia de protocolos TCP/IP que se utiliza para enviar mensajes de diagnóstico y control en las comunicaciones entre dispositivos de una red. Su principal objetivo es reportar errores, proporcionar información sobre problemas de conectividad y verificar el estado de la red.





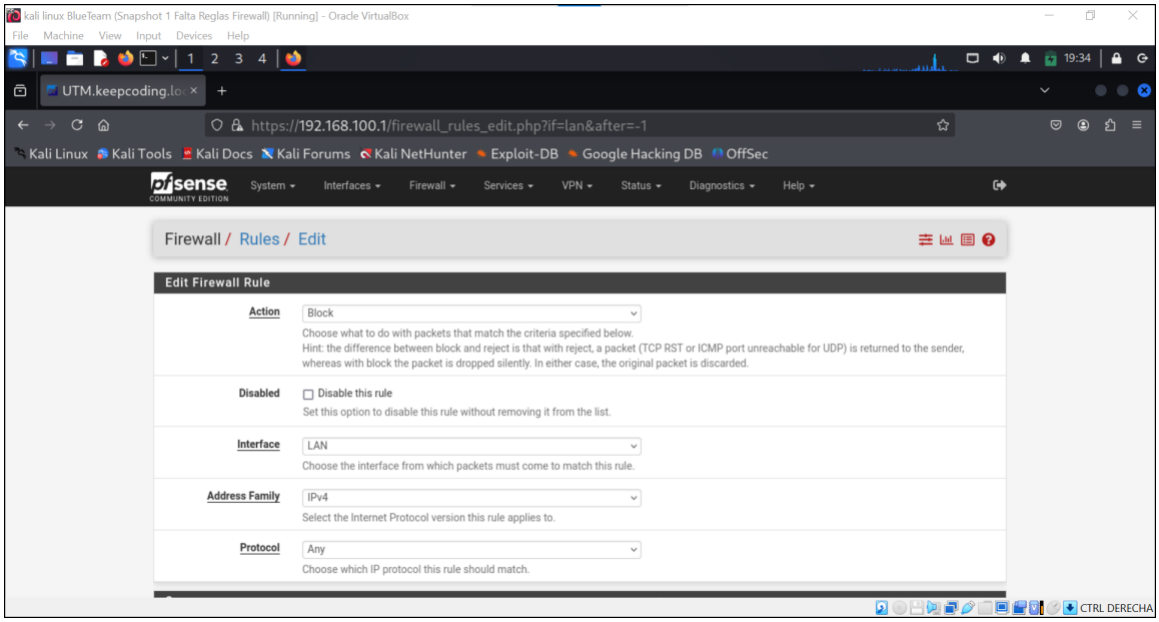
Y aquí tenemos todas las reglas de firewall que hemos asignado a DMZ.

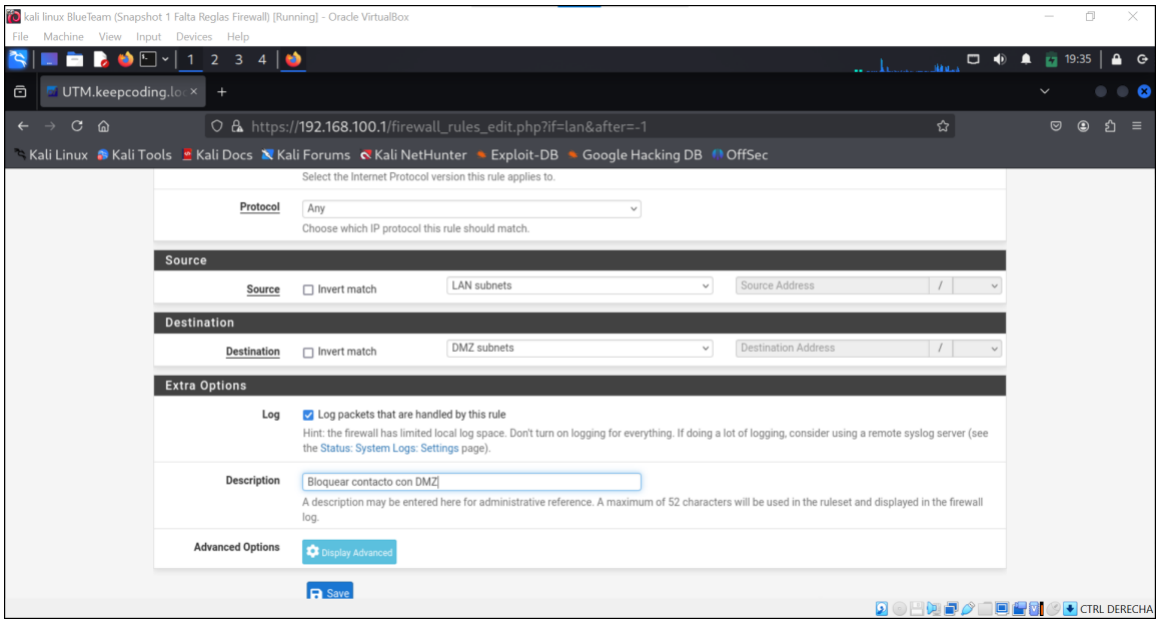


1.4.3. Reglas Firewall LAN

Aquí solo vamos a añadir solamente una regla, porque las demás ya estaban creadas automáticamente.

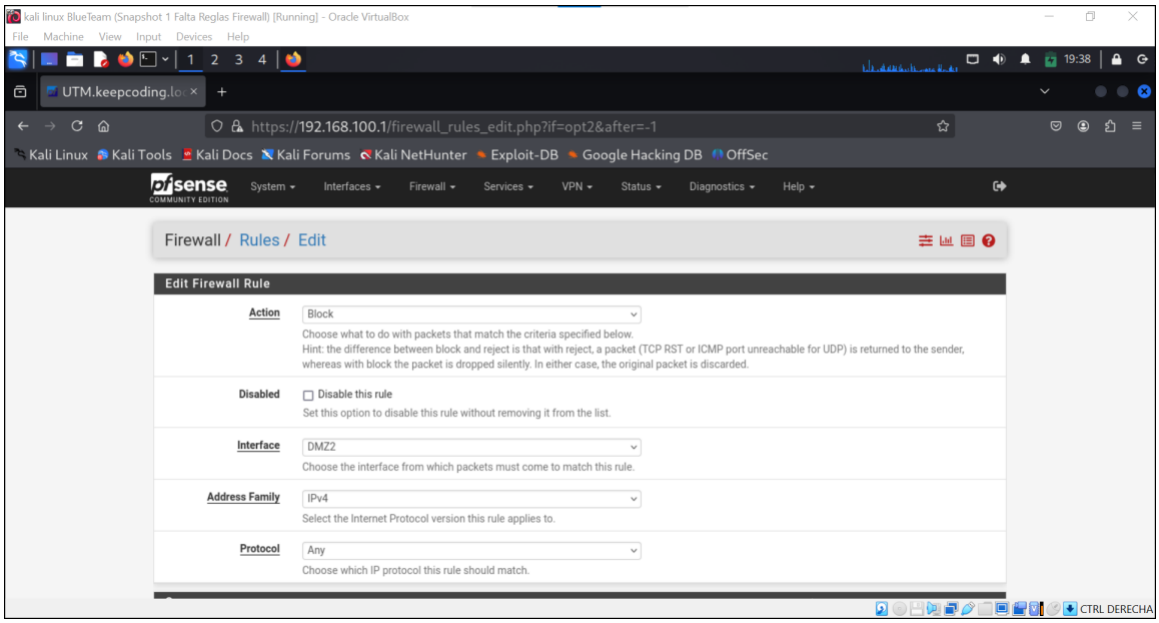
Vamos a bloquear la conexión con la red DMZ.

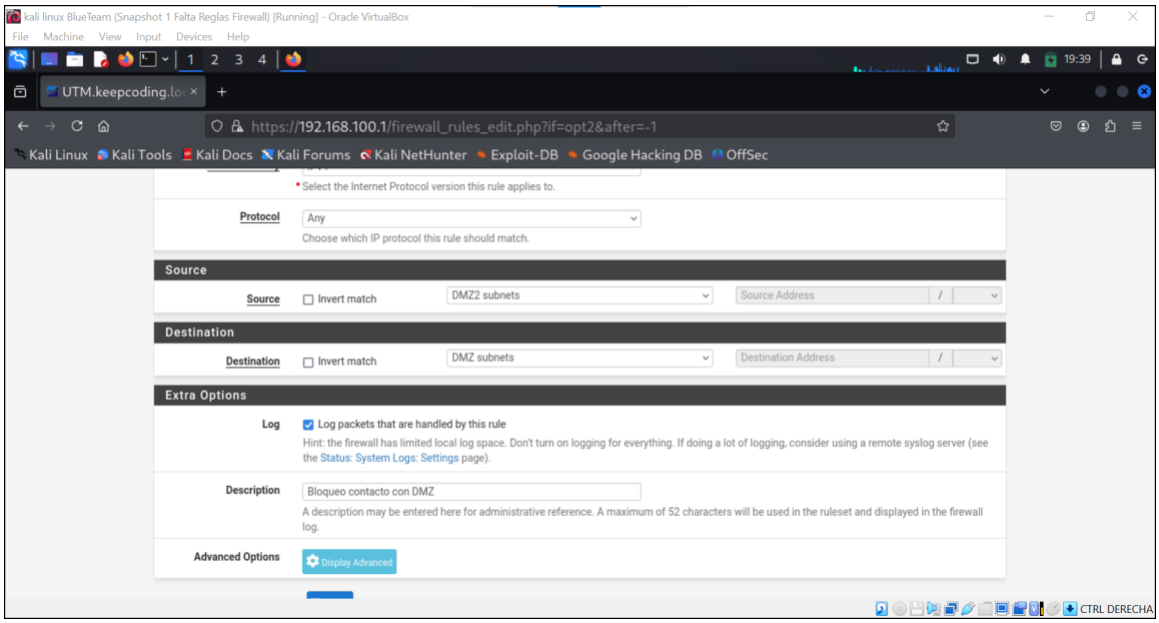




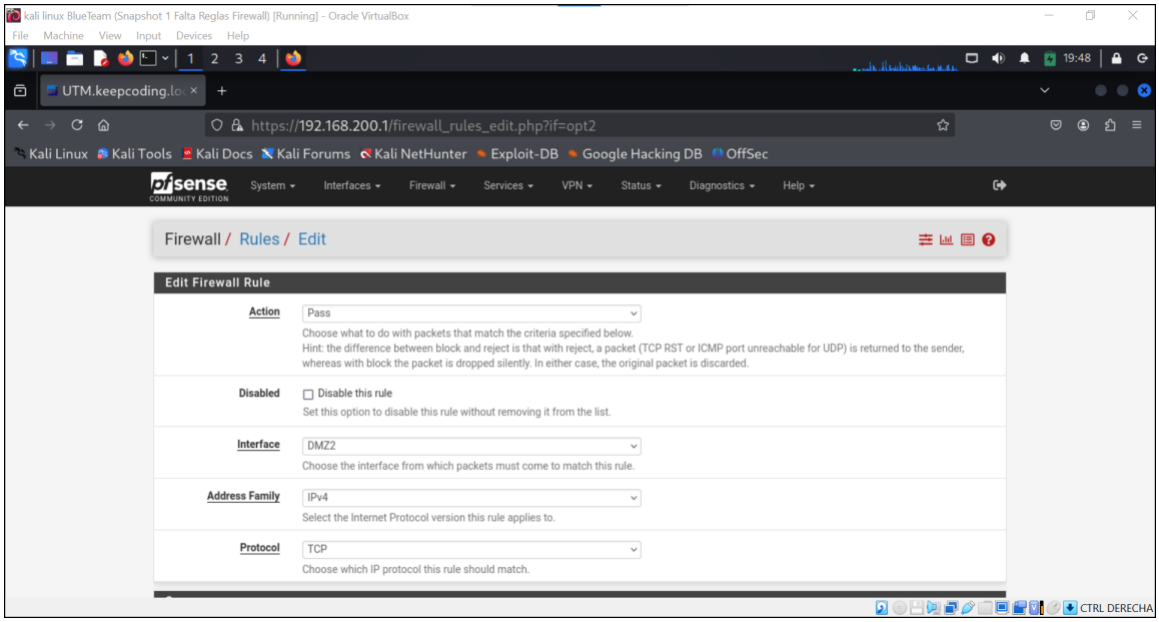
1.4.4. Reglas firewall DMZ2

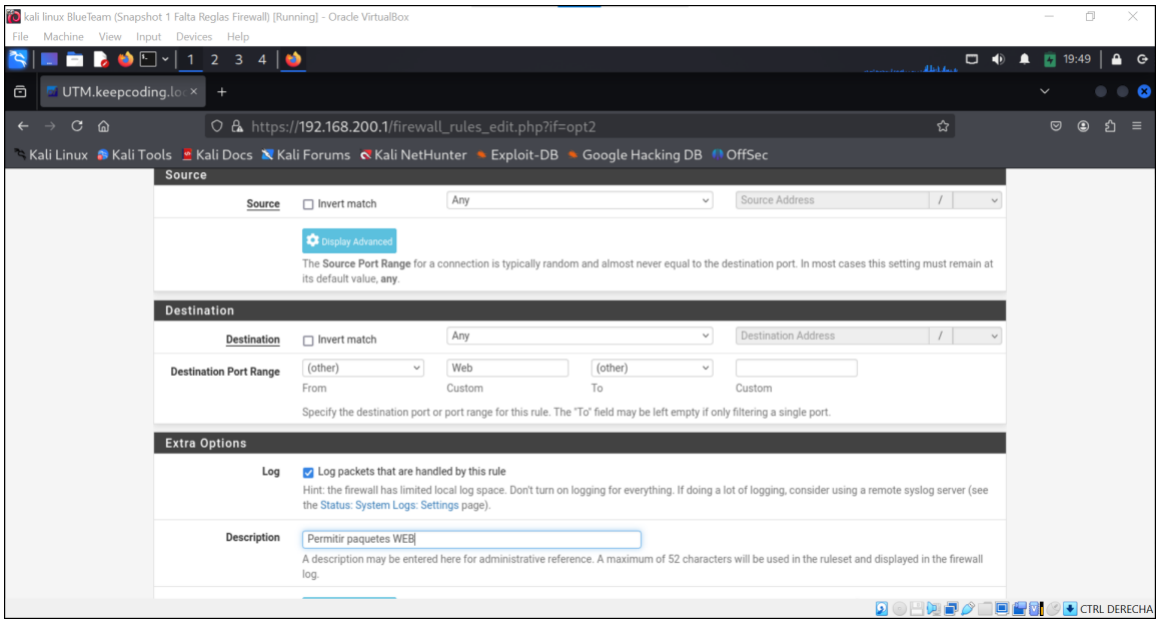
Vamos a bloquear la comunicación con la red DMZ



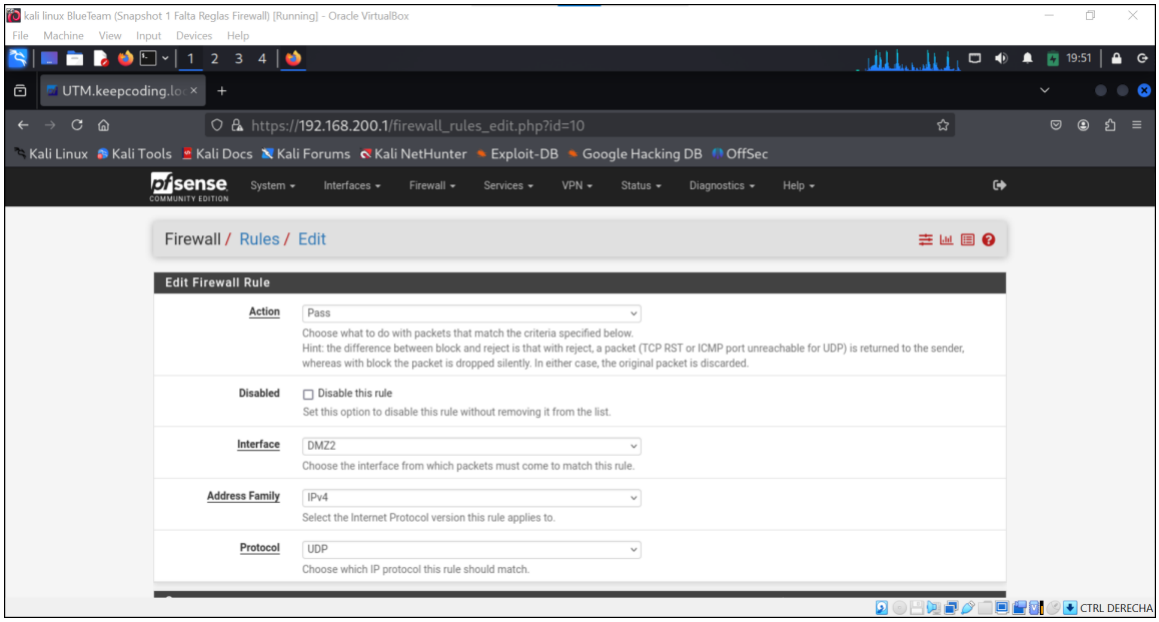


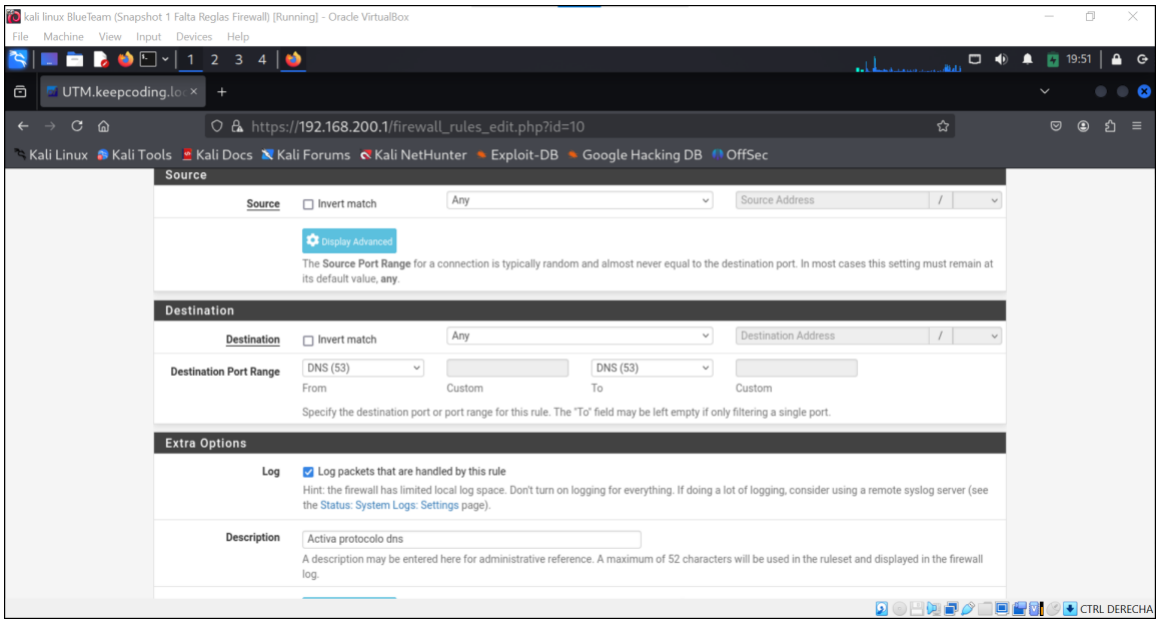
Ahora vamos a permitir los paquetes web a las red DMZ2.



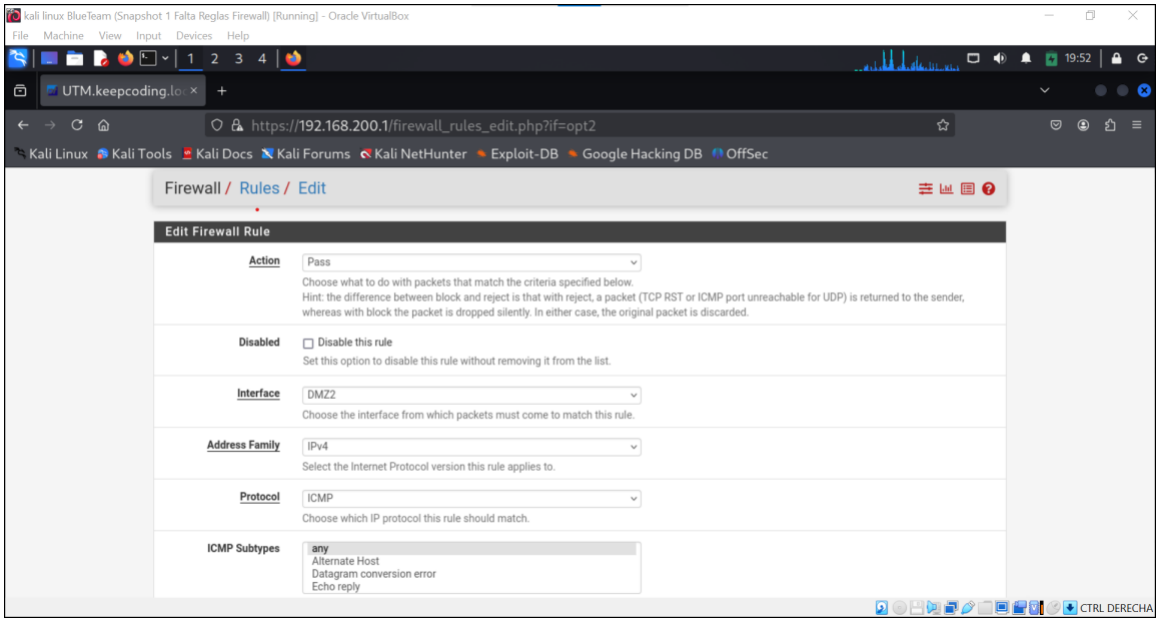


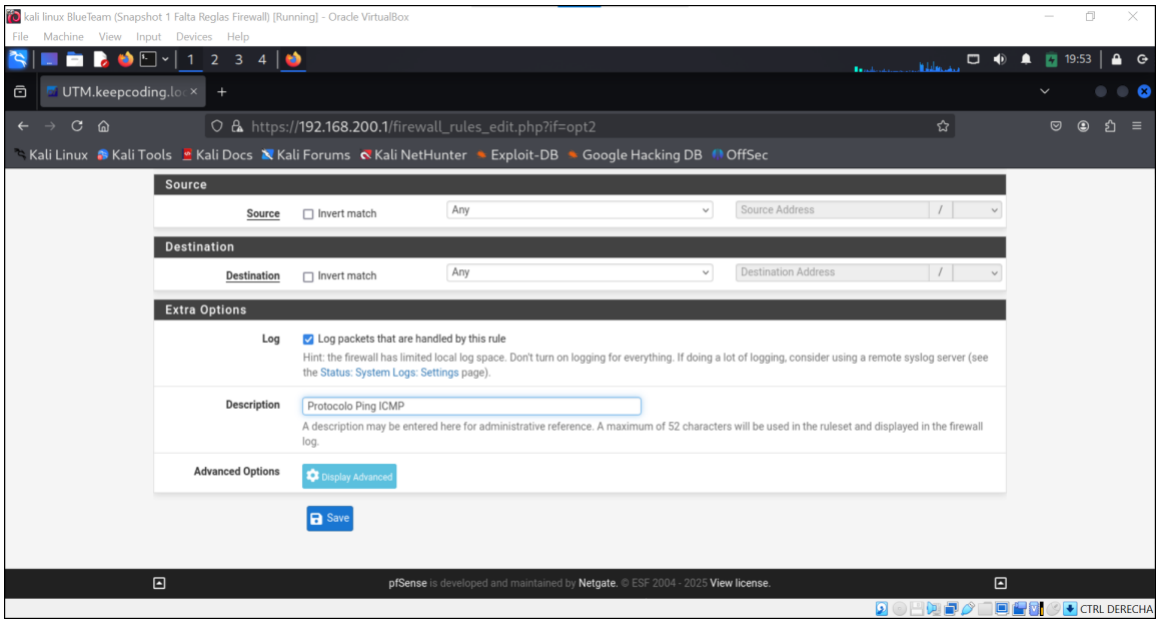
Ahora vamos a crear la regla DNS.





Protocolo ping.



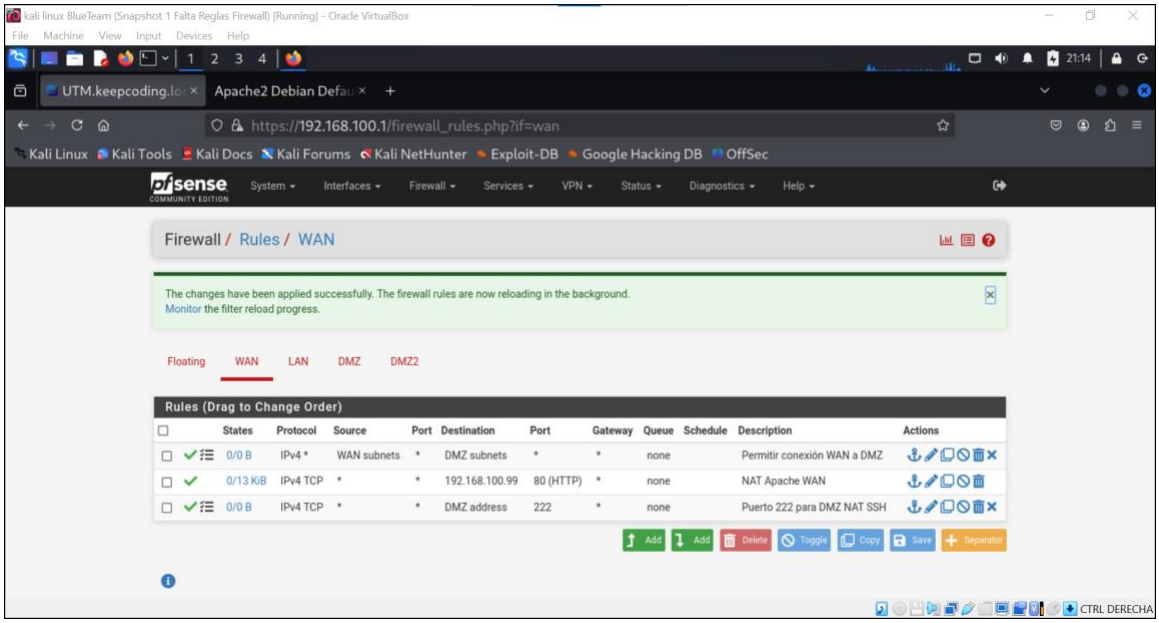


1.4.5. Reglas firewall WAN

En este apartado hemos definido 3 reglas:

La primera es la que permite la conexión con red dentro de casa con la red DMZ.

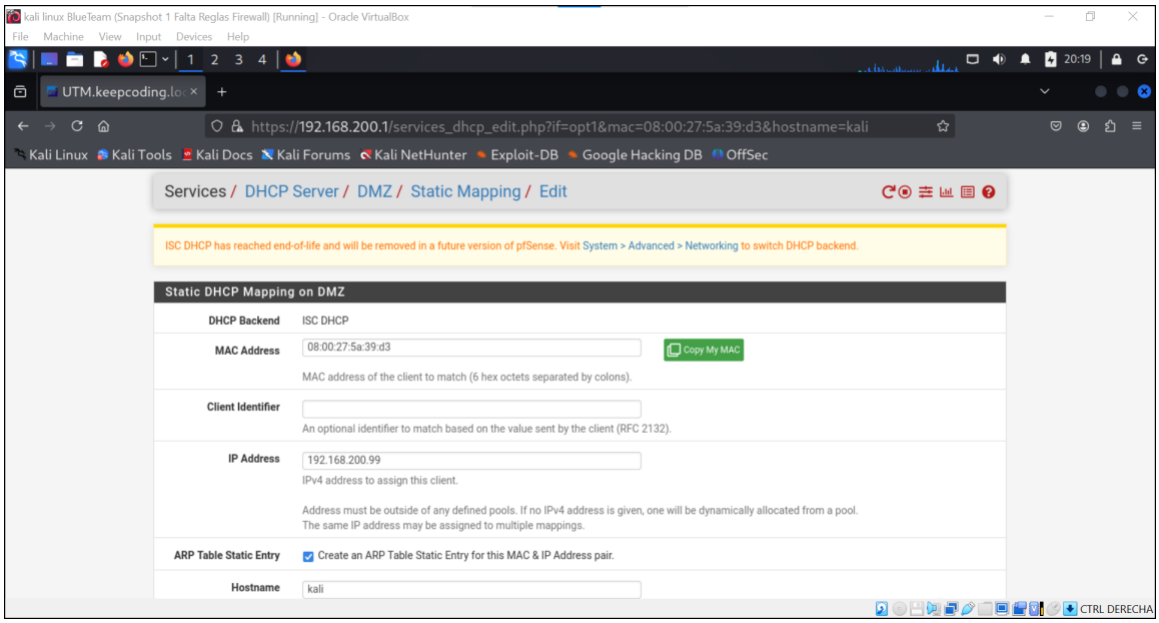
La tercera es que nos podemos conectar mediante SSH a la red DMZ por el puerto 222.

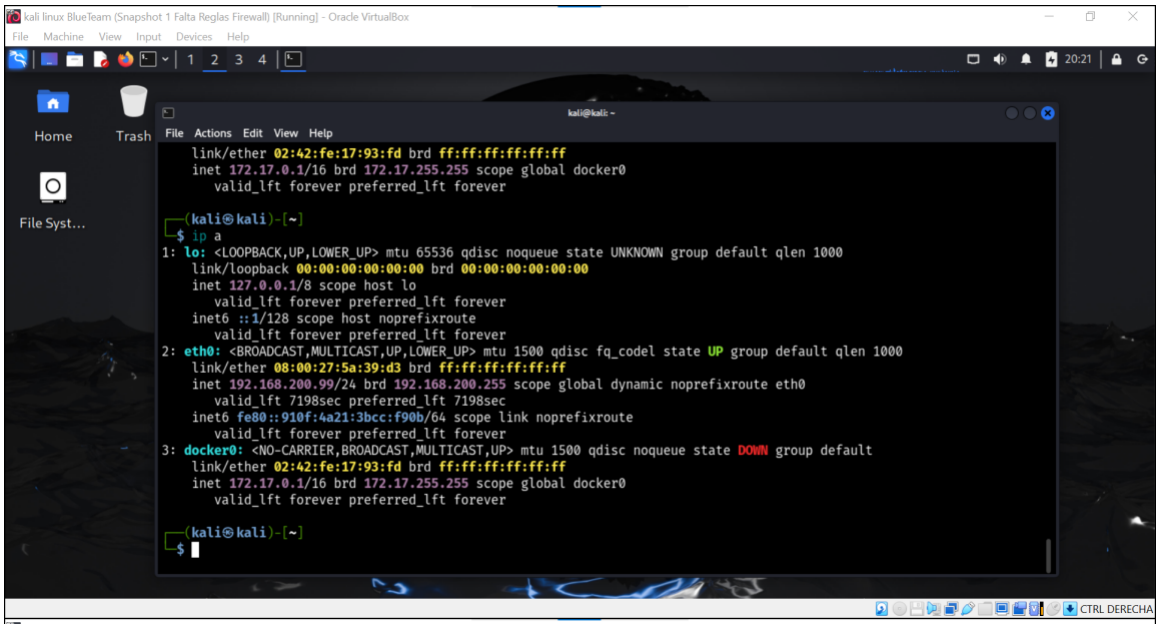


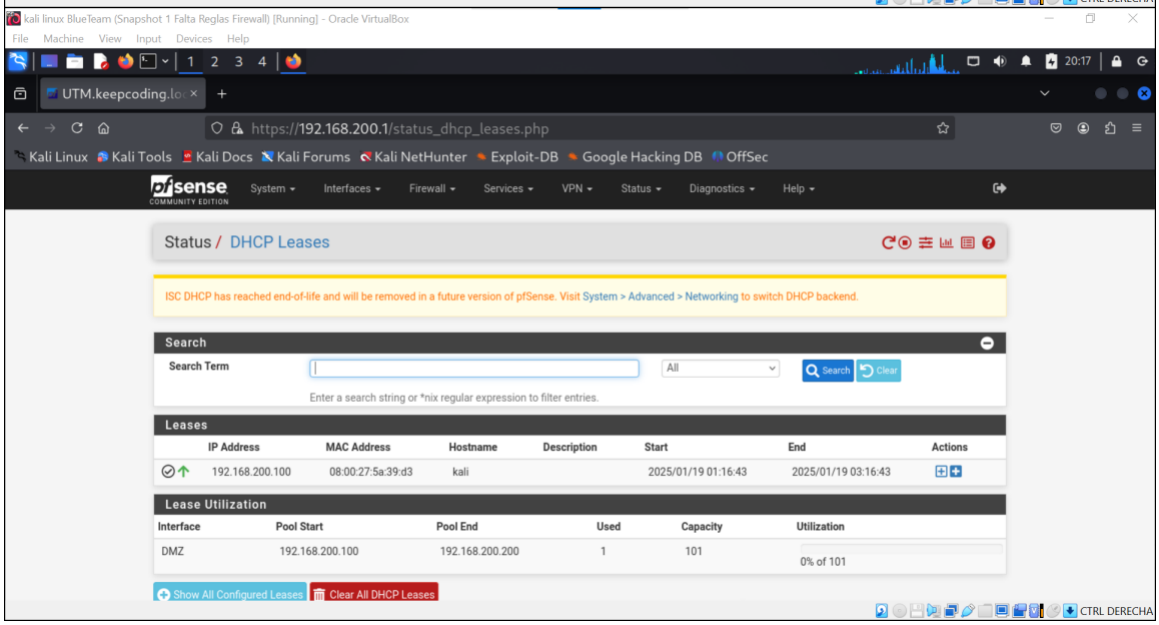
1.5. Defenir IPs estáticas

En este punto vamos a definir las IPs estáticas para las redes internas LAN, DMZ y DMZ2. El objetivo de esto es poder comprobar las conexiones entre ellas para verificar las reglas del firewall.

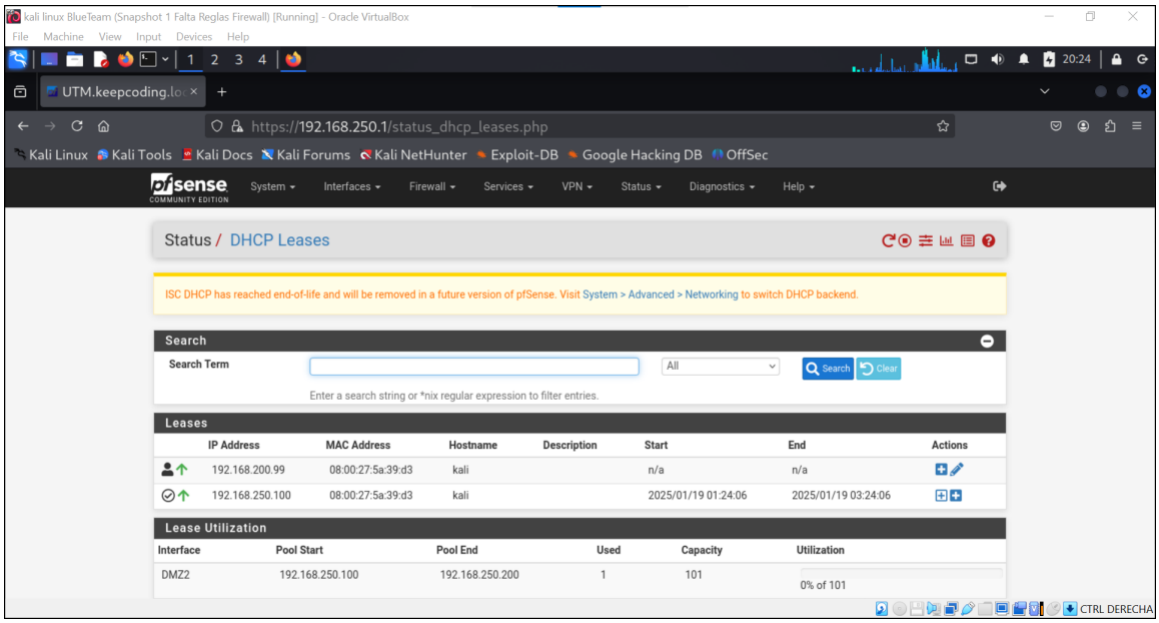
1.5.1 DMZ

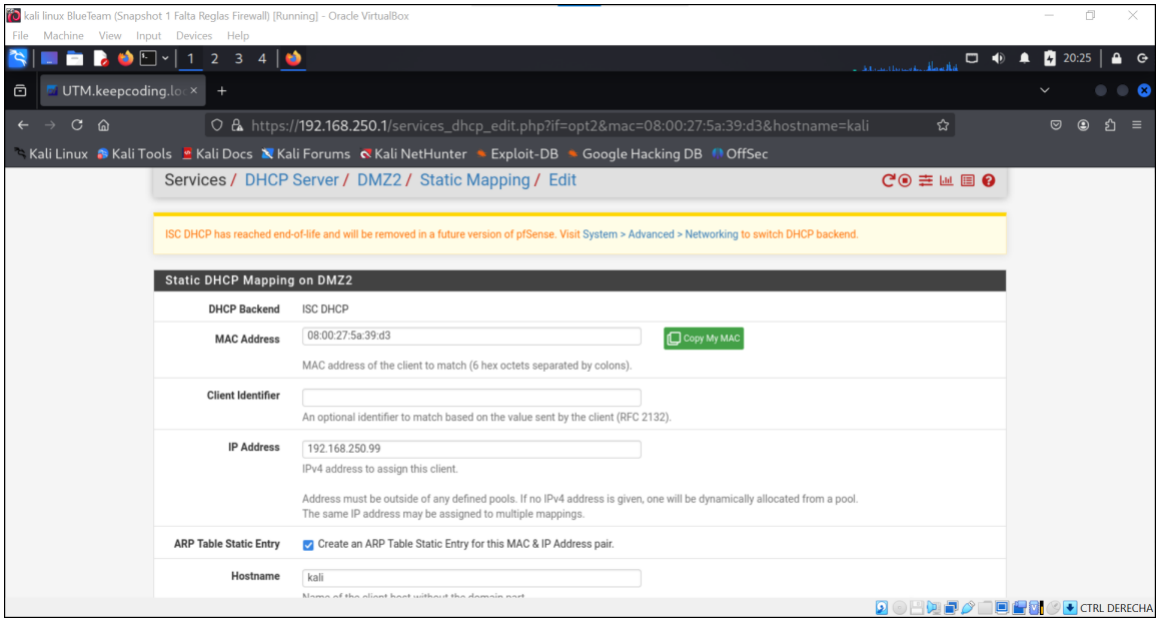


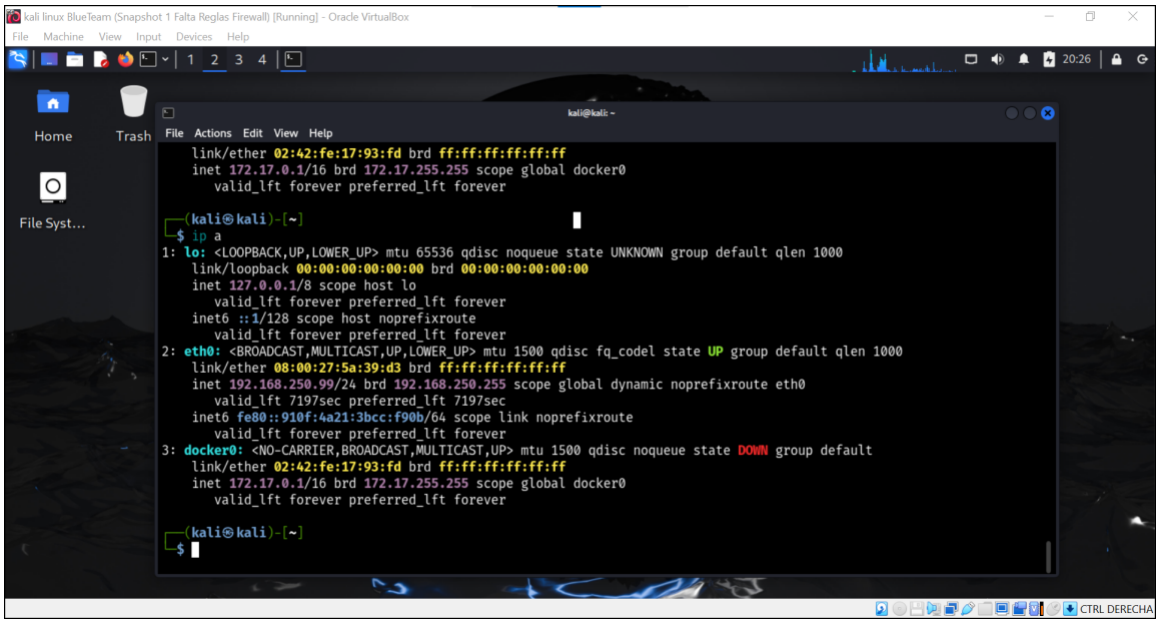

kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
20:21
Home
Trash
File Syst...
kali@kali: ~
File Actions Edit View Help
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
inet 192.168.200.99/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
valid_lft 7198sec preferred_lft 7198sec
inet6 fe80::910f:4a21:3bcc:f90b/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$
CTRL DERECHA


kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
20:17
UTM.keepcoding.lo
https://192.168.200.1/status_dhcp_leases.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Status / DHCP Leases
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
Search
Search Term
All
Search Clear
Enter a search string or *nix regular expression to filter entries.
Leases
IP Address MAC Address Hostname Description Start End Actions
192.168.200.100 08:00:27:5a:39:d3 kali 2025/01/19 01:16:43 2025/01/19 03:16:43
Lease Utilization
Interface Pool Start Pool End Used Capacity Utilization
DMZ 192.168.200.100 192.168.200.200 1 101 0% of 101
Show All Configured Leases
Clear All DHCP Leases
CTRL DERECHA

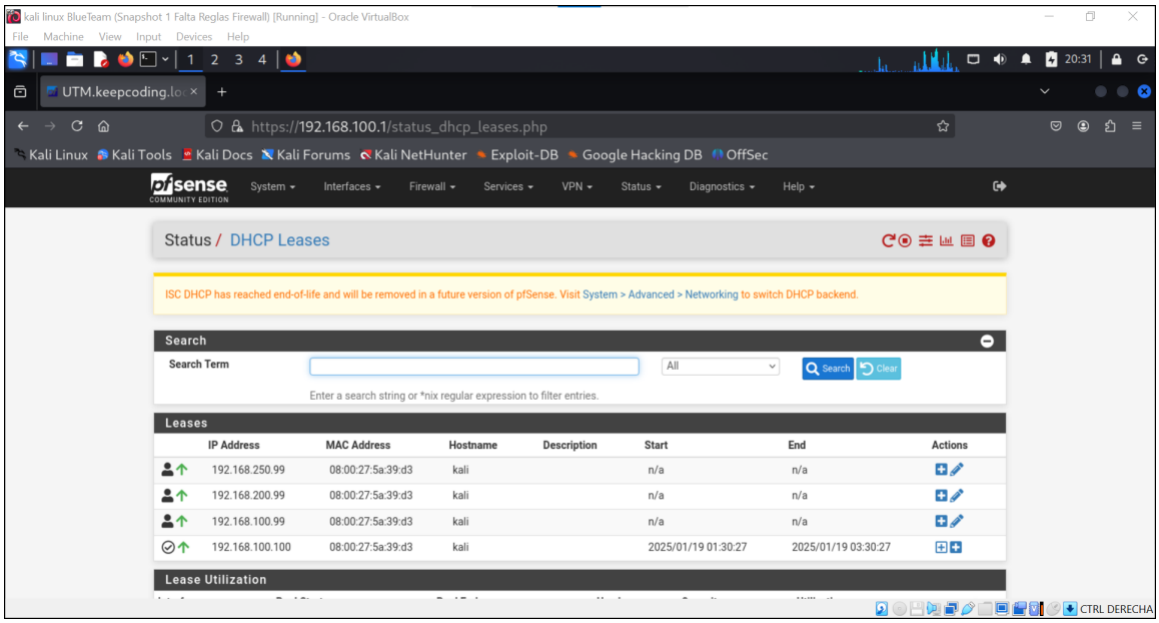
1.5.2 DMZ2

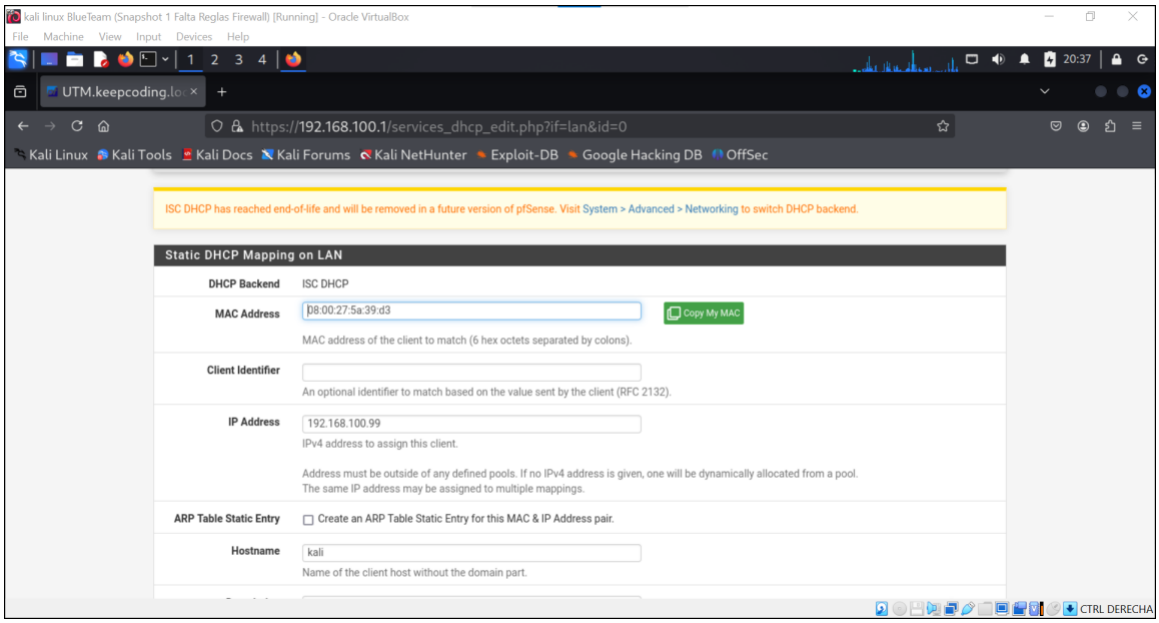

kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
https://192.168.250.1/status_dhcp_leases.php
Status / DHCP Leases
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
Search
Search Term
Enter a search string or *nix regular expression to filter entries.
Leases
IP Address MAC Address Hostname Description Start End Actions
192.168.200.99 08:00:27:5a:39:d3 kali n/a n/a
192.168.250.100 08:00:27:5a:39:d3 kali 2025/01/19 01:24:06 2025/01/19 03:24:06
Lease Utilization
Interface Pool Start Pool End Used Capacity Utilization
DMZ2 192.168.250.100 192.168.250.200 1 101
0% of 101

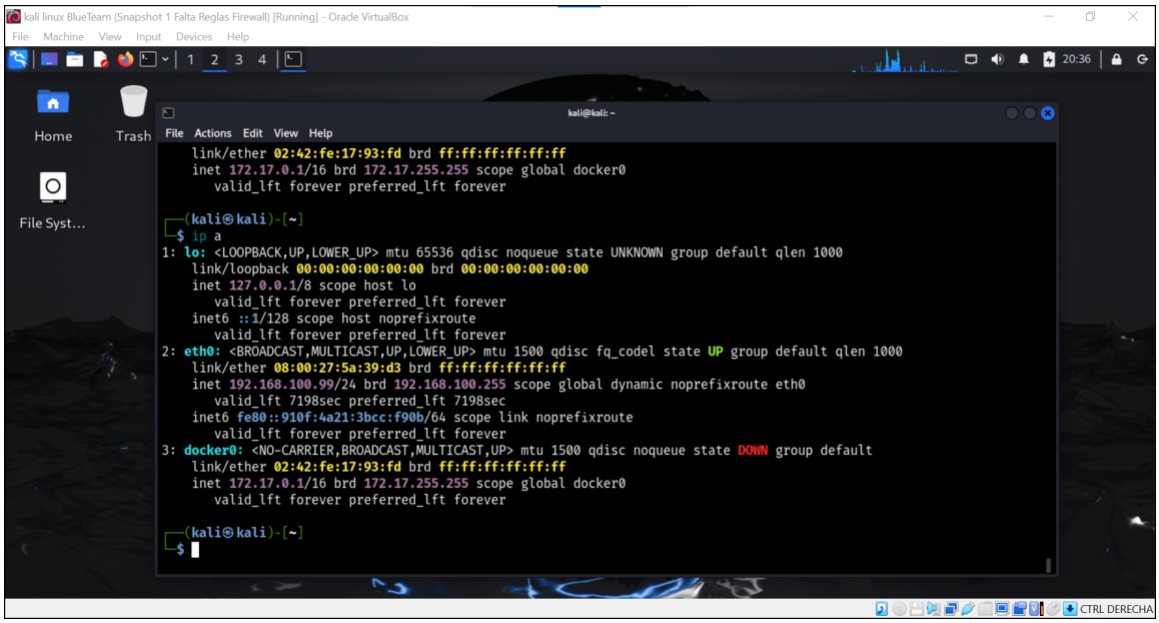

kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
https://192.168.250.1/services_dhcp_edit.php?if=opt2&mac=08:00:27:5a:39:d3&hostname=kali
Services / DHCP Server / DMZ2 / Static Mapping / Edit
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
Static DHCP Mapping on DMZ2
DHCP Backend ISC DHCP
MAC Address 08:00:27:5a:39:d3 Copy My MAC
MAC address of the client to match (6 hex octets separated by colons).
Client Identifier
An optional identifier to match based on the value sent by the client (RFC 2132).
IP Address 192.168.250.99
IPv4 address to assign this client.
Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool.
The same IP address may be assigned to multiple mappings.
ARP Table Static Entry Create an ARP Table Static Entry for this MAC & IP Address pair.
Hostname kali


kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
20:26
Home
Trash
File Syst...
kali@kali: ~
File Actions Edit View Help
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
inet 192.168.250.99/24 brd 192.168.250.255 scope global dynamic noprefixroute eth0
valid_lft 7197sec preferred_lft 7197sec
inet6 fe80::910f:4a21:3bcc:f90b/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$
CTRL DERECHA

1.5.3 LAN


kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
20:31
UTM.keepcoding.lo
https://192.168.100.1/status_dhcp_leases.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Status / DHCP Leases
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
Search
Search Term
All
Search
Clear
Enter a search string or *nix regular expression to filter entries.
Leases
IP Address MAC Address Hostname Description Start End Actions
192.168.250.99 08:00:27:5a:39:d3 kali n/a n/a
192.168.200.99 08:00:27:5a:39:d3 kali n/a n/a
192.168.100.99 08:00:27:5a:39:d3 kali n/a n/a
192.168.100.100 08:00:27:5a:39:d3 kali 2025/01/19 01:30:27 2025/01/19 03:30:27
Lease Utilization
CTRL DERECHA





2. Honeypots

Un honeypot es una herramienta que simula un equipo virtual, cuya función es enmascararse y adaptarse con la mayor exactitud a una página web ya existente para atraer a atacantes y estudiar su “modus operandi”. Por lo tanto, los puertos a esta máquina se suelen dejar fácilmente accesibles para que el atacante pueda acceder con una facilidad relativa; por el simple hecho de que si es demasiado simple acceder entonces sería fácil de llegar a la conclusión de que se trata de un honeypot.

También hay que recoger todos los logs en un documento de texto para después enviárselos a la plataforma web Elastic. Esto se ha logrado utilizando el comando “tail -f rdpy.log | tee >> /var/log/log_honeypots”. Y después habría que sincronizar este archivo con otro que se encontraría en el escritorío. Todo esto nos va a permitir secopilar y analizar los logs en “tiempo real”.

Por lo tanto, para crear y configurar esta herramienta primero debemos a acceder a nuestra máquina virtual Kali y nos conectaremos a la red DMZ.

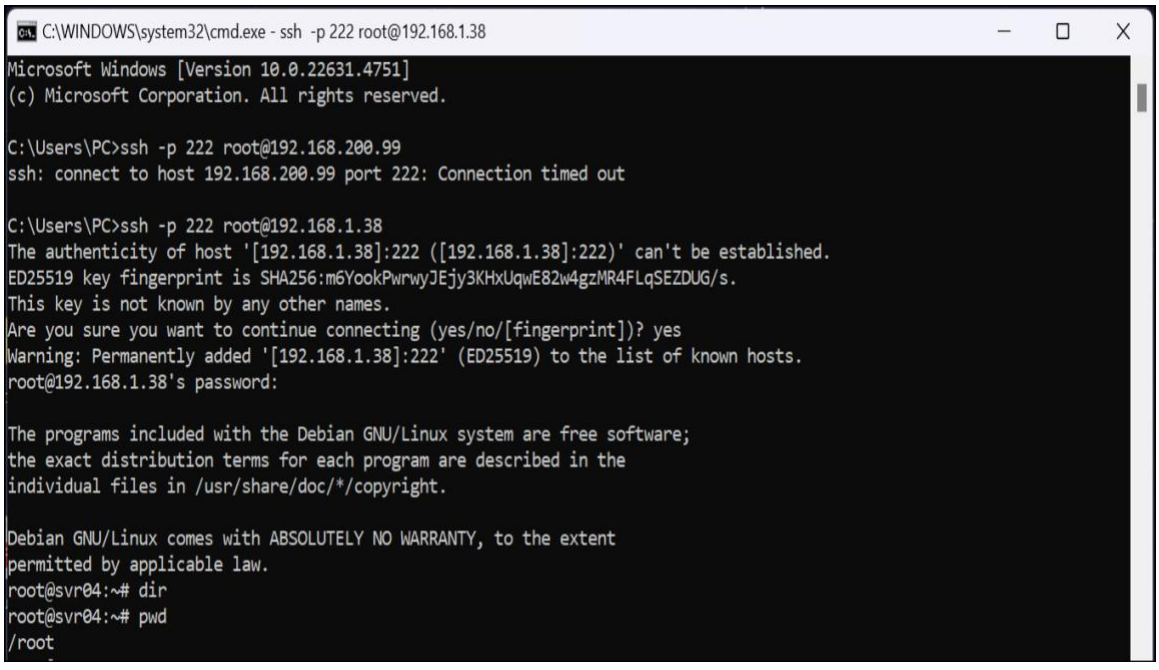
Cuando estemos dentro, activaremos la terminal y seguiremos los siguientes pasos:

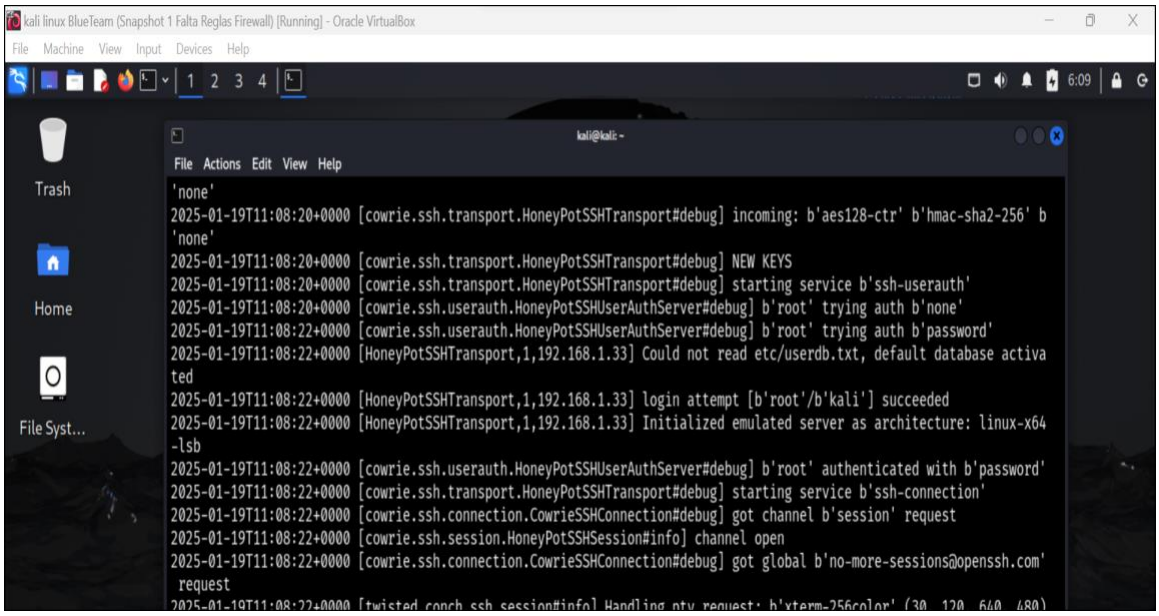
1. Pondremos el siguiente comando:

   docker run -p 222:2222 cowrie/cowrie #| El puerto 22 es el que corre el ssh.

2. Después en nuestra maquina Kali tenemos que hacer ip -a para saber nuestra ip.
3. Ejecutamos el siguiente comando en nuestro Windows, donde la ip es nuestra ip estatica:
   ssh -p 222 root@192.168.200.99

4. Y desde ese momento ya tenemos el control sobre la máquina virtual.

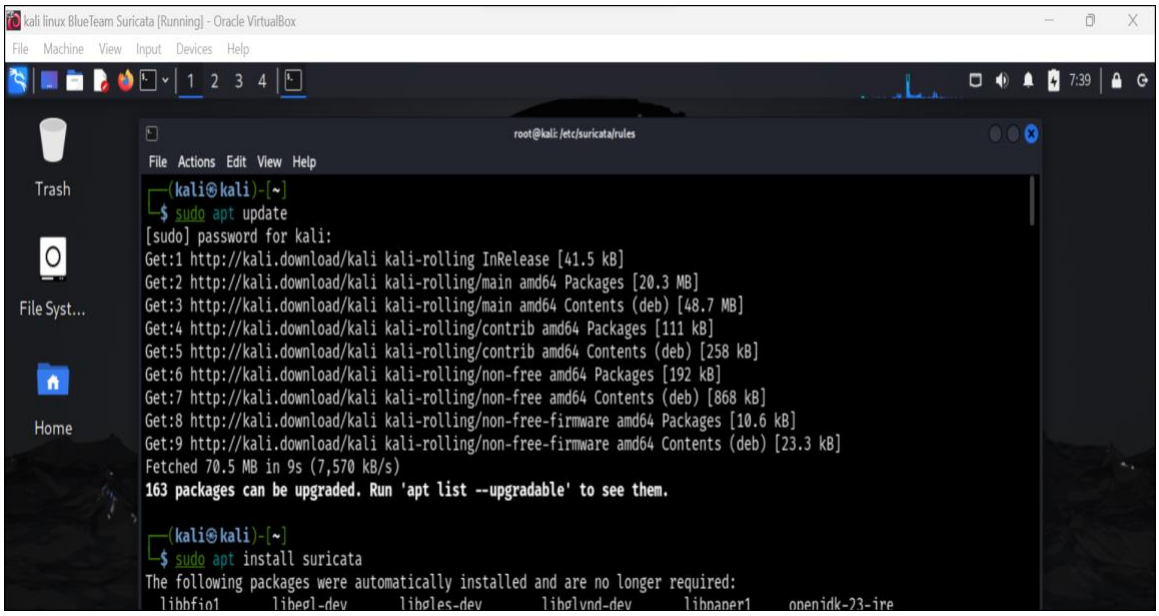


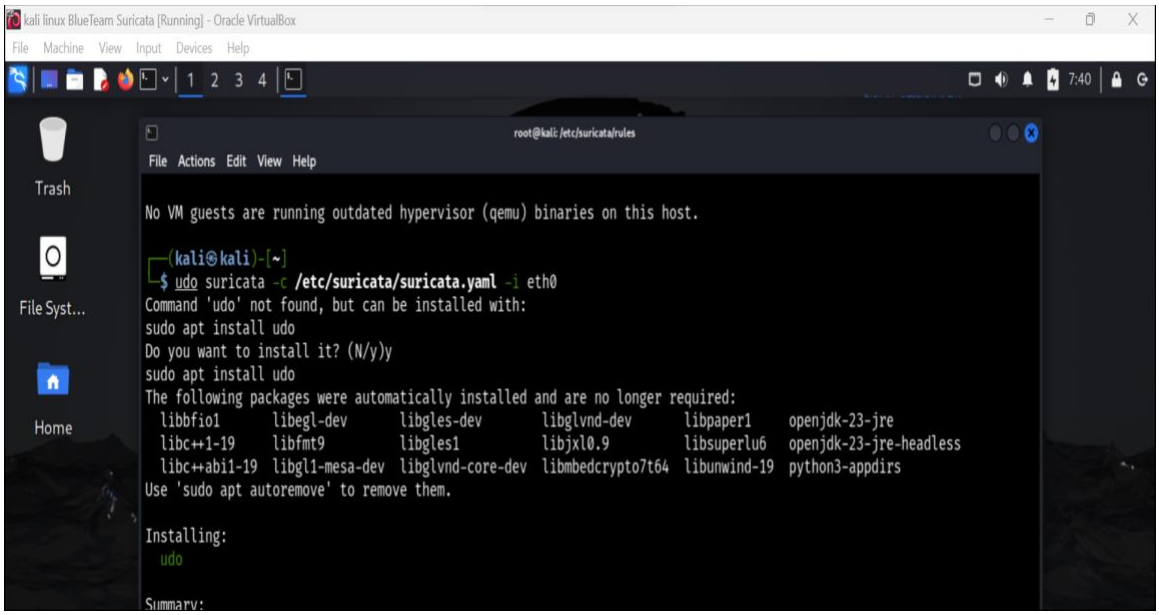


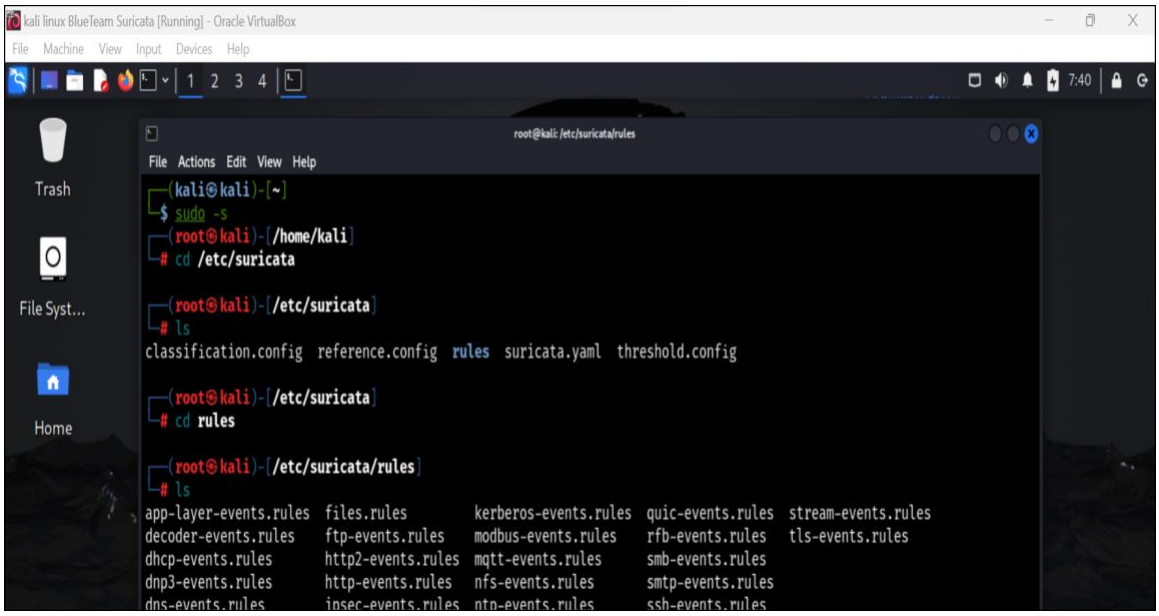
3. Suricata

Suricata es una herramienta avanzada de detección y prevención de intrusiones que permite monitorear redes para identificar actividades sospechosas. Vamos a documentar su instalación, configuración y personalización mediante reglas diseñadas para detectar eventos específicos, como tráfico de red, intentos de conexión SSH y descargas de archivos PDF. La instalación se realiza actualizando los paquetes del sistema e instalando Suricata, seguida de una ejecución inicial para verificar su funcionamiento.

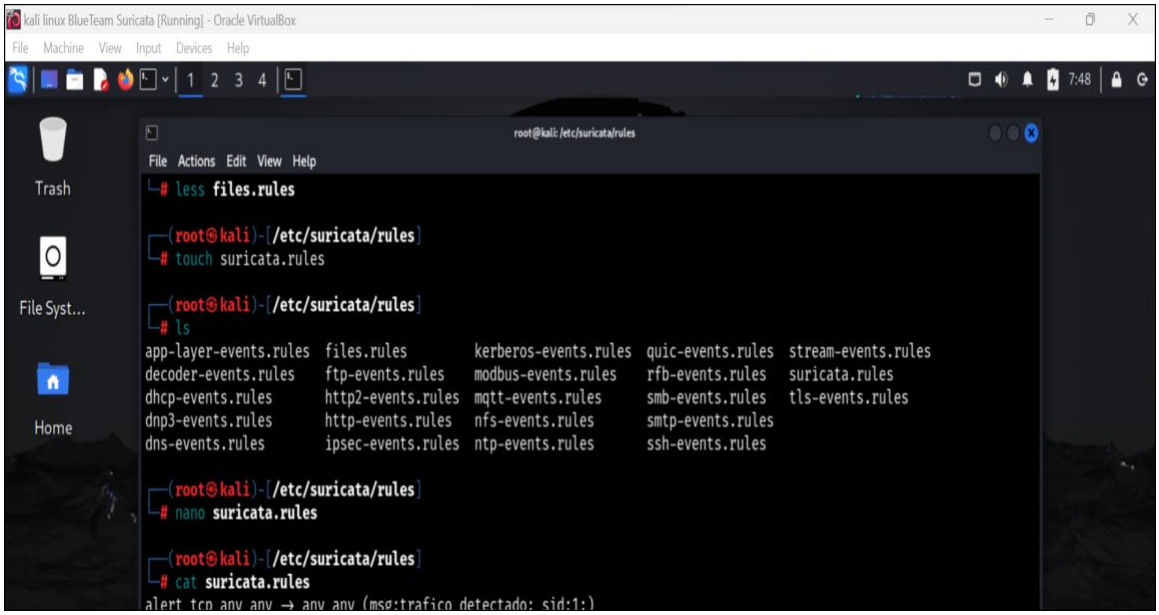
Además, se describieron procedimientos para analizar y guardar los logs generados, esenciales para el análisis posterior y la respuesta a incidentes. Los logs se almacenan en el directorio /var/log/suricata, y se pueden respaldar mediante compresión y transferencia a un servidor remoto para asegurar su disponibilidad. En conjunto, estas configuraciones convierten a Suricata en una herramienta poderosa para fortalecer la seguridad de la red, proporcionando visibilidad y capacidad de respuesta frente a posibles amenazas. Los logs posteriormente se guardarán en la plataforma web Elastic.

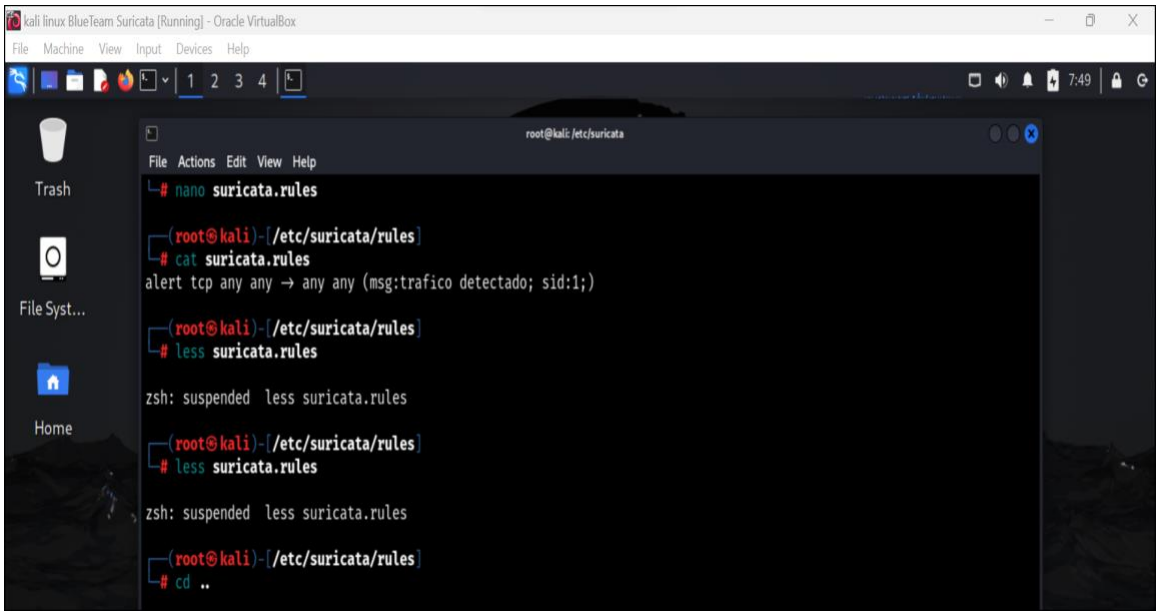

kali linux BlueTeam Suricata [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:39
Trash
File Syst...
Home
root@kali: /etc/suricata/rules
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.7 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [258 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [868 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.3 kB]
Fetched 70.5 MB in 9s (7,570 kB/s)
163 packages can be upgraded. Run 'apt list --upgradable' to see them.
┌──(kali㉿kali)-[~]
└─$ sudo apt install suricata
The following packages were automatically installed and are no longer required:
libbfio1 libegl-dev libgles-dev libglvnd-dev libpaper1 openjdk-23-jre

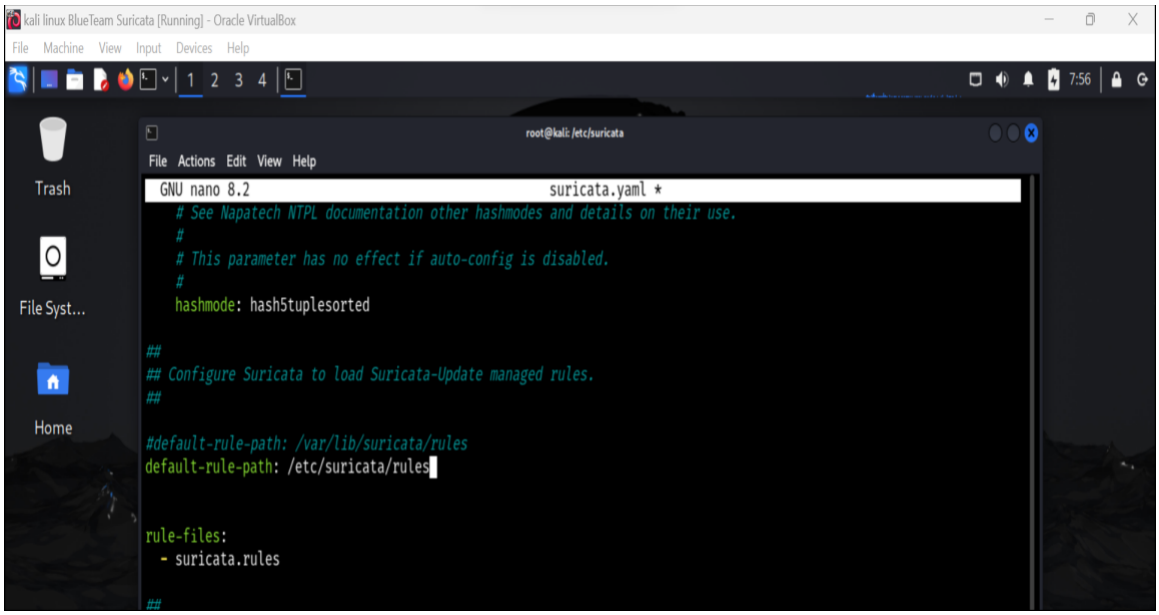

kali linux BlueTeam Suricata [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:40
Trash
File Syst...
Home
root@kali: /etc/suricata/rules
File Actions Edit View Help
No VM guests are running outdated hypervisor (qemu) binaries on this host.
┌──(kali㉿kali)-[~]
└─$ udo suricata -c /etc/suricata/suricata.yaml -i eth0
Command 'udo' not found, but can be installed with:
sudo apt install udo
Do you want to install it? (N/y)y
sudo apt install udo
The following packages were automatically installed and are no longer required:
libbfio1 libegl-dev libgles-dev libglvnd-dev libpaper1 openjdk-23-jre
libc++1-19 libfmt9 libgles1 libjxl0.9 libsuperlu6 openjdk-23-jre-headless
libc++abi1-19 libgl1-mesa-dev libglvnd-core-dev libmbedcrypto7t64 libunwind-19 python3-appdirs
Use 'sudo apt autoremove' to remove them.
Installing:
udo
Summary:

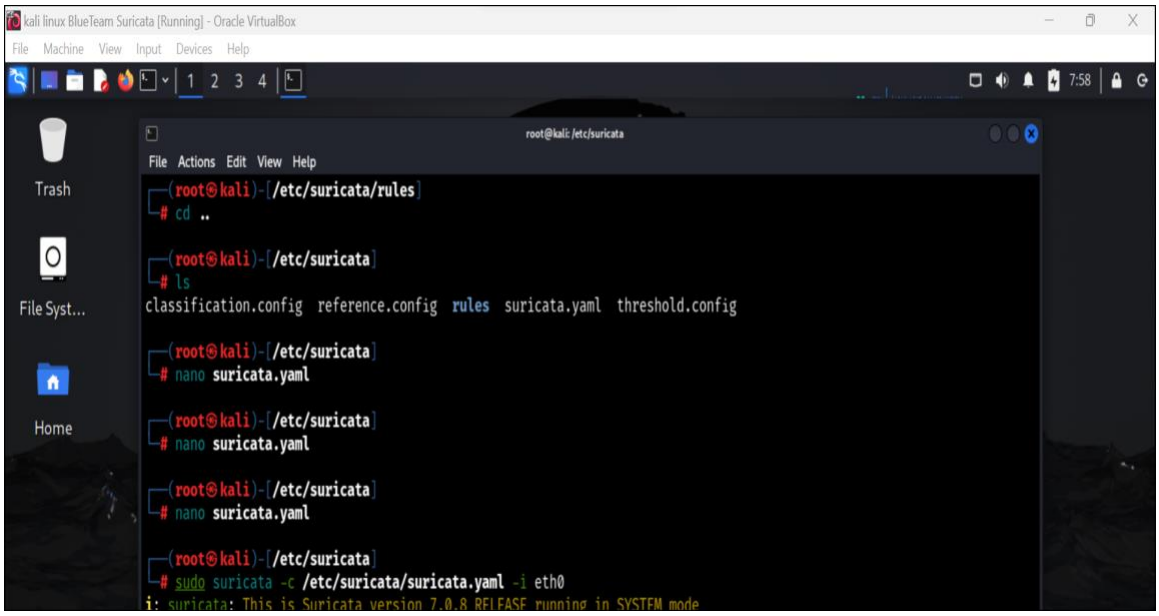


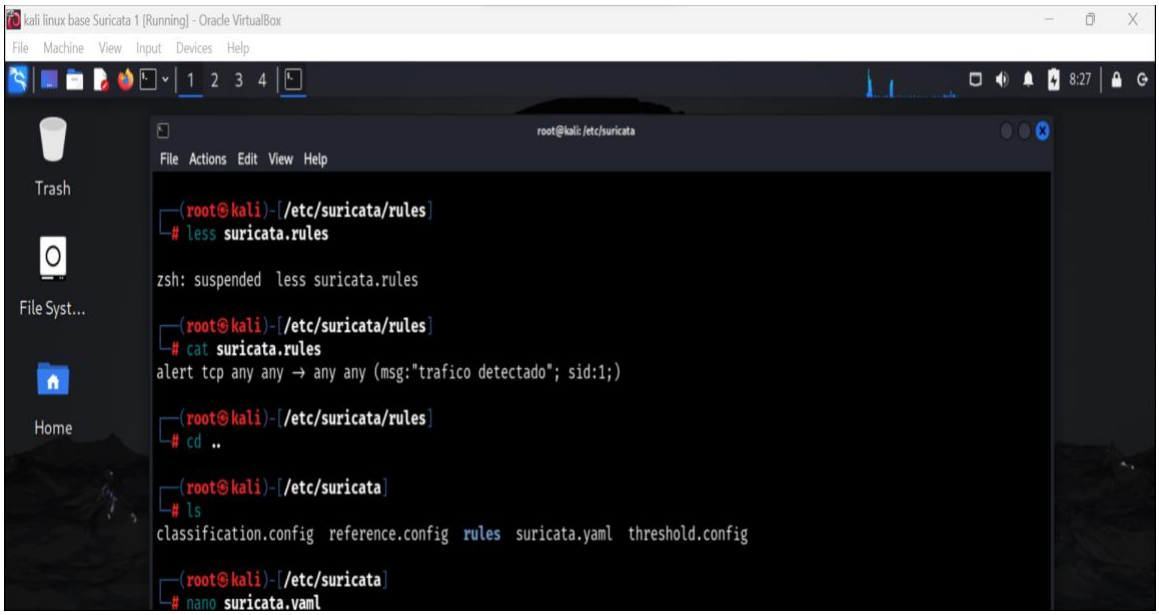
Primera regla de suricata.

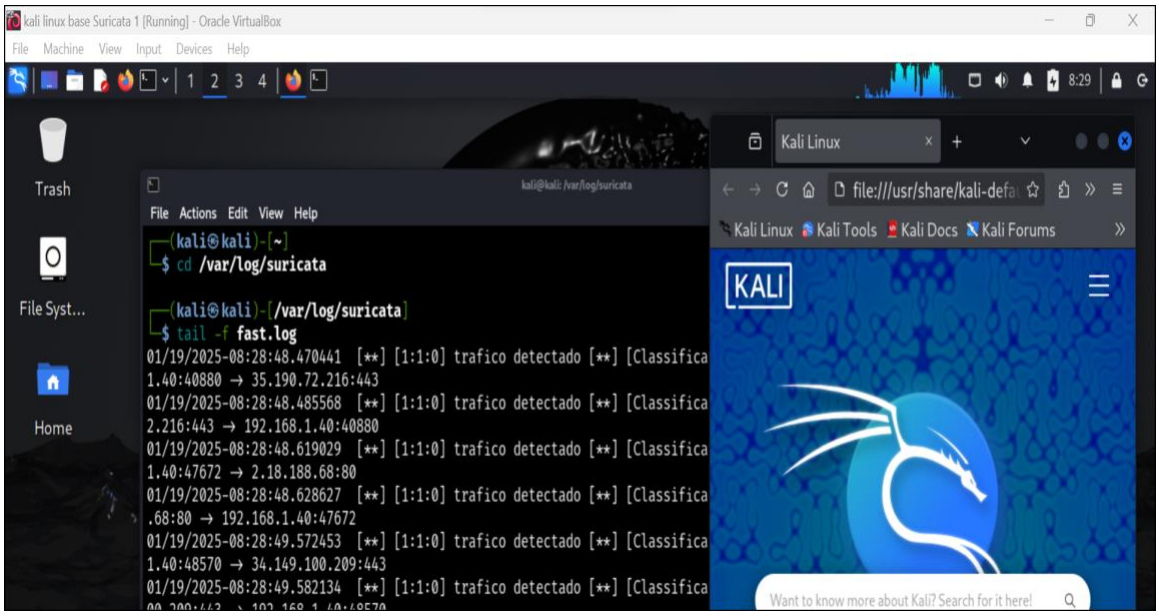



kali linux BlueTeam Suricata [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:49
Trash
File Syst...
Home
root@kali: /etc/suricata
File Actions Edit View Help
nano suricata.rules
(root㉿kali)-[/etc/suricata/rules]
cat suricata.rules
alert tcp any any → any any (msg:trafico detectado; sid:1;)
(root㉿kali)-[/etc/suricata/rules]
less suricata.rules
zsh: suspended less suricata.rules
(root㉿kali)-[/etc/suricata/rules]
less suricata.rules
zsh: suspended less suricata.rules
(root㉿kali)-[/etc/suricata/rules]
cd ..

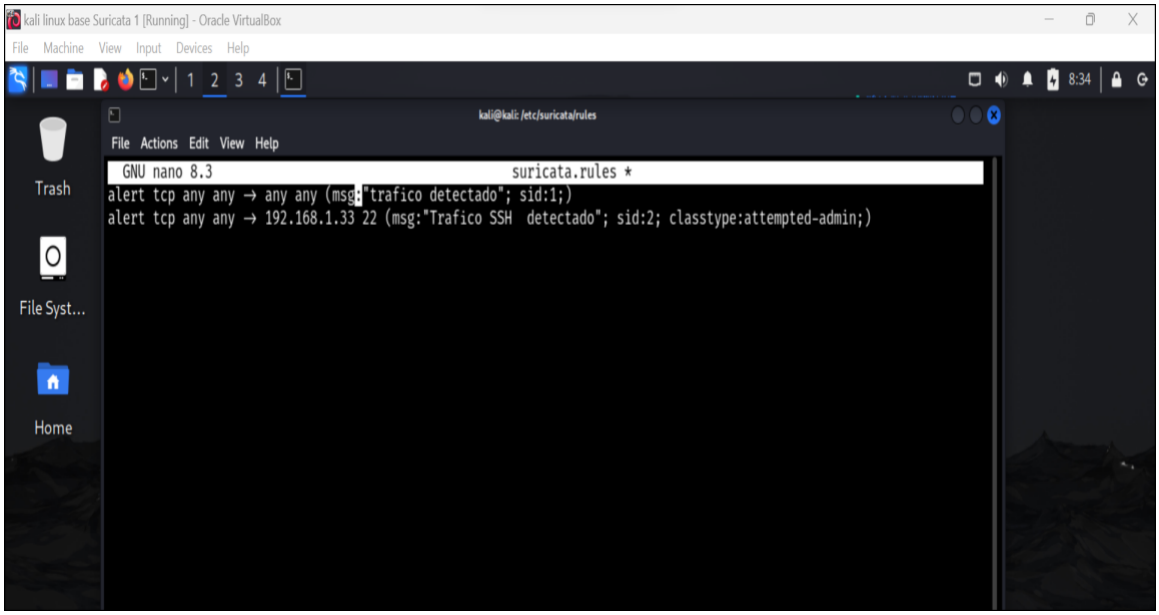

kali linux BlueTeam Suricata [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:56
Trash
File Syst...
Home
root@kali: /etc/suricata
File Actions Edit View Help
GNU nano 8.2 suricata.yaml *
See Napatech NTPL documentation other hashmodes and details on their use.
#
This parameter has no effect if auto-config is disabled.
#
hashmode: hash5tuplesorted
##
Configure Suricata to load Suricata-Update managed rules.
##
#default-rule-path: /var/lib/suricata/rules
default-rule-path: /etc/suricata/rules
rule-files:
- suricata.rules
##

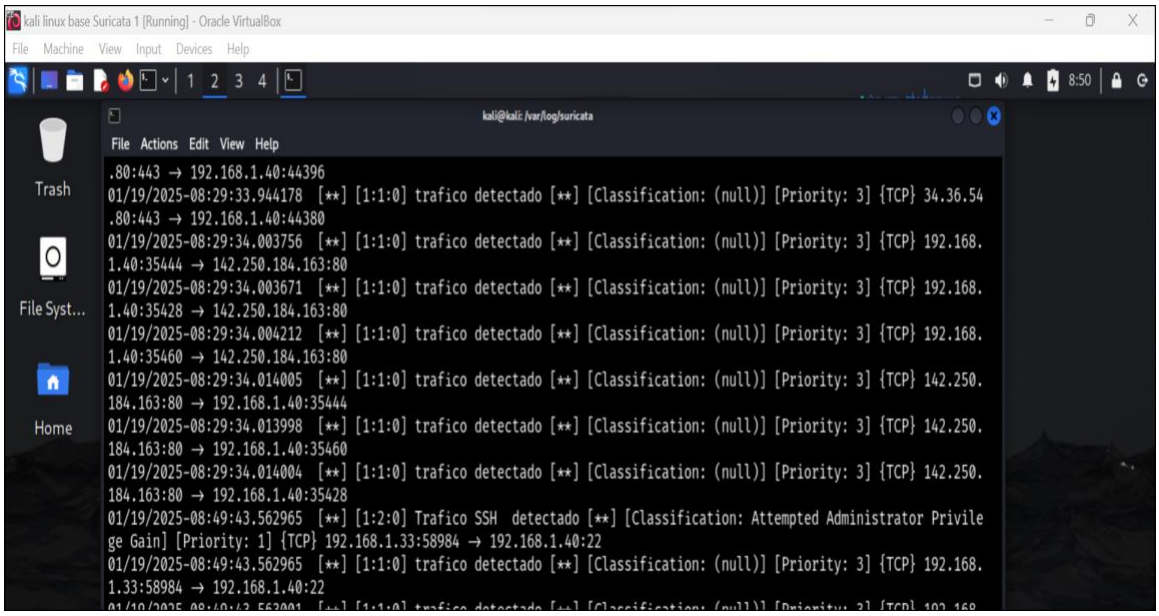

kali linux BlueTeam Suricata [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:58
Trash
File Syst...
Home
root@kali: /etc/suricata
File Actions Edit View Help
┌──(root㉿kali)-[/etc/suricata/rules]
└─# cd ..
┌──(root㉿kali)-[/etc/suricata]
└─# ls
classification.config reference.config rules suricata.yaml threshold.config
┌──(root㉿kali)-[/etc/suricata]
└─# nano suricata.yaml
┌──(root㉿kali)-[/etc/suricata]
└─# nano suricata.yaml
┌──(root㉿kali)-[/etc/suricata]
└─# nano suricata.yaml
┌──(root㉿kali)-[/etc/suricata]
└─# sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode

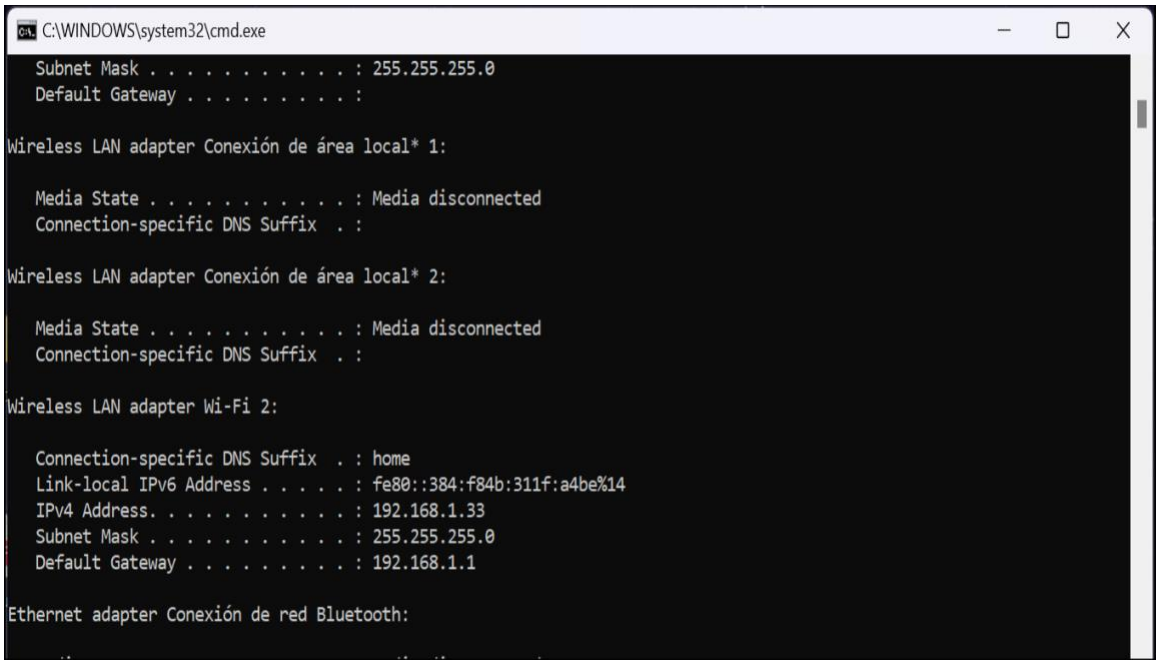

kali linux base Suricata 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:27
Trash
File Syst...
Home
root@kali: /etc/suricata
File Actions Edit View Help
┌──(root㉿kali)-[/etc/suricata/rules]
└─# less suricata.rules
zsh: suspended less suricata.rules
┌──(root㉿kali)-[/etc/suricata/rules]
└─# cat suricata.rules
alert tcp any any → any any (msg:"trafico detectado"; sid:1;)
┌──(root㉿kali)-[/etc/suricata/rules]
└─# cd ..
┌──(root㉿kali)-[/etc/suricata]
└─# ls
classification.config reference.config rules suricata.yaml threshold.config
┌──(root㉿kali)-[/etc/suricata]
└─# nano suricata.yaml

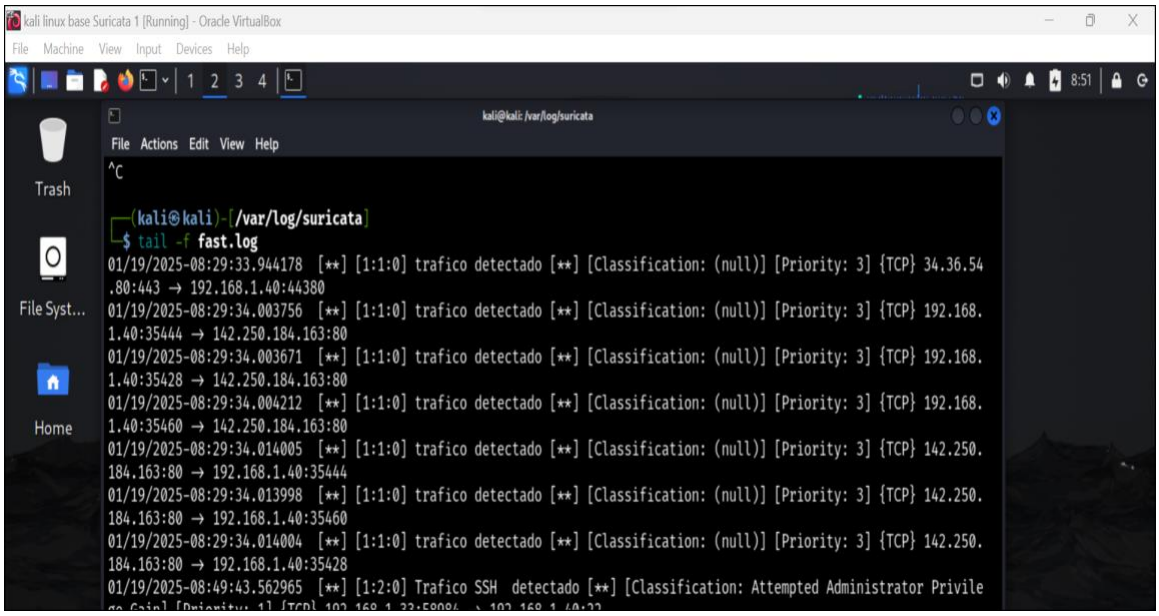


Segunda regla de suricata.

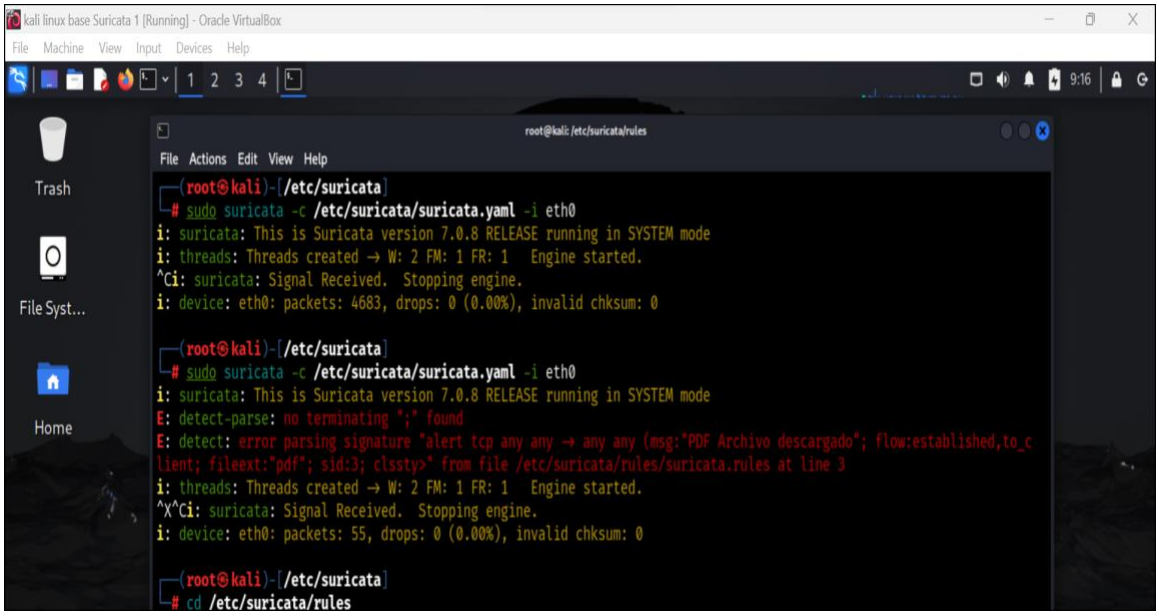


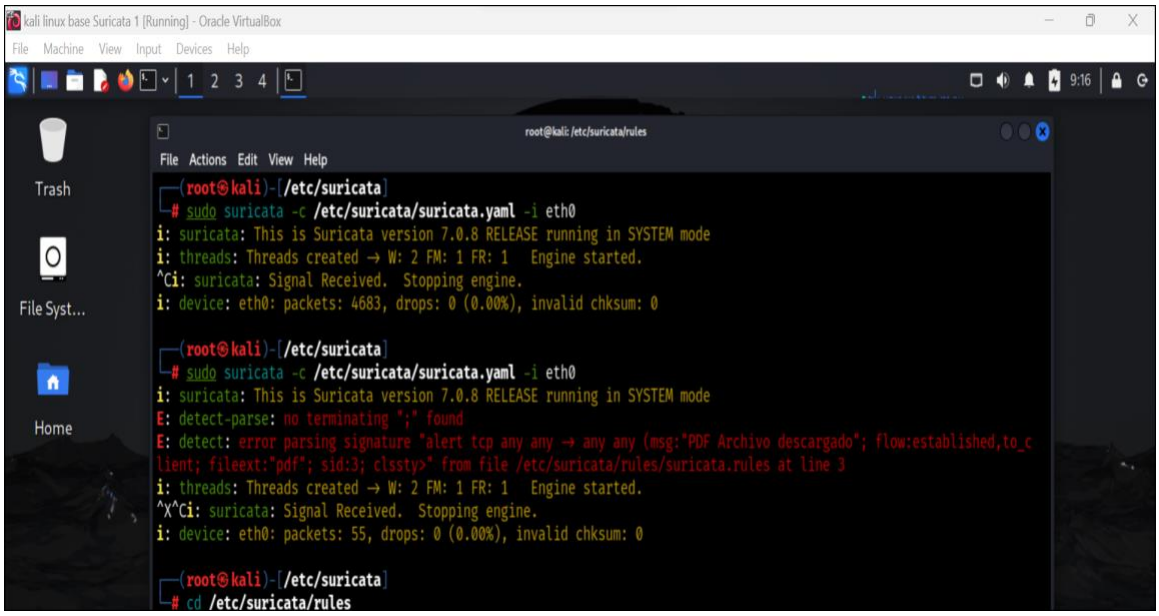

kali linux base Suricata 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:50
kali@kali: /var/log/suricata
File Actions Edit View Help
Trash
File Syst...
Home
.80:443 → 192.168.1.40:44396
01/19/2025-08:29:33.944178 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 34.36.54
.80:443 → 192.168.1.40:44380
01/19/2025-08:29:34.003756 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.
1.40:35444 → 142.250.184.163:80
01/19/2025-08:29:34.003671 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.
1.40:35428 → 142.250.184.163:80
01/19/2025-08:29:34.004212 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.
1.40:35460 → 142.250.184.163:80
01/19/2025-08:29:34.014005 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 142.250.
184.163:80 → 192.168.1.40:35444
01/19/2025-08:29:34.013998 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 142.250.
184.163:80 → 192.168.1.40:35460
01/19/2025-08:29:34.014004 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 142.250.
184.163:80 → 192.168.1.40:35428
01/19/2025-08:49:43.562965 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privile
ge Gain] [Priority: 1] {TCP} 192.168.1.33:58984 → 192.168.1.40:22
01/19/2025-08:49:43.562965 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.
1.33:58984 → 192.168.1.40:22

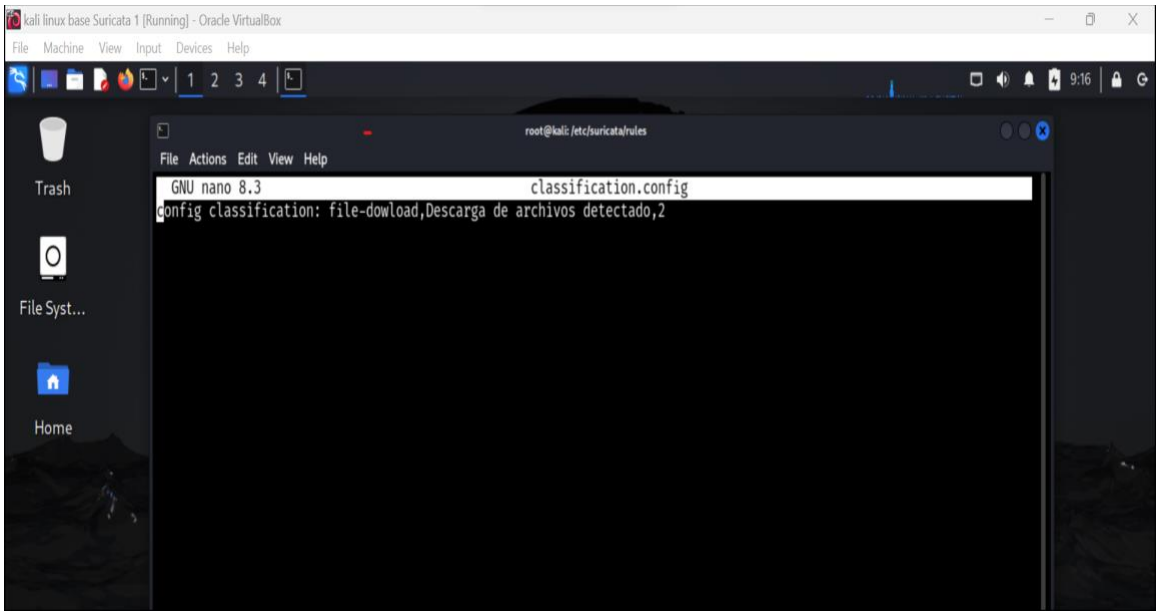

C:\WINDOWS\system32\cmd.exe
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Conexión de área local* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Conexión de área local* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi 2:
Connection-specific DNS Suffix . : home
Link-local IPv6 Address . . . . . : fe80::384:f84b:311f:a4be%14
IPv4 Address. . . . . : 192.168.1.33
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Ethernet adapter Conexión de red Bluetooth:

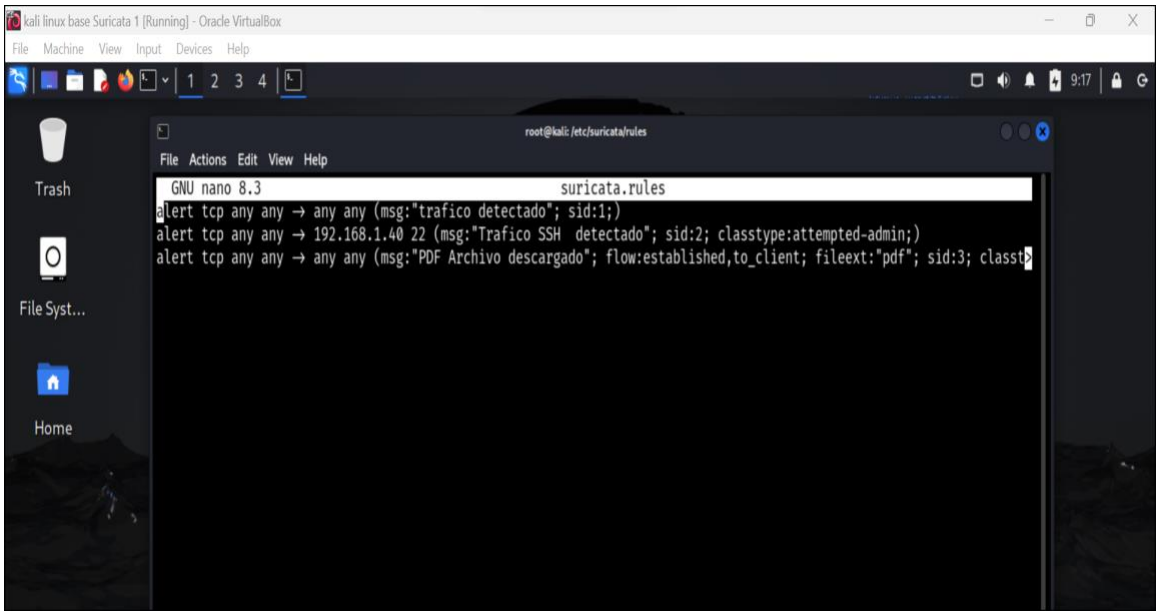


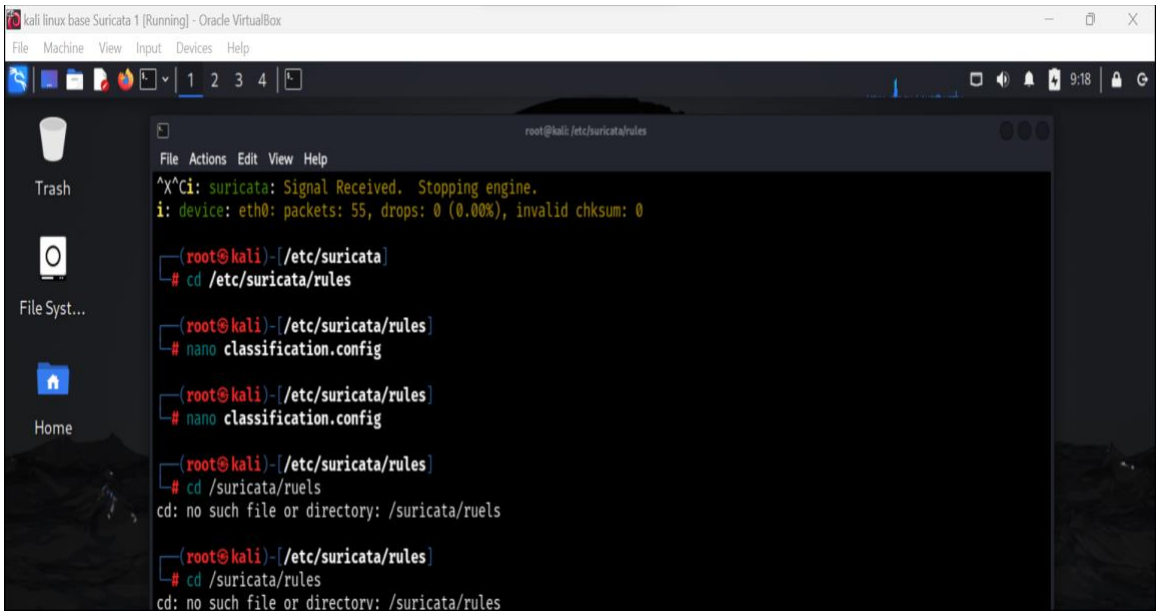
Tercera regla de suricata.

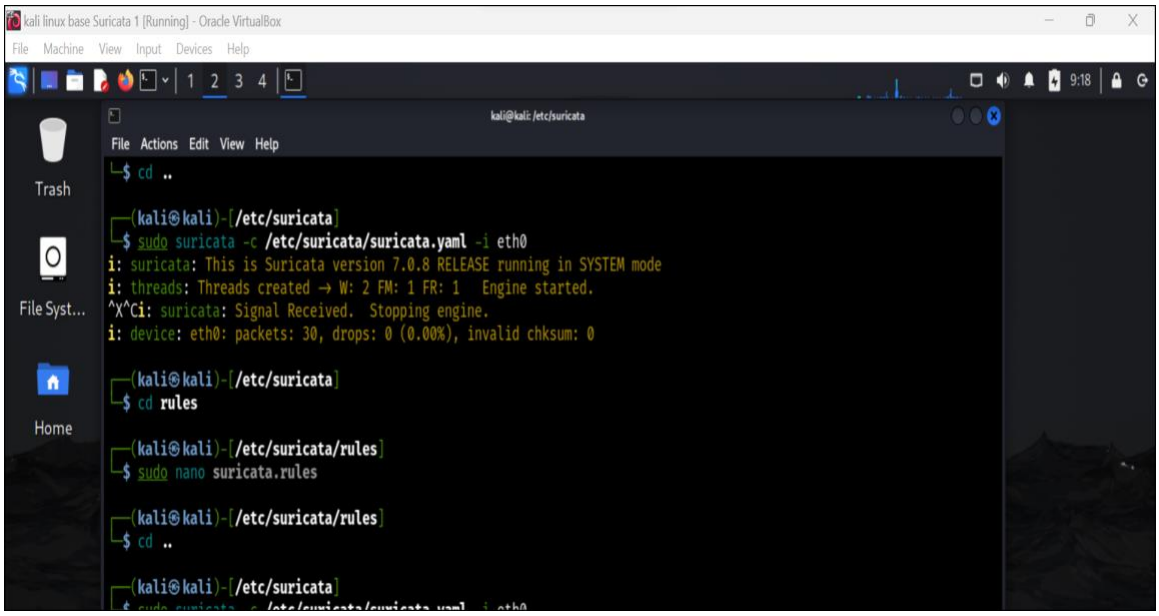



kali linux base Suricata 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:16
Trash
File Syst...
Home
root@kali: /etc/suricata/rules
File Actions Edit View Help
┌──(root㉿kali)-[/etc/suricata]
└─# sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.
^Ci: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 4683, drops: 0 (0.00%), invalid chksum: 0
┌──(root㉿kali)-[/etc/suricata]
└─# sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
E: detect-parse: no terminating ";" found
E: detect: error parsing signature "alert tcp any any → any any (msg:"PDF Archivo descargado"; flow:established,to_client; fileext:"pdf"; sid:3; clsstyp" from file /etc/suricata/rules/suricata.rules at line 3
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.
^X^Ci: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 55, drops: 0 (0.00%), invalid chksum: 0
┌──(root㉿kali)-[/etc/suricata]
└─# cd /etc/suricata/rules

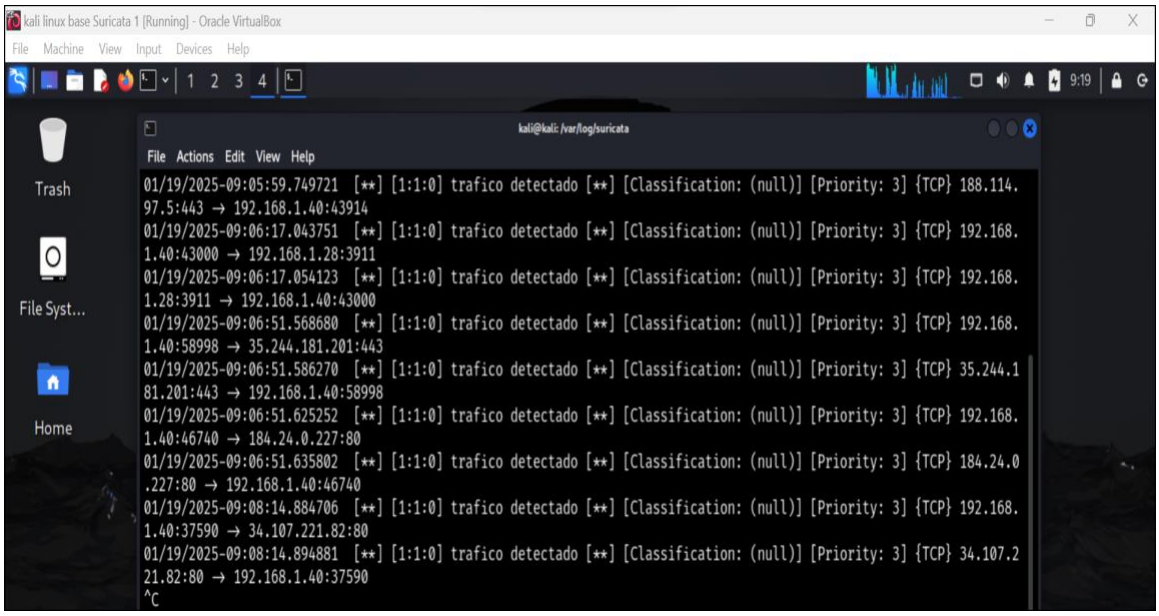

kali linux base Suricata 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:16
Trash
File Syst...
Home
root@kali: /etc/suricata/rules
File Actions Edit View Help
GNU nano 8.3 classification.config
config classification: file-dowload,Descarga de archivos detectado,2


kali linux base Suricata 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:17
Trash
File Syst...
Home
root@kali: /etc/suricata/rules
File Actions Edit View Help
GNU nano 8.3 suricata.rules
alert tcp any any → any any (msg:"trafico detectado"; sid:1;)
alert tcp any any → 192.168.1.40 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted-admin;)
alert tcp any any → any any (msg:"PDF Archivo descargado"; flow:established,to_client; fileext:"pdf"; sid:3; classt


kali linux base Suricata 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:18
Trash
File Syst...
Home
root@kali: /etc/suricata/rules
File Actions Edit View Help
^X^Ci: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 55, drops: 0 (0.00%), invalid chksum: 0
┌──(root㉿kali)-[/etc/suricata]
└─# cd /etc/suricata/rules
┌──(root㉿kali)-[/etc/suricata/rules]
└─# nano classification.config
┌──(root㉿kali)-[/etc/suricata/rules]
└─# nano classification.config
┌──(root㉿kali)-[/etc/suricata/rules]
└─# cd /suricata/ruels
cd: no such file or directory: /suricata/ruels
┌──(root㉿kali)-[/etc/suricata/rules]
└─# cd /suricata/rules
cd: no such file or directory: /suricata/rules


kali linux base Suricata 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: /etc/suricata
File Actions Edit View Help
Trash
File Syst...
Home
$ cd ..
(kali㉿kali)-[/etc/suricata]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.
^X^Ci: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 30, drops: 0 (0.00%), invalid chksum: 0
(kali㉿kali)-[/etc/suricata]
$ cd rules
(kali㉿kali)-[/etc/suricata/rules]
$ sudo nano suricata.rules
(kali㉿kali)-[/etc/suricata/rules]
$ cd ..
(kali㉿kali)-[/etc/suricata]


kali linux base Suricata 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Microsoft Word - C
https://biblus.us.es/bibing/proyectos/abreproy/11214/fichero/TOMO+I%252F05+Capitulo+5+Protoco
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
1 of 8
Automatic Zoom
Capítulo 5: Protocolo HTTP
CAPÍTULO 5: PROTOCOLO HTTP
En este proyecto, se establece que los clientes, a través de la aplicación instalada en sus terminales, accedan al servicio que le proporciona la transacción económica, de alguna forma. Puesto que tanto el servicio como el terminal móvil admiten conexiones



4. Elastic

Por último, vamos a almacenar los logs en la web Elastic.

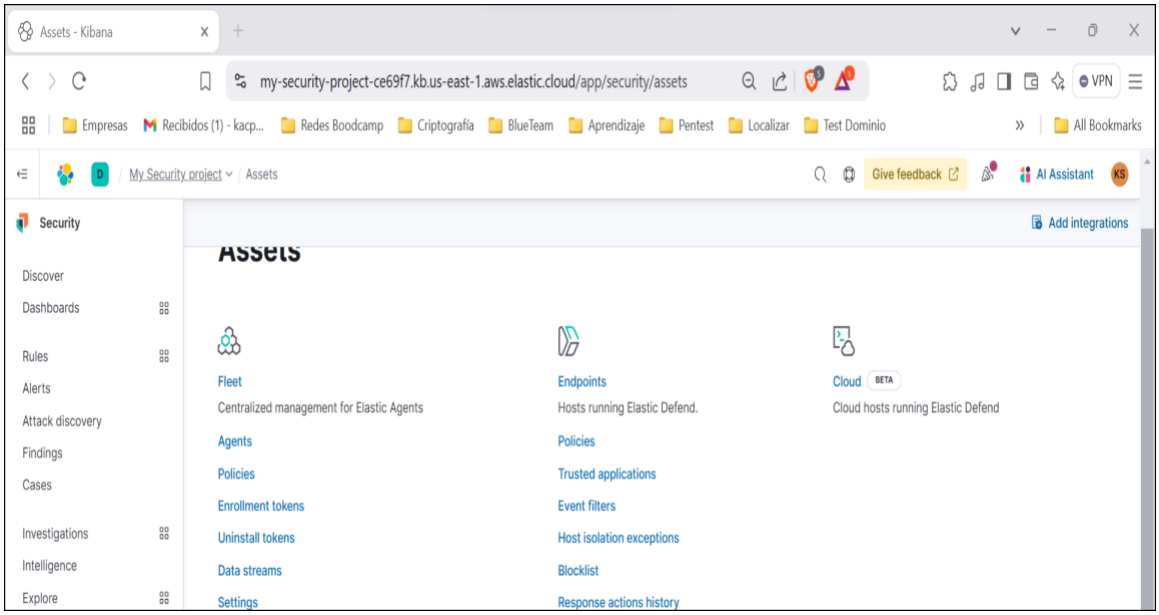
Para ello primero nos debemos de meter en la plataforma, en el apartado de Fleet, que lo que representa son las políticas del SIEM, que son un conjunto de reglas que se van aplicar a nuestros sistemas. Por ejemplo, para que un sistema operativo como kali tenga la misma configuración em toda la empresa. O podemos configurarlo por departamento, etc.

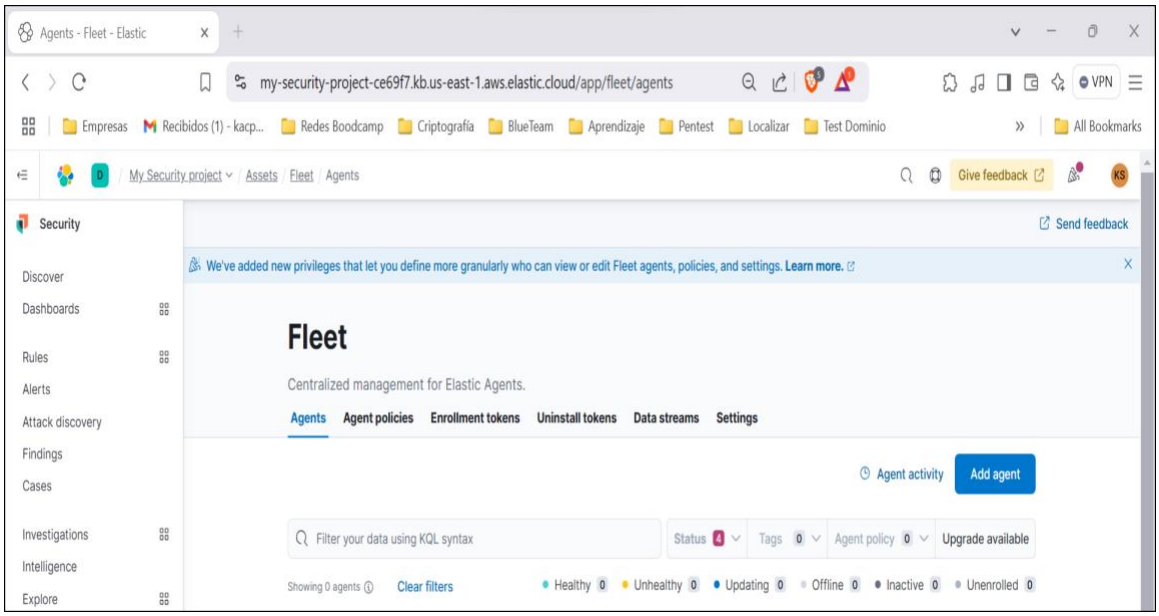
En conclusión, sirve para otorgar reglas de funcionamiento y acción.

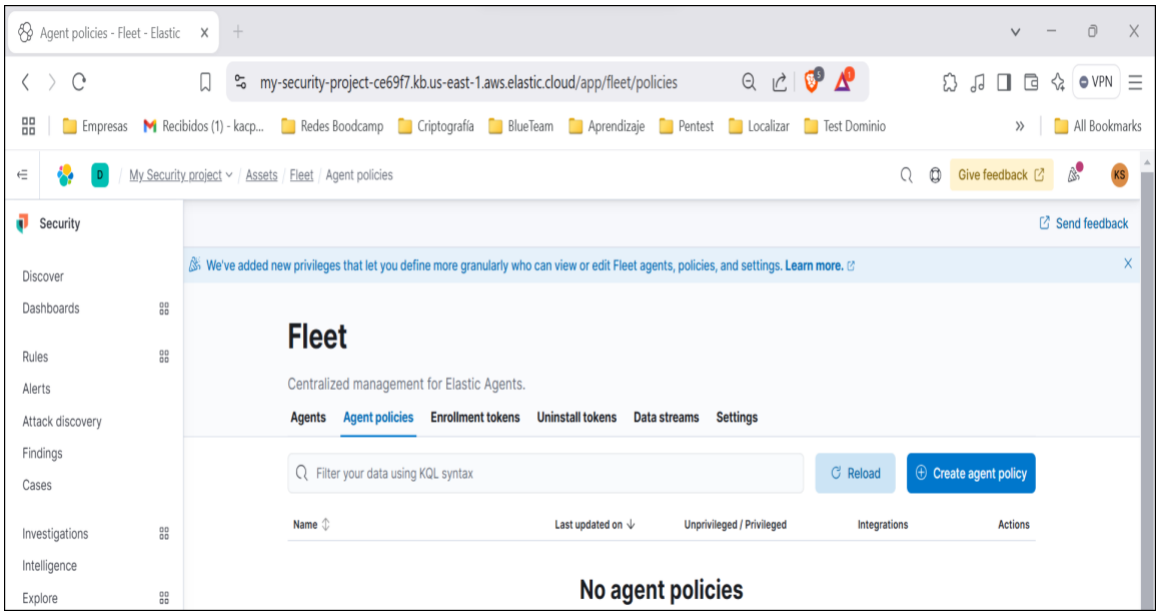
En el primer caso que vamos a crear unas reglas para Suricata. Cuando vayamos a crear la primera política aparecerá una casilla automáticamente clicada “Collect system logs and metrics” que por defecto nos va a recoger los logs generados.

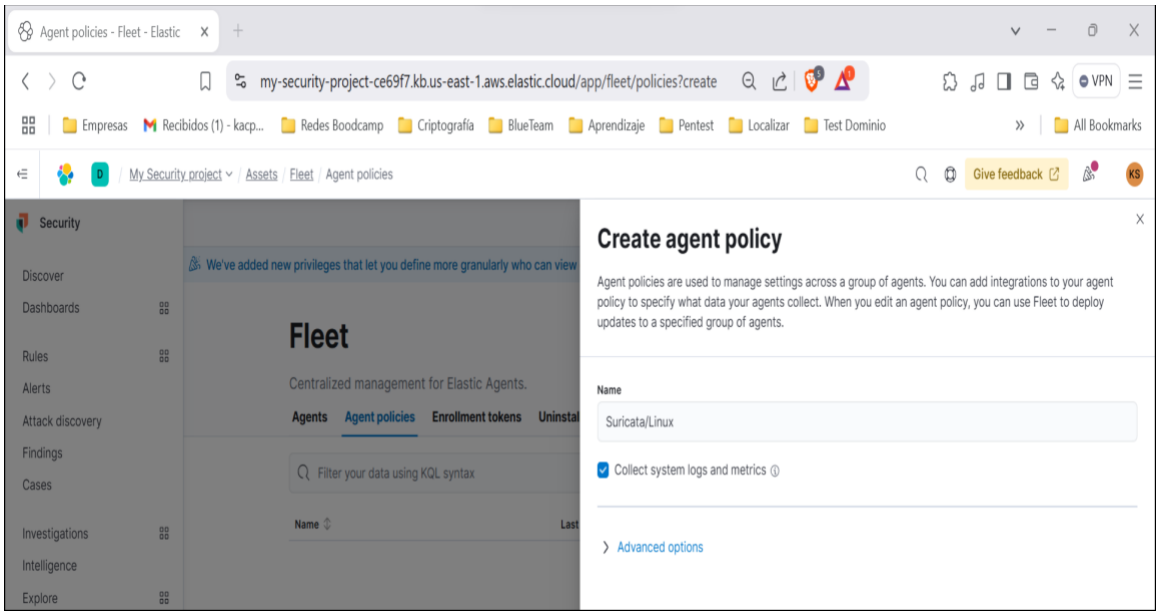
Cuando lleguemos a la parte de pegar el link que nos proporciona elastic, lo copiamos, abrimos nuestra máquina kali, y lo pegamos y ejecutamos.

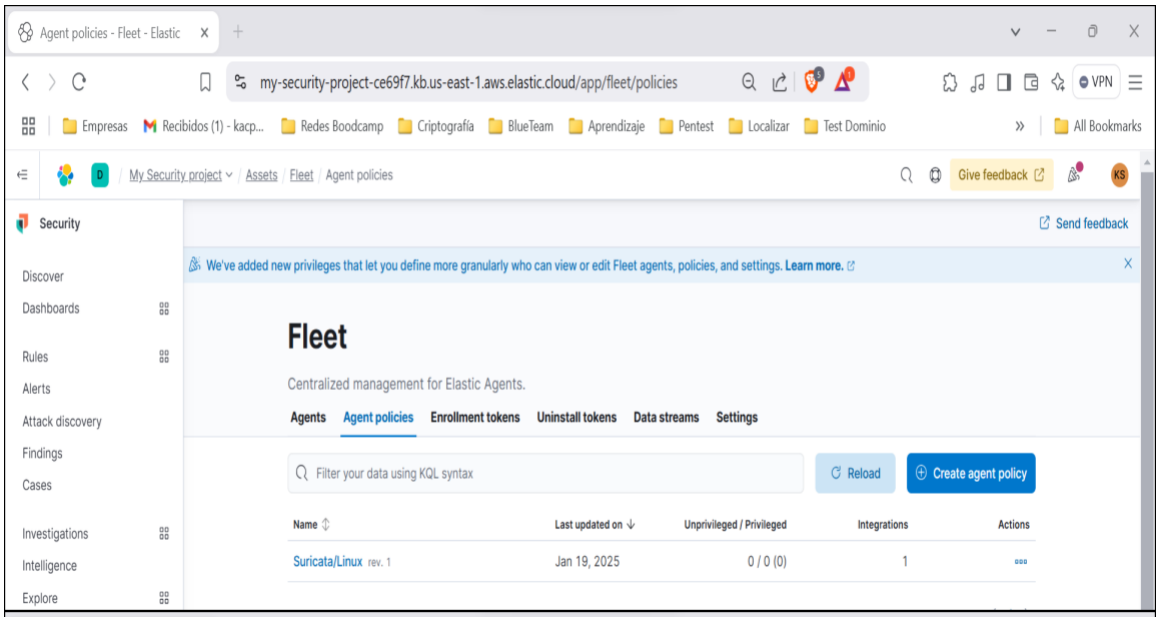
4.1. Suricata

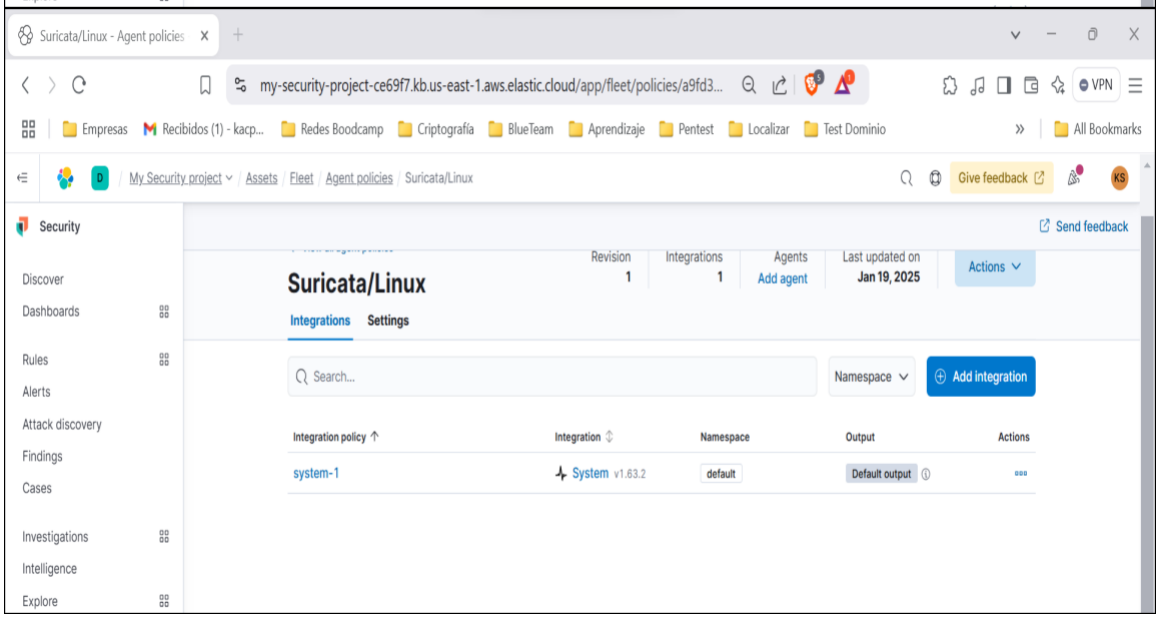

Assets - Kibana
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/security/assets
My Security project / Assets
Give feedback
AI Assistant
Security
Add integrations
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Fleet
Centralized management for Elastic Agents
Agents
Policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Endpoints
Hosts running Elastic Defend.
Policies
Trusted applications
Event filters
Host isolation exceptions
Blocklist
Response actions history
Cloud
BETA
Cloud hosts running Elastic Defend

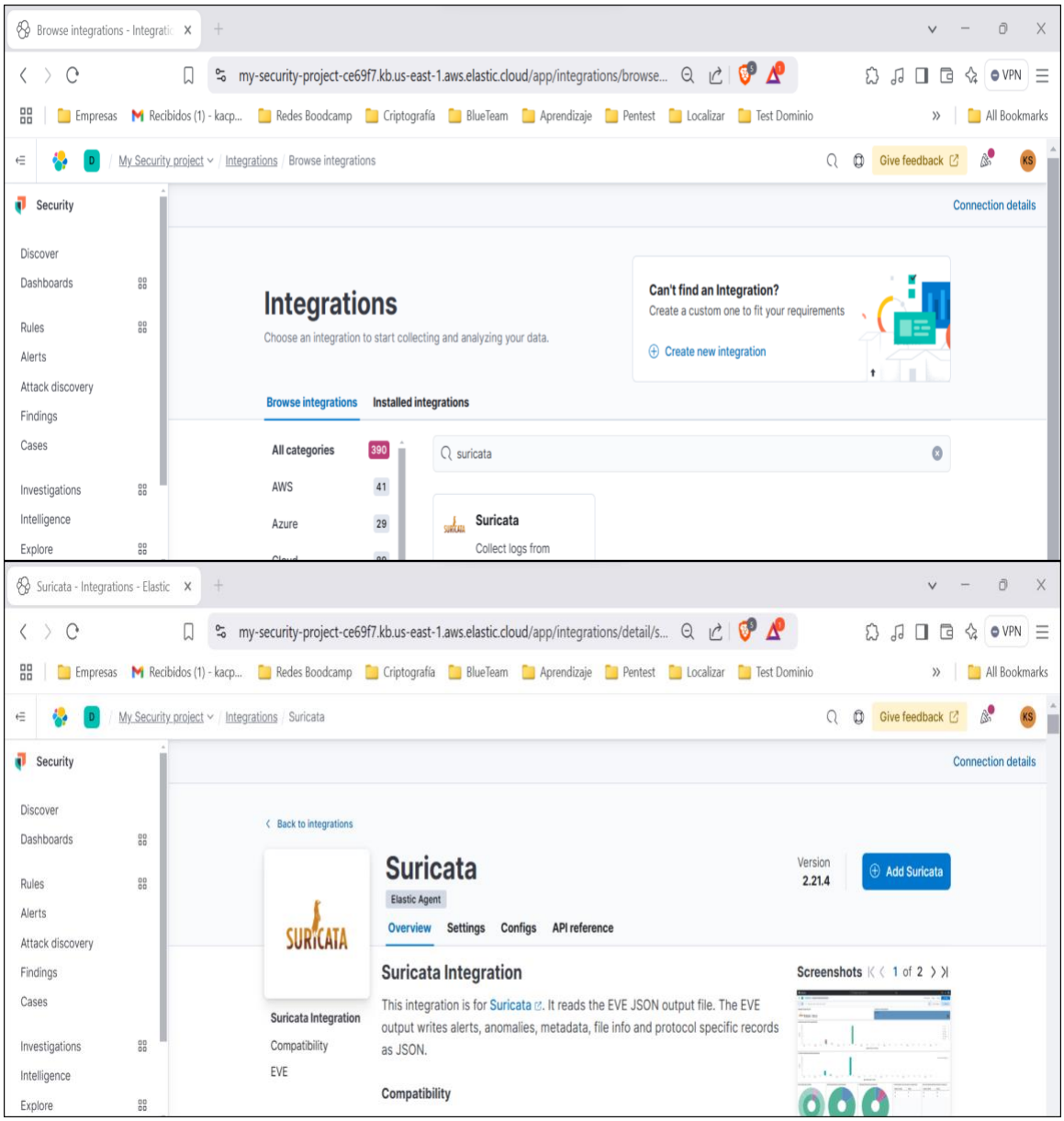

Agents - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/agents
My Security project / Assets / Fleet / Agents
Give feedback
Security
Send feedback
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Agent activity
Add agent
Filter your data using KQL syntax
Status 4
Tags 0
Agent policy 0
Upgrade available
Showing 0 agents
Clear filters
Healthy 0
Unhealthy 0
Updating 0
Offline 0
Inactive 0
Unenrolled 0


Agent policies - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
VPN
My Security project
Assets
Fleet
Agent policies
Give feedback
Send feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Filter your data using KQL syntax
Reload
Create agent policy
Name
Last updated on
Unprivileged / Privileged
Integrations
Actions
No agent policies

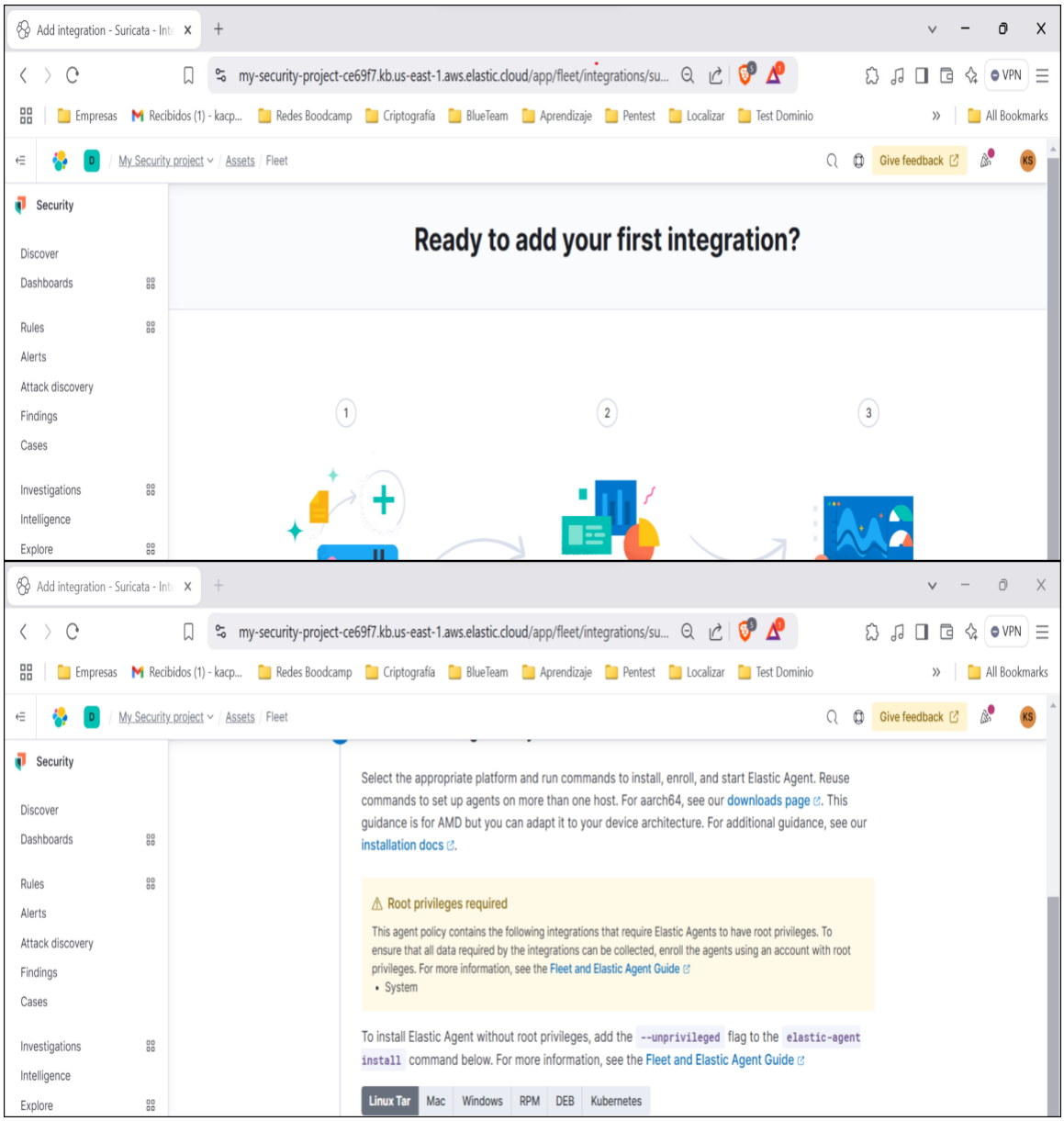

Agent policies - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies?create
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
VPN
My Security project
Assets
Fleet
Agent policies
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Filter your data using KQL syntax
Create agent policy
Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.
Name
Suricata/Linux
Collect system logs and metrics
Advanced options

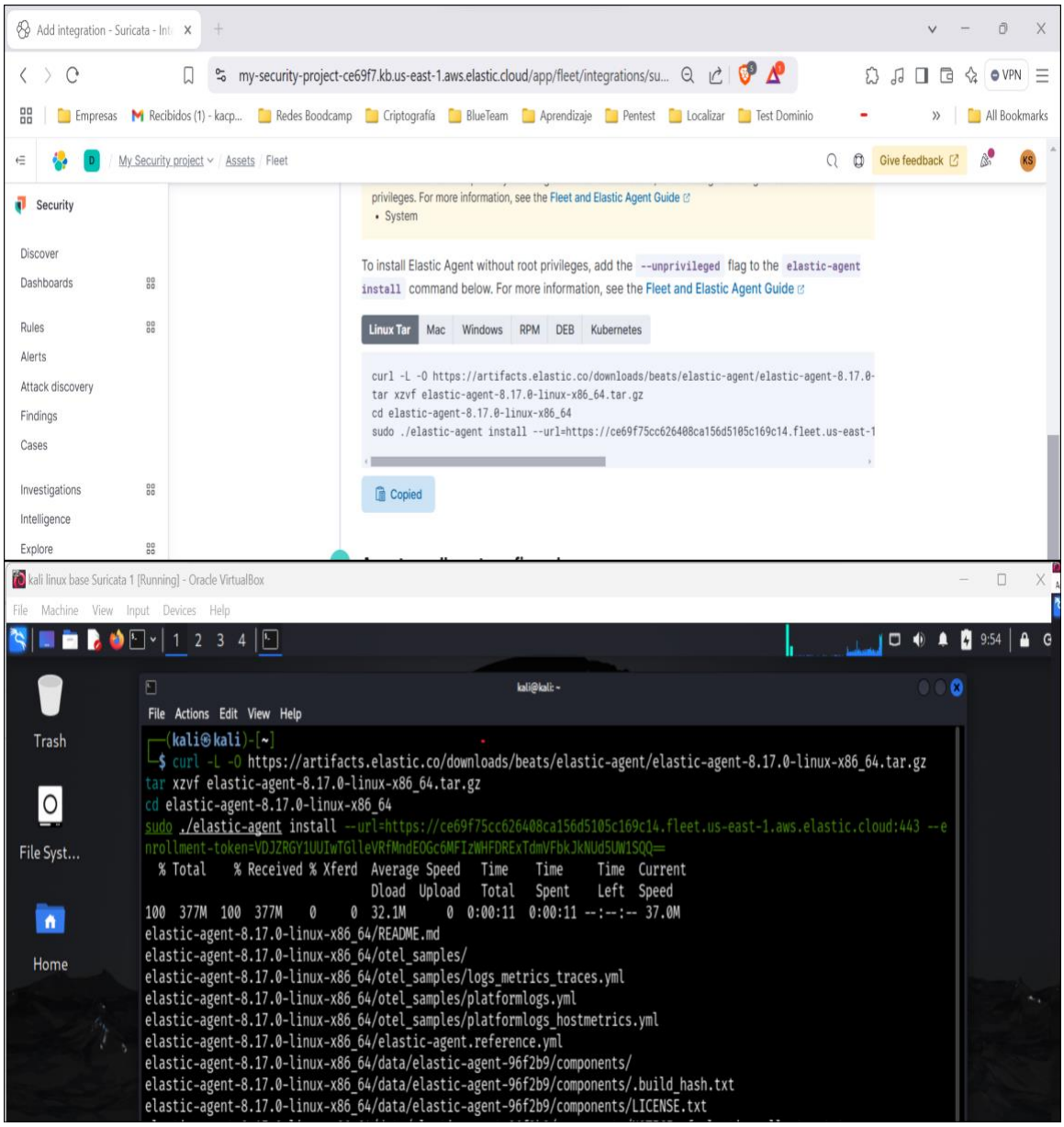

Agent policies - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project / Assets / Fleet / Agent policies
Give feedback
Send feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Filter your data using KQL syntax
Reload
Create agent policy
Name
Last updated on
Unprivileged / Privileged
Integrations
Actions
Suricata/Linux rev. 1
Jan 19, 2025
0 / 0 (0)
1


Suricata/Linux - Agent policies
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/a9fd3...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project / Assets / Fleet / Agent policies / Suricata/Linux
Give feedback
Send feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Suricata/Linux
Revision
1
Integrations
1
Agents
Add agent
Last updated on
Jan 19, 2025
Actions
Integrations
Settings
Search...
Namespace
Add integration
Integration policy
Integration
Namespace
Output
Actions
system-1
System v1.63.2
default
Default output

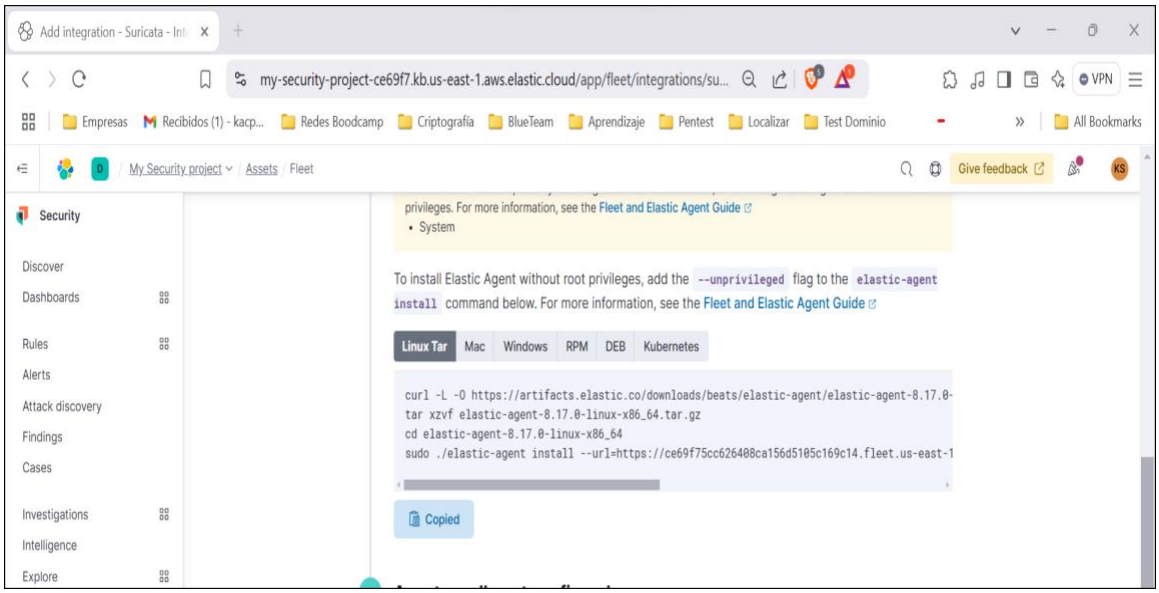

Browse integrations - Integratic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/browse...
VPN
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Integrations
Browse integrations
Give feedback
KS
Security
Connection details
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Integrations
Choose an integration to start collecting and analyzing your data.
Can't find an Integration?
Create a custom one to fit your requirements
Create new integration
Browse integrations
Installed integrations
All categories
390
AWS
41
Azure
29
suricata
Suricata
Collect logs from

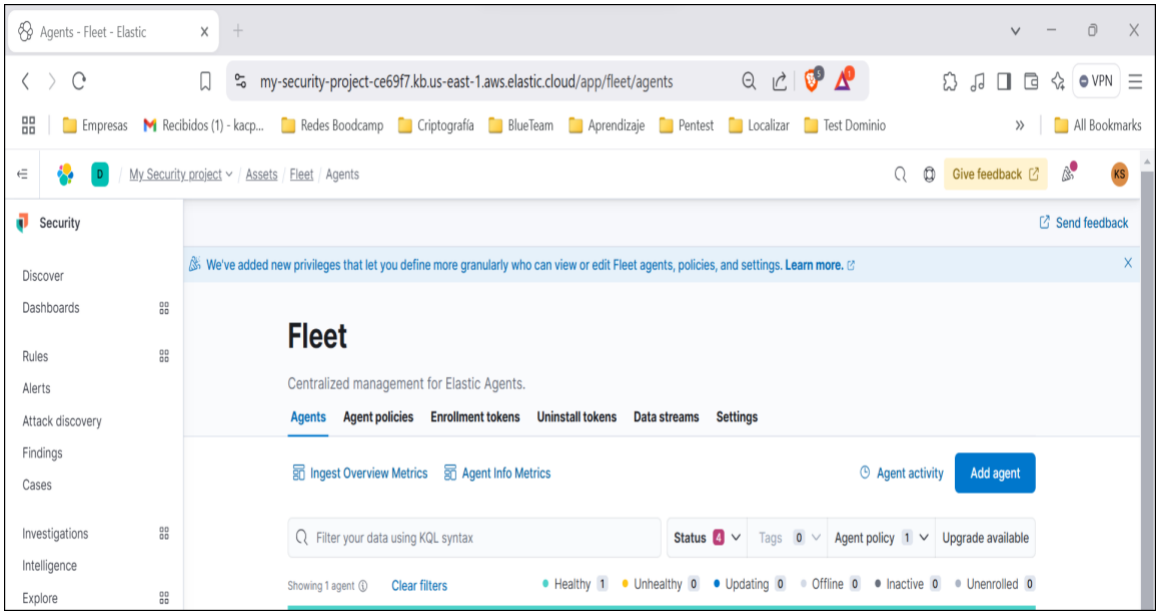
Suricata - Integrations - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/detail/s...
VPN
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Integrations
Suricata
Give feedback
KS
Security
Connection details
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Back to integrations
Suricata
Elastic Agent
Version
2.21.4
Add Suricata
Overview
Settings
Configs
API reference
Suricata Integration
Compatibility
EVE
Suricata Integration
This integration is for Suricata. It reads the EVE JSON output file. The EVE output writes alerts, anomalies, metadata, file info and protocol specific records as JSON.
Compatibility
Screenshots
1 of 2

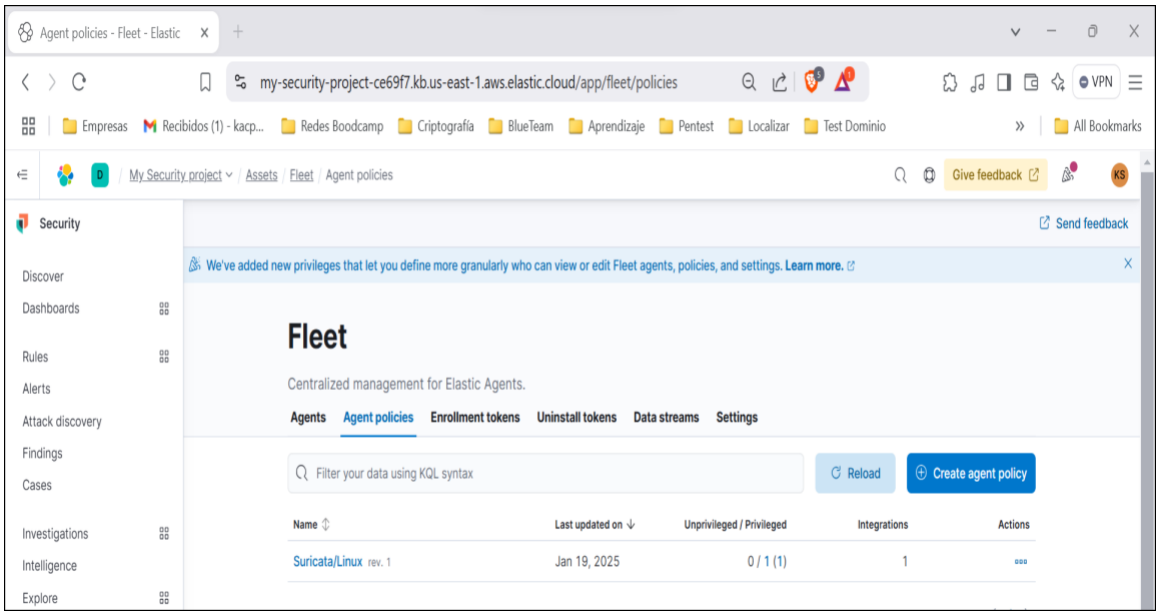

Add integration - Suricata - Int
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/su...
VPN
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
KS
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Ready to add your first integration?
1
2
3
Add integration - Suricata - Int
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/su...
VPN
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
KS
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation docs.
Root privileges required
This agent policy contains the following integrations that require Elastic Agents to have root privileges. To ensure that all data required by the integrations can be collected, enroll the agents using an account with root privileges. For more information, see the Fleet and Elastic Agent Guide
System
To install Elastic Agent without root privileges, add the --unprivileged flag to the elastic-agent install command below. For more information, see the Fleet and Elastic Agent Guide
Linux Tar
Mac
Windows
RPM
DEB
Kubernetes

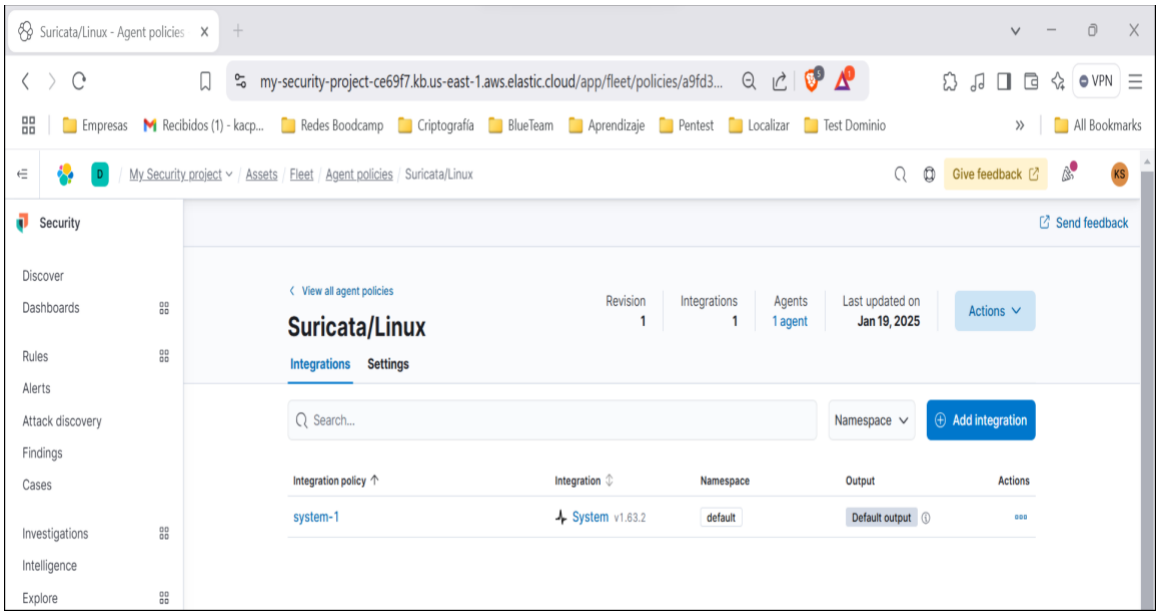

Add integration - Suricata - Int
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/su...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
privileges. For more information, see the Fleet and Elastic Agent Guide
System
To install Elastic Agent without root privileges, add the --unprivileged flag to the elastic-agent install command below. For more information, see the Fleet and Elastic Agent Guide
Linux Tar
Mac
Windows
RPM
DEB
Kubernetes
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
cd elastic-agent-8.17.0-linux-x86_64
sudo ./elastic-agent install --url=https://ce69f75cc626408ca156d5105c169c14.fleet.us-east-1
Copied

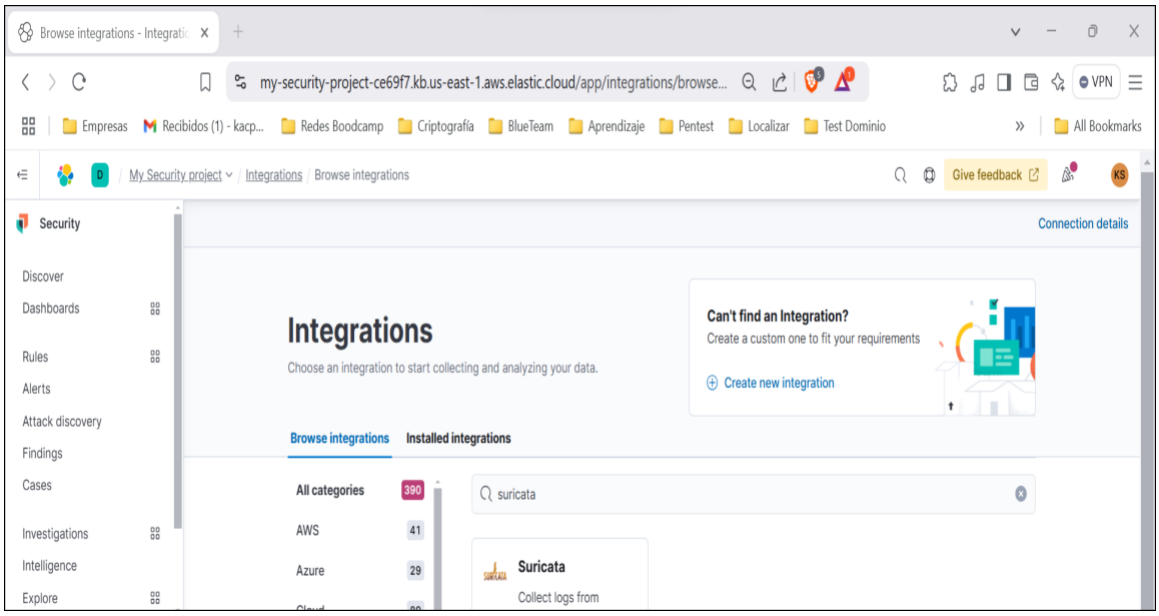
kali linux base Suricata 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:54
Trash
File Syst...
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
cd elastic-agent-8.17.0-linux-x86_64
sudo ./elastic-agent install --url=https://ce69f75cc626408ca156d5105c169c14.fleet.us-east-1.aws.elastic.cloud:443 --enrollment-token=VDJZRGY1UUIwTGlleVRfMndEOGc6MFIzWHFDRExTdmVFbkJkNUd5UW1SQQ==
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 377M 100 377M 0 0 32.1M 0 0:00:11 0:00:11 --:--:-- 37.0M
elastic-agent-8.17.0-linux-x86_64/README.md
elastic-agent-8.17.0-linux-x86_64/otel_samples/
elastic-agent-8.17.0-linux-x86_64/otel_samples/logs_metrics_traces.yml
elastic-agent-8.17.0-linux-x86_64/otel_samples/platformlogs.yml
elastic-agent-8.17.0-linux-x86_64/otel_samples/platformlogs_hostmetrics.yml
elastic-agent-8.17.0-linux-x86_64/elastic-agent.reference.yml
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b9/components/
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b9/components/.build_hash.txt
elastic-agent-8.17.0-linux-x86_64/data/elastic-agent-96f2b9/components/LICENSE.txt

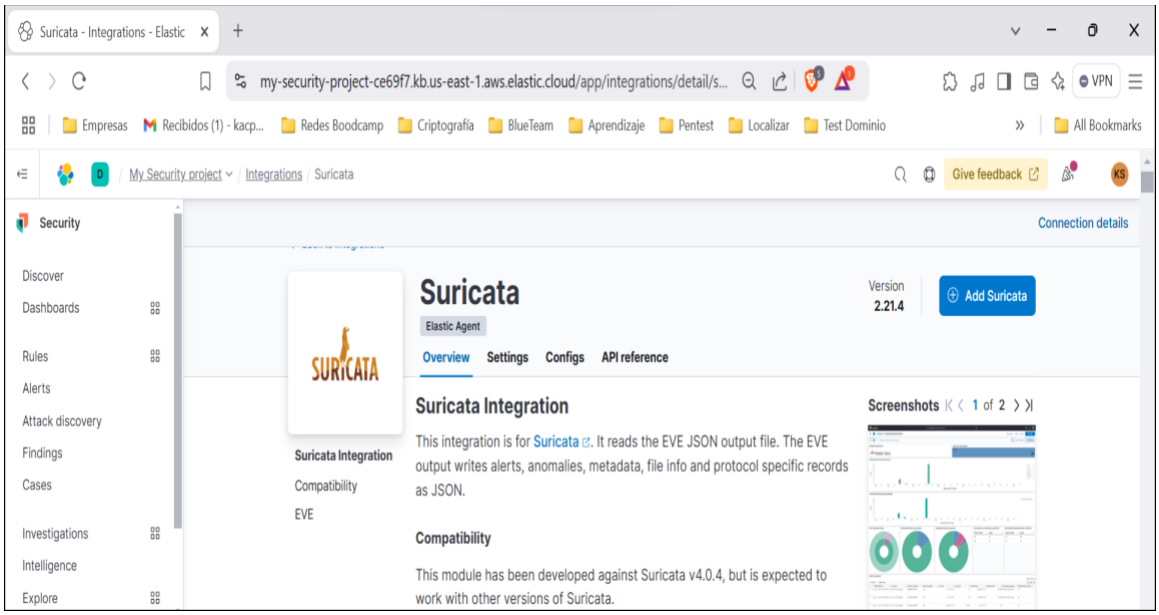

Add integration - Suricata - Int
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/su...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
privileges. For more information, see the Fleet and Elastic Agent Guide
System
To install Elastic Agent without root privileges, add the --unprivileged flag to the elastic-agent install command below. For more information, see the Fleet and Elastic Agent Guide
Linux Tar
Mac
Windows
RPM
DEB
Kubernetes
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
cd elastic-agent-8.17.0-linux-x86_64
sudo ./elastic-agent install --url=https://ce69f75cc626408ca156d5105c169c14.fleet.us-east-1
Copied

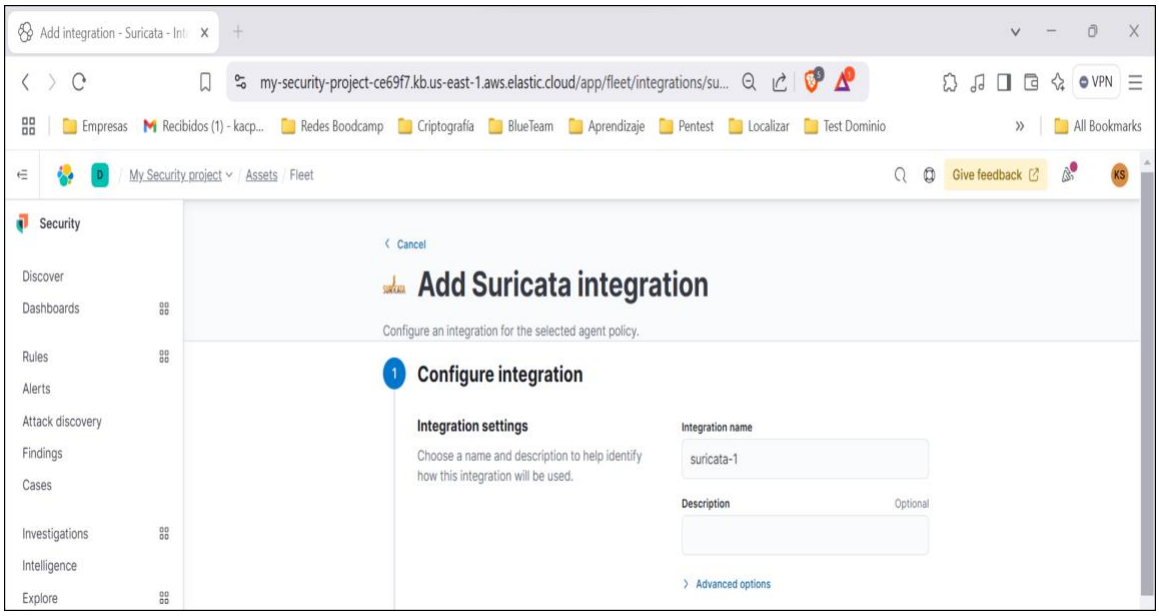

Agents - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/agents
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agents
Give feedback
Security
Send feedback
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
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 agent
Filter your data using KQL syntax
Status
Tags
Agent policy
Upgrade available
Showing 1 agent
Clear filters
Healthy 1
Unhealthy 0
Updating 0
Offline 0
Inactive 0
Unenrolled 0

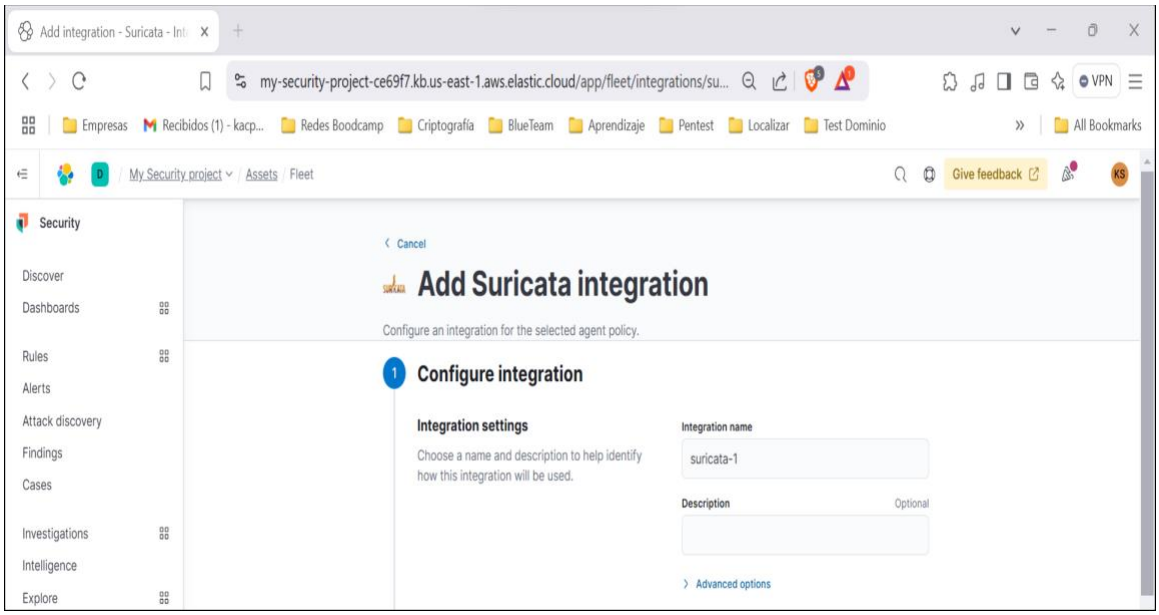

Agent policies - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agent policies
Give feedback
Security
Send feedback
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Filter your data using KQL syntax
Reload
Create agent policy
Name
Last updated on
Unprivileged / Privileged
Integrations
Actions
Suricata/Linux rev. 1
Jan 19, 2025
0 / 1 (1)
1

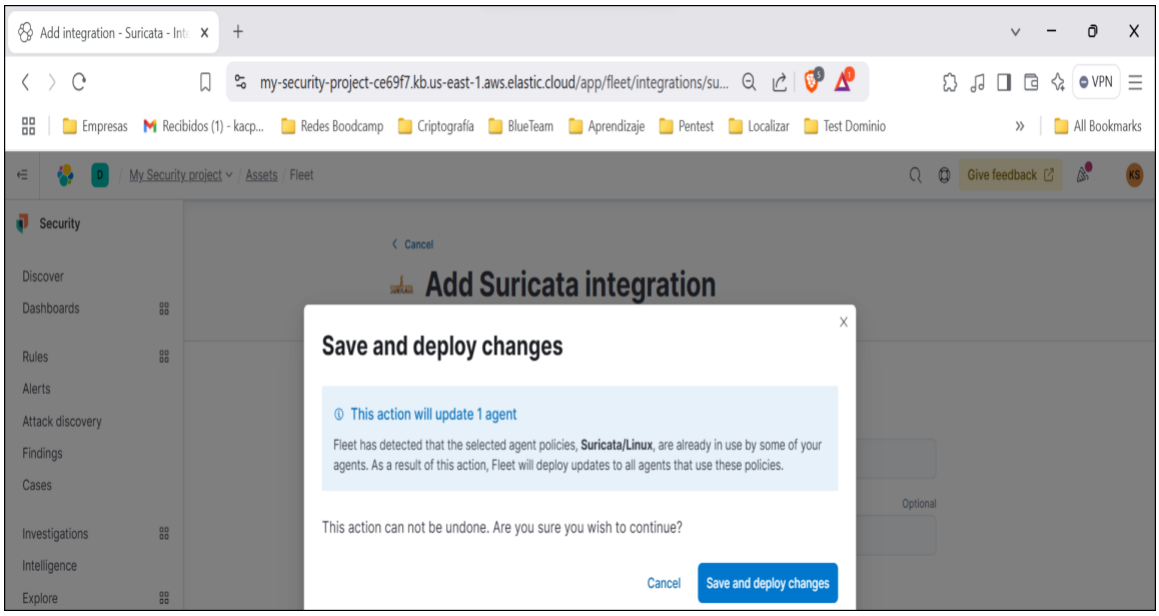

Suricata/Linux - Agent policies
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/a9fd3...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agent policies
Suricata/Linux
Give feedback
Security
Send feedback
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
View all agent policies
Suricata/Linux
Revision
1
Integrations
1
Agents
1 agent
Last updated on
Jan 19, 2025
Actions
Integrations
Settings
Search...
Namespace
Add integration
Integration policy
Integration
Namespace
Output
Actions
system-1
System v1.63.2
default
Default output

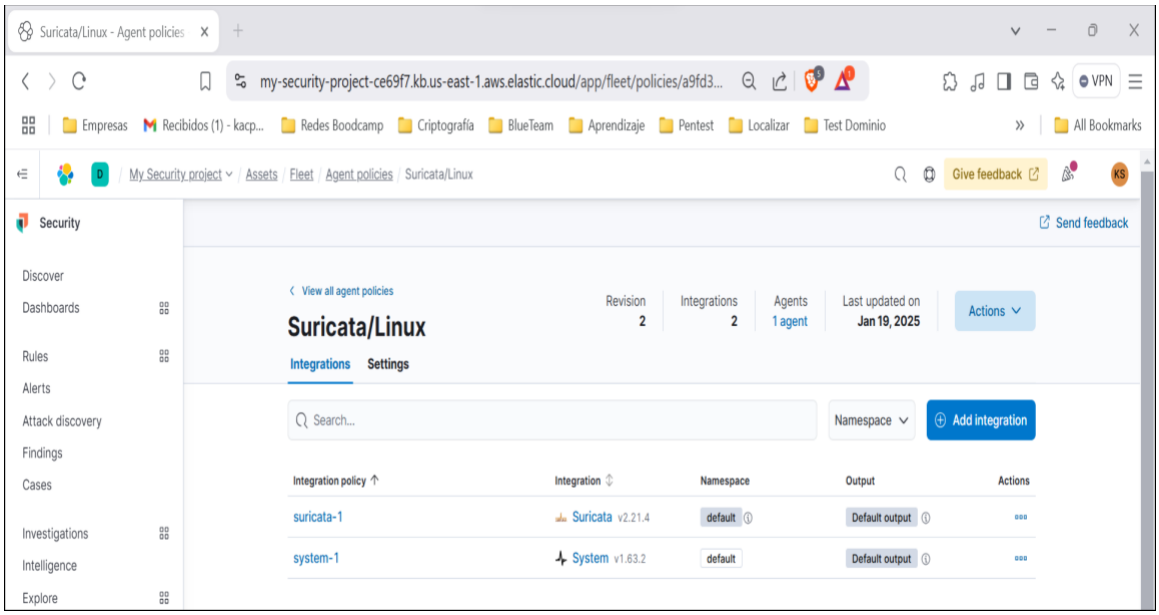

Browse integrations - Integratic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/browse...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Integrations
Browse integrations
Give feedback
Security
Connection details
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Integrations
Choose an integration to start collecting and analyzing your data.
Can't find an Integration?
Create a custom one to fit your requirements
Create new integration
Browse integrations
Installed integrations
All categories
390
AWS
41
Azure
29
suricata
Suricata
Collect logs from

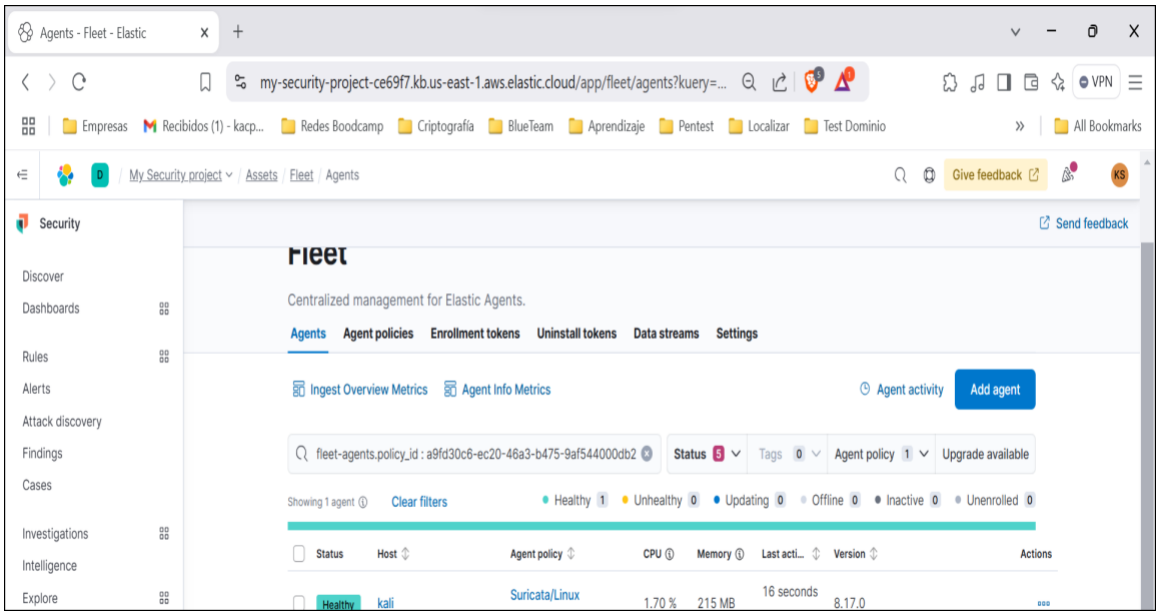

Suricata - Integrations - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/detail/s...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Integrations
Suricata
Give feedback
Security
Connection details
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Suricata
Elastic Agent
Version
2.21.4
Add Suricata
Overview
Settings
Configs
API reference
Suricata Integration
Compatibility
EVE
Suricata Integration
This integration is for Suricata. It reads the EVE JSON output file. The EVE output writes alerts, anomalies, metadata, file info and protocol specific records as JSON.
Compatibility
This module has been developed against Suricata v4.0.4, but is expected to work with other versions of Suricata.
Screenshots
1 of 2

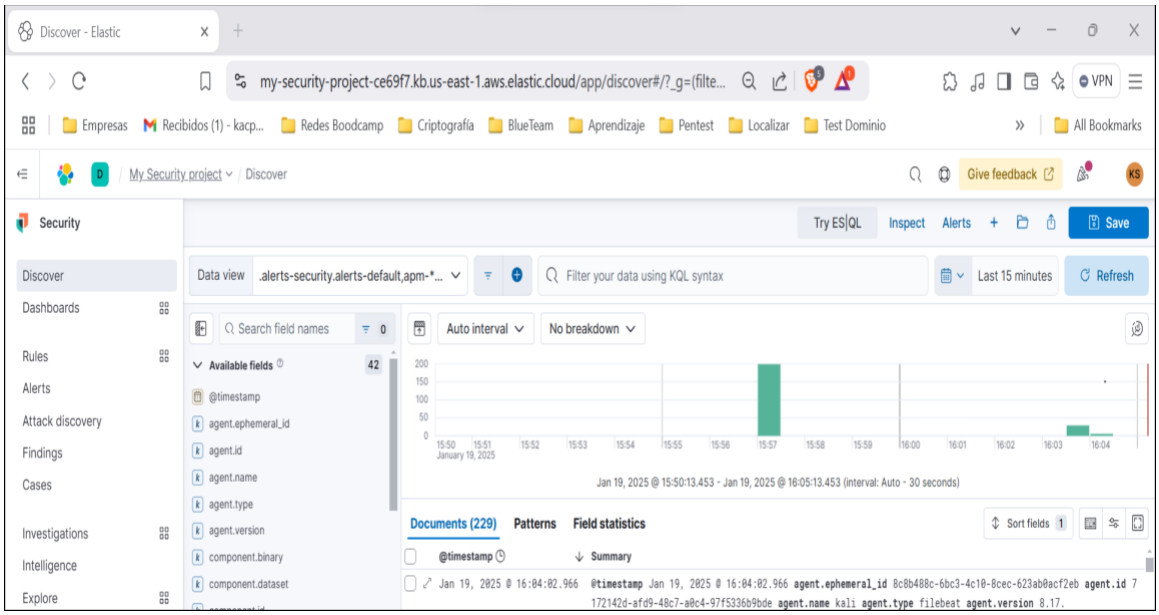

Add integration - Suricata - Int
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/su...
VPN
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
KS
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Cancel
Add Suricata integration
Configure an integration for the selected agent policy.
1
Configure integration
Integration settings
Choose a name and description to help identify how this integration will be used.
Integration name
suricata-1
Description
Optional
Advanced options


Add integration - Suricata - Int
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/su...
VPN
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
KS
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Cancel
Add Suricata integration
Configure an integration for the selected agent policy.
1
Configure integration
Integration settings
Choose a name and description to help identify how this integration will be used.
Integration name
suricata-1
Description
Optional
Advanced options


Add integration - Suricata - Int
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/su...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Cancel
Add Suricata integration
Save and deploy changes
This action will update 1 agent
Fleet has detected that the selected agent policies, Suricata/Linux, are already in use by some of your agents. As a result of this action, Fleet will deploy updates to all agents that use these policies.
This action can not be undone. Are you sure you wish to continue?
Cancel
Save and deploy changes
Optional


Suricata/Linux - Agent policies
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/a9fd3...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agent policies
Suricata/Linux
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Send feedback
View all agent policies
Suricata/Linux
Revision 2
Integrations 2
Agents 1 agent
Last updated on Jan 19, 2025
Actions
Integrations
Settings
Search...
Namespace
Add integration
Integration policy
Integration
Namespace
Output
Actions
suricata-1
Suricata v2.21.4
default
Default output
system-1
System v1.63.2
default
Default output





Ejemplo:


```
{
 "@timestamp": [
  "2025-01-19T15:37:22.952Z"
 ],
 "agent.ephemeral_id": [
  "06a43a1d-699c-40c9-9b07-3dee85e78bcd"
```

```
],
"agent.id": [
  "7172142d-afd9-48c7-a0c4-97f5336b9bde"
],
"agent.name": [
  "kali"
],
"agent.type": [
  "filebeat"
],
"agent.version": [
  "8.17.0"
],
"component.id": [
  "log-default"
],
"component.state": [
  "HEALTHY"
],
"container.id": [
  "elastic-agent-8.17.0-96f2b9"
],
"data_stream.dataset": [
  "elastic_agent"
],
"data_stream.namespace": [
```

```
  "default"
],
"data_stream.type": [
  "logs"
],
"ecs.version": [
  "8.0.0"
],
"elastic_agent.id": [
  "7172142d-afd9-48c7-a0c4-97f5336b9bde"
],
"elastic_agent.snapshot": [
  false
],
"elastic_agent.version": [
  "8.17.0"
],
"event.agent_id_status": [
  "verified"
],
"event.dataset": [
  "elastic_agent"
],
"event.ingested": [
  "2025-01-19T15:37:38.000Z"
],
```

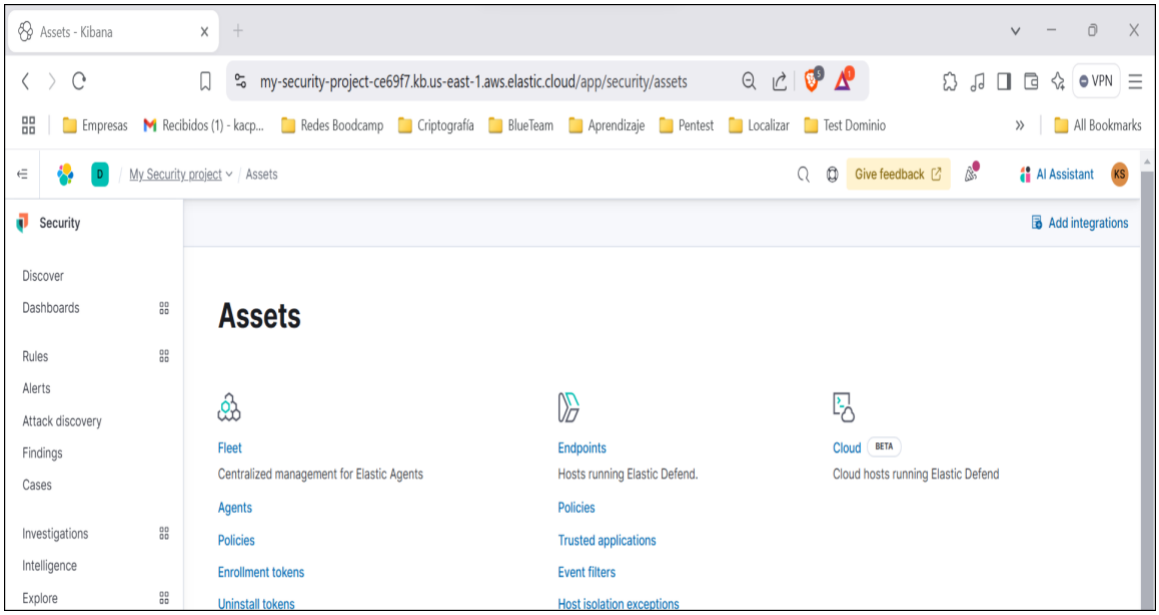
```
"host.architecture": [
  "x86_64"
],
"host.containerized": [
  false
],
"host.hostname": [
  "kali"
],
"host.id": [
  "55e5305955694ed3b6c7506b1268fad8"
],
"host.ip": [
  "192.168.1.40",
  "fe80::a414:97ff:512:c48b",
  "172.17.0.1"
],
"host.mac": [
  "02-42-86-07-EA-9E",
  "08-00-27-DF-0F-2D"
],
"host.name": [
  "kali"
],
"host.os.codename": [
  "kali-rolling"
```

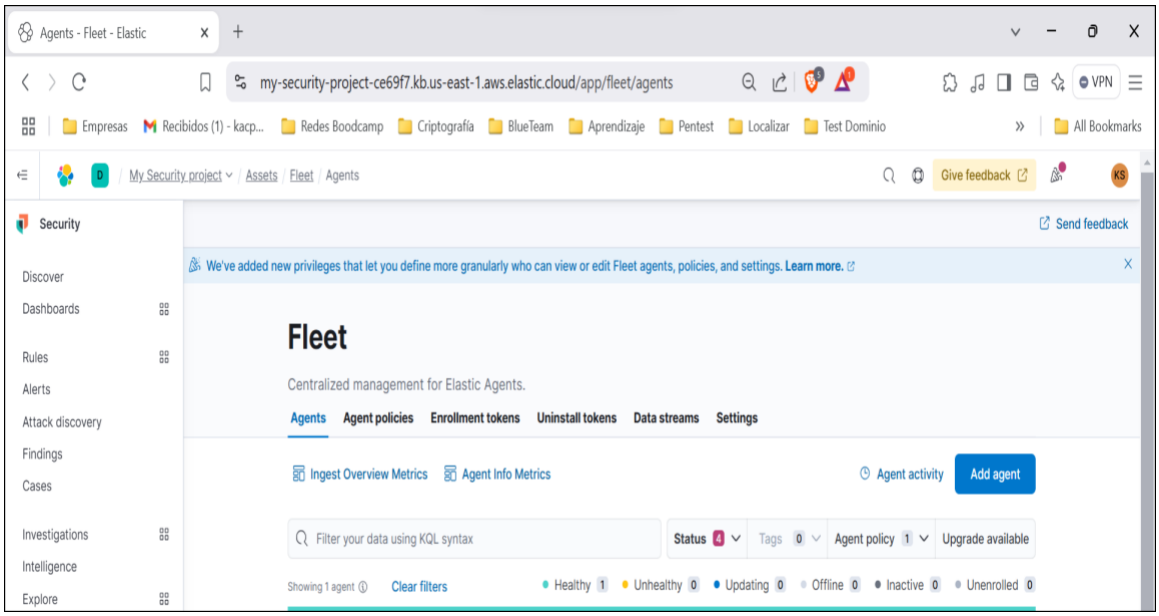
```
],
"host.os.family": [
  "debian"
],
"host.os.kernel": [
  "6.11.2-amd64"
],
"host.os.name": [
  "Kali GNU/Linux"
],
"host.os.name.text": [
  "Kali GNU/Linux"
],
"host.os.platform": [
  "kali"
],
"host.os.type": [
  "linux"
],
"host.os.version": [
  "2024.4"
],
"input.type": [
  "filestream"
],
"log.file.device_id": [
```

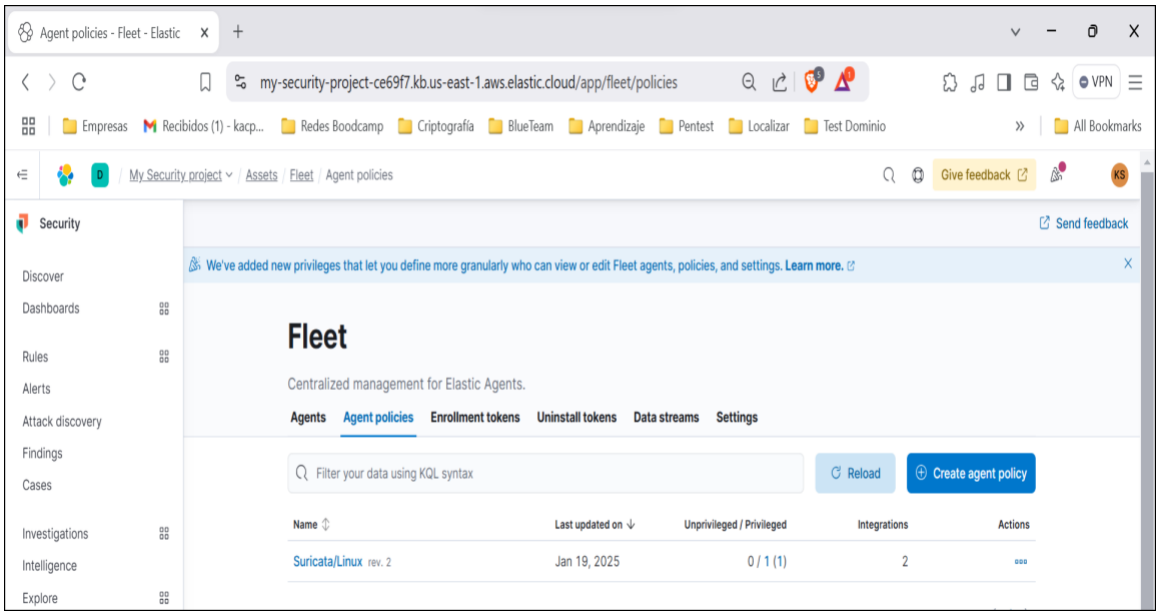
```
  "2049"
 ],
 "log.file.inode": [
  "1836133"
 ],
 "log.file.path": [
  "/opt/Elastic/Agent/data/elastic-agent-8.17.0-96f2b9/logs/elastic-agent-20250119-2.ndjson"
 ],
 "log.level": [
  "info"
 ],
 "log.offset": [
  78081
 ],
 "log.origin.file.line": [
  663
 ],
 "log.origin.file.name": [
  "coordinator/coordinator.go"
 ],
 "log.origin.function": [
  "github.com/elastic/elastic-agent/internal/pkg/agent/application/coordinator.(*Coordinator).watchRuntimeComponents"
 ],
 "log.source": [
```

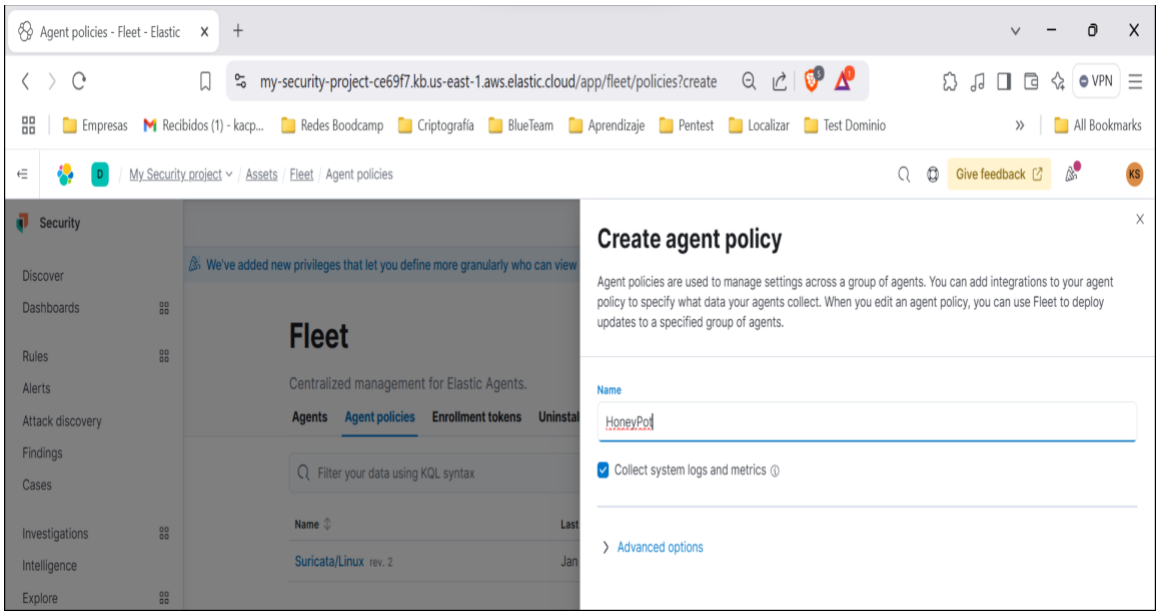
```
    "elastic-agent"
  ],
  "message": [
    "Unit state changed log-default-logfile-suricata-4219fd77-11b9-4bf6-9a49-0e43da5419e1 (STARTING->HEALTHY): Healthy"
  ],
  "unit.id": [
    "log-default-logfile-suricata-4219fd77-11b9-4bf6-9a49-0e43da5419e1"
  ],
  "unit.old_state": [
    "STARTING"
  ],
  "unit.state": [
    "HEALTHY"
  ],
  "unit.type": [
    "input"
  ],
  "_id": "AZR_NrR0sttFzmZkTyyt",
  "_index": ".ds-logs-elastic_agent-default-2025.01.19-000001",
  "_score": null
}
```

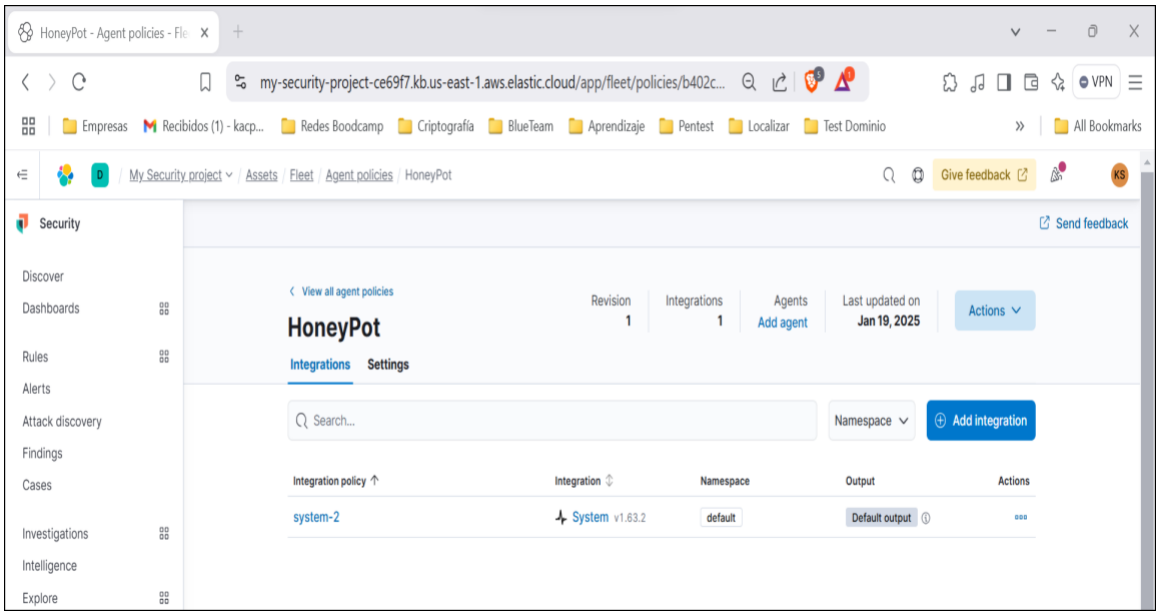
4.2. HoneyPot

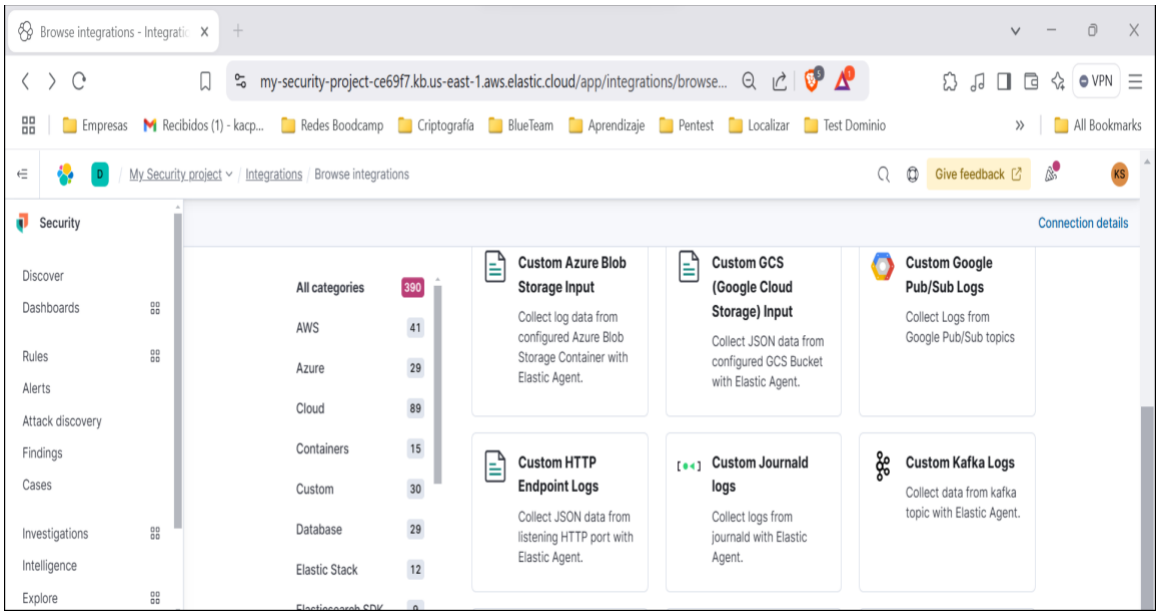

Assets - Kibana
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/security/assets
My Security project / Assets
Give feedback
AI Assistant
Security
Add integrations
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Fleet
Centralized management for Elastic Agents
Agents
Policies
Enrollment tokens
Uninstall tokens
Endpoints
Hosts running Elastic Defend.
Policies
Trusted applications
Event filters
Host isolation exceptions
Cloud
BETA
Cloud hosts running Elastic Defend

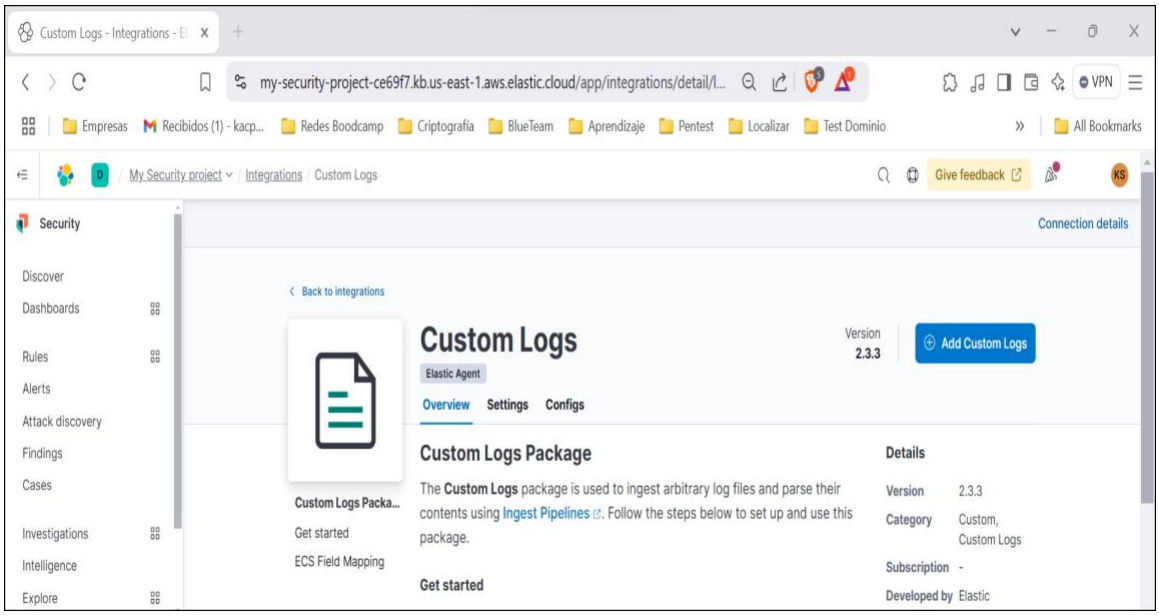

Agents - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/agents
My Security project / Assets / Fleet / Agents
Give feedback
Security
Send feedback
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
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 agent
Filter your data using KQL syntax
Status
Tags
Agent policy
Upgrade available
Showing 1 agent
Clear filters
Healthy 1
Unhealthy 0
Updating 0
Offline 0
Inactive 0
Unenrolled 0

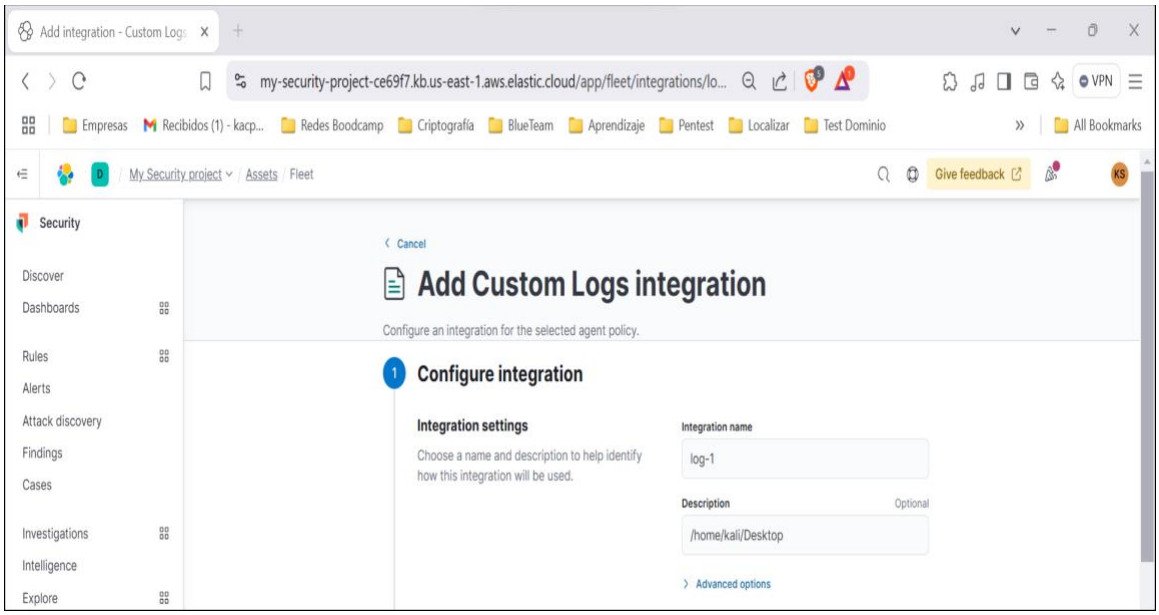

Agent policies - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
VPN
My Security project
Assets
Fleet
Agent policies
Give feedback
Send feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Filter your data using KQL syntax
Reload
Create agent policy
Name
Last updated on
Unprivileged / Privileged
Integrations
Actions
Suricata/Linux rev. 2
Jan 19, 2025
0 / 1 (1)
2

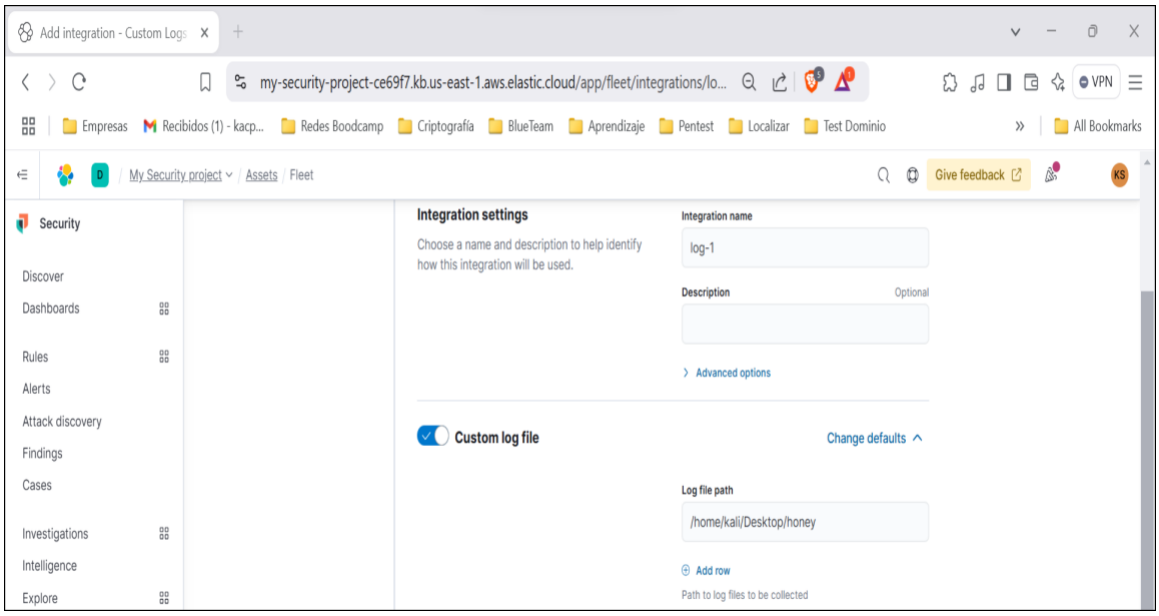

Agent policies - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies?create
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
VPN
My Security project
Assets
Fleet
Agent policies
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Filter your data using KQL syntax
Suricata/Linux rev. 2
Create agent policy
Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.
Name
HoneyPot
Collect system logs and metrics
Advanced options

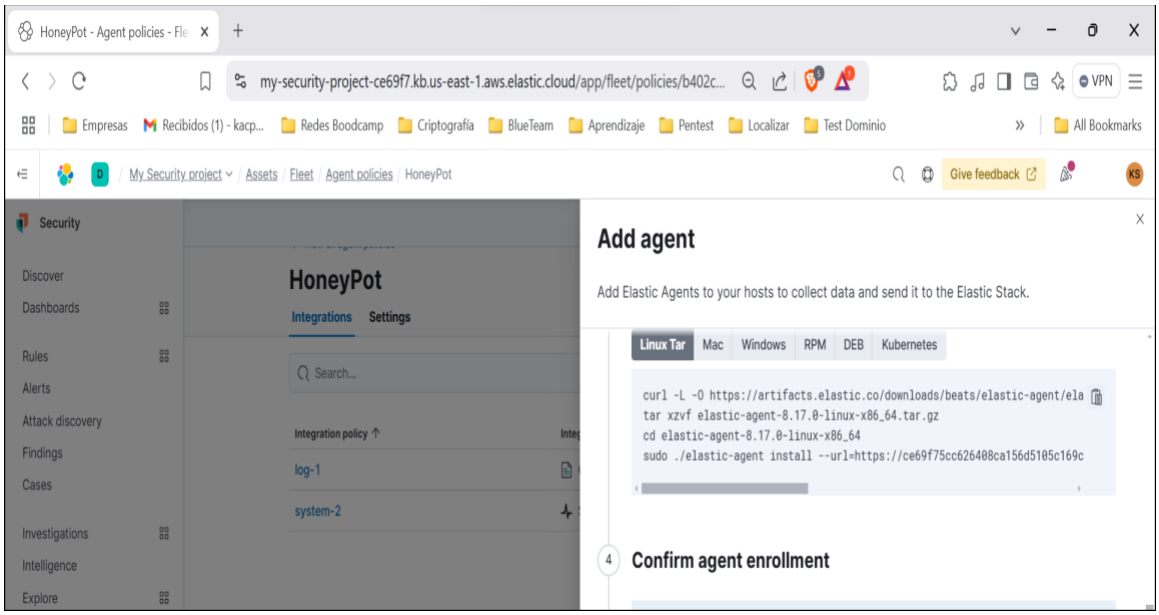

HoneyPot - Agent policies - Fle
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/b402c...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agent policies
HoneyPot
Give feedback
Send feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
View all agent policies
HoneyPot
Revision
1
Integrations
1
Agents
Add agent
Last updated on
Jan 19, 2025
Actions
Integrations
Settings
Search...
Namespace
Add integration
Integration policy
Integration
Namespace
Output
Actions
system-2
System v1.63.2
default
Default output

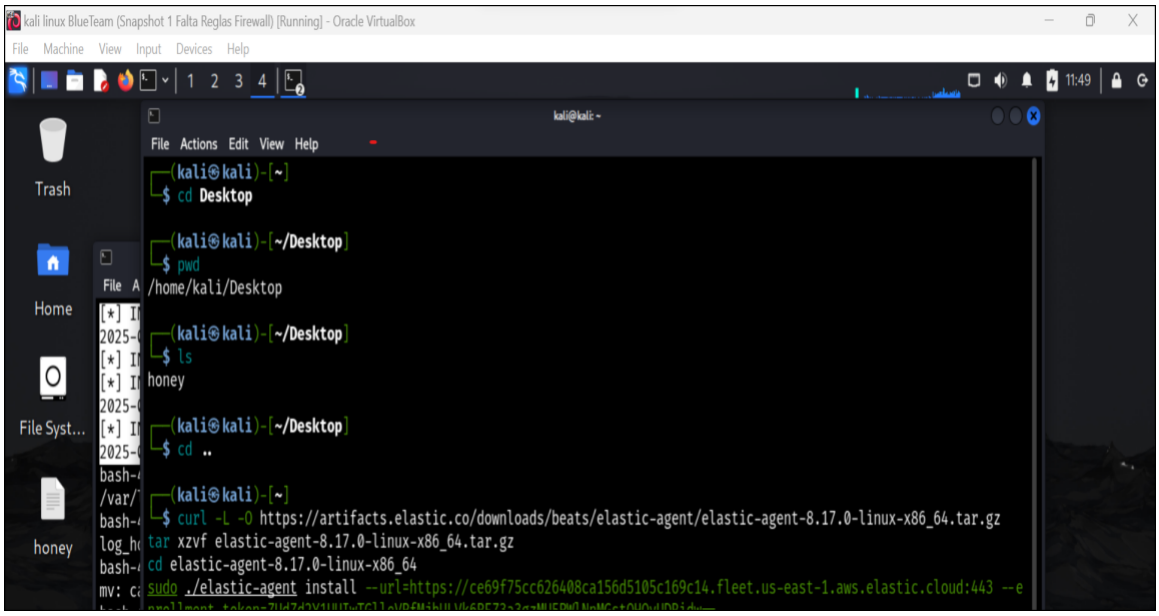

Browse integrations - Integratic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/browse...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Integrations
Browse integrations
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Connection details
All categories 390
AWS 41
Azure 29
Cloud 89
Containers 15
Custom 30
Database 29
Elastic Stack 12
Custom Azure Blob Storage Input
Collect log data from configured Azure Blob Storage Container with Elastic Agent.
Custom GCS (Google Cloud Storage) Input
Collect JSON data from configured GCS Bucket with Elastic Agent.
Custom Google Pub/Sub Logs
Collect Logs from Google Pub/Sub topics
Custom HTTP Endpoint Logs
Collect JSON data from listening HTTP port with Elastic Agent.
Custom Journald logs
Collect logs from journald with Elastic Agent.
Custom Kafka Logs
Collect data from kafka topic with Elastic Agent.

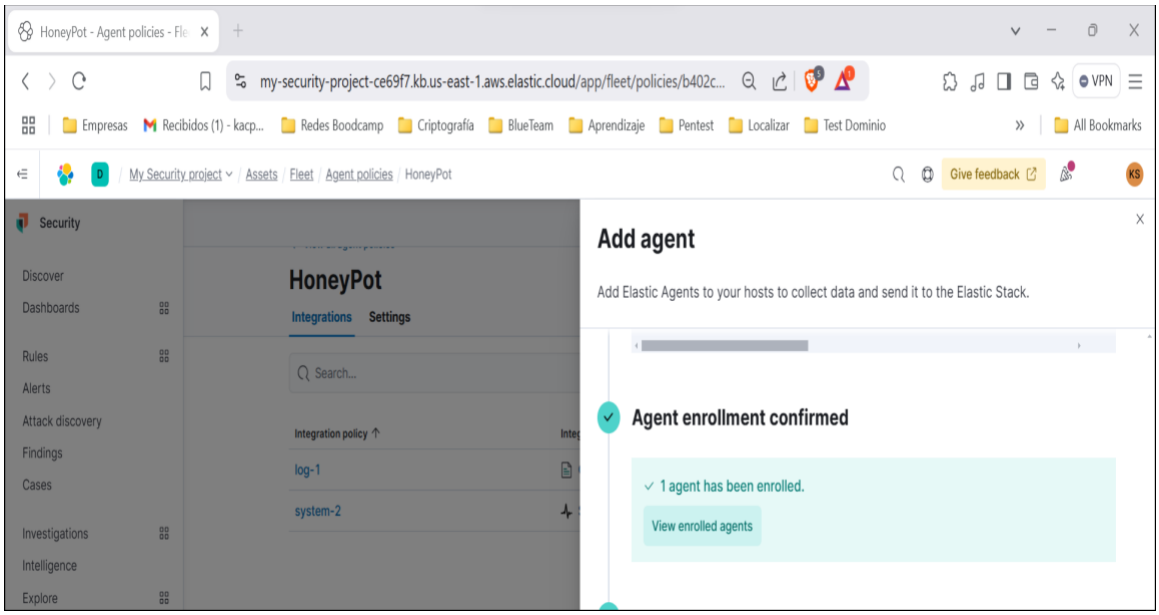

Custom Logs - Integrations - E
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/detail/l...
VPN
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Integrations
Custom Logs
Give feedback
KS
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Connection details
Back to integrations
Custom Logs
Elastic Agent
Version
2.3.3
Add Custom Logs
Overview
Settings
Configs
Custom Logs Package
The Custom Logs package is used to ingest arbitrary log files and parse their contents using Ingest Pipelines. Follow the steps below to set up and use this package.
Get started
Details
Version 2.3.3
Category Custom, Custom Logs
Subscription -
Developed by Elastic
Custom Logs Packa...
Get started
ECS Field Mapping

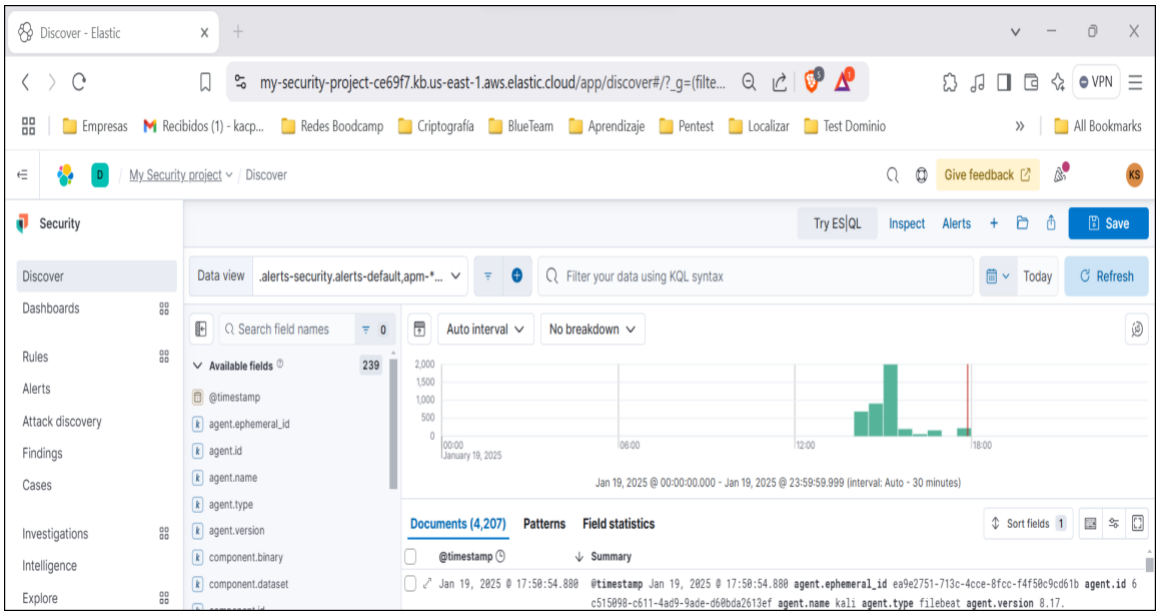

Add integration - Custom Logs
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/lo...
VPN
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
KS
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Cancel
Add Custom Logs integration
Configure an integration for the selected agent policy.
1
Configure integration
Integration settings
Choose a name and description to help identify how this integration will be used.
Integration name
log-1
Description
Optional
/home/kali/Desktop
Advanced options


Add integration - Custom Logs
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/lo...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Integration settings
Choose a name and description to help identify how this integration will be used.
Integration name
log-1
Description
Optional
Advanced options
Custom log file
Change defaults
Log file path
/home/kali/Desktop/honey
Add row
Path to log files to be collected


HoneyPot - Agent policies - Fle
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/b402c...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agent policies
HoneyPot
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
HoneyPot
Integrations
Settings
Search...
Integration policy
log-1
system-2
Add agent
Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.
Linux Tar
Mac
Windows
RPM
DEB
Kubernetes
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/ela
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
cd elastic-agent-8.17.0-linux-x86_64
sudo ./elastic-agent install --url=https://ce69f75cc626408ca156d5105c169c
4
Confirm agent enrollment


kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
Home
File Syst...
honey
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ pwd
/home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ ls
honey
(kali㉿kali)-[~/Desktop]
$ cd ..
(kali㉿kali)-[~]
$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
cd elastic-agent-8.17.0-linux-x86_64
sudo ./elastic-agent install --url=https://ce69f75cc626408ca156d5105c169c14.fleet.us-east-1.aws.elastic.cloud:443 --e


HoneyPot - Agent policies - Fle
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/b402c...
VPN
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agent policies
HoneyPot
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
HoneyPot
Integrations
Settings
Search...
Integration policy
log-1
system-2
Add agent
Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.
Agent enrollment confirmed
1 agent has been enrolled.
View enrolled agents



Ejemplo:


```
{
 "@timestamp": [
  "2025-01-19T16:50:43.343Z"
 ],
 "agent.ephemeral_id": [
  "3c02ab2e-e741-4b27-b23a-692c003e04a4"
 ],
 "agent.id": [
  "6c515098-c611-4ad9-9ade-d60bda2613ef"
 ],
 "agent.name": [
  "kali"
 ],
 "agent.type": [
  "filebeat"
```

```
],
"agent.version": [
  "8.17.0"
],
"data_stream.dataset": [
  "generic"
],
"data_stream.namespace": [
  "default"
],
"data_stream.type": [
  "logs"
],
"ecs.version": [
  "8.0.0"
],
"elastic_agent.id": [
  "6c515098-c611-4ad9-9ade-d60bda2613ef"
],
"elastic_agent.snapshot": [
  false
],
"elastic_agent.version": [
  "8.17.0"
],
"event.agent_id_status": [
```

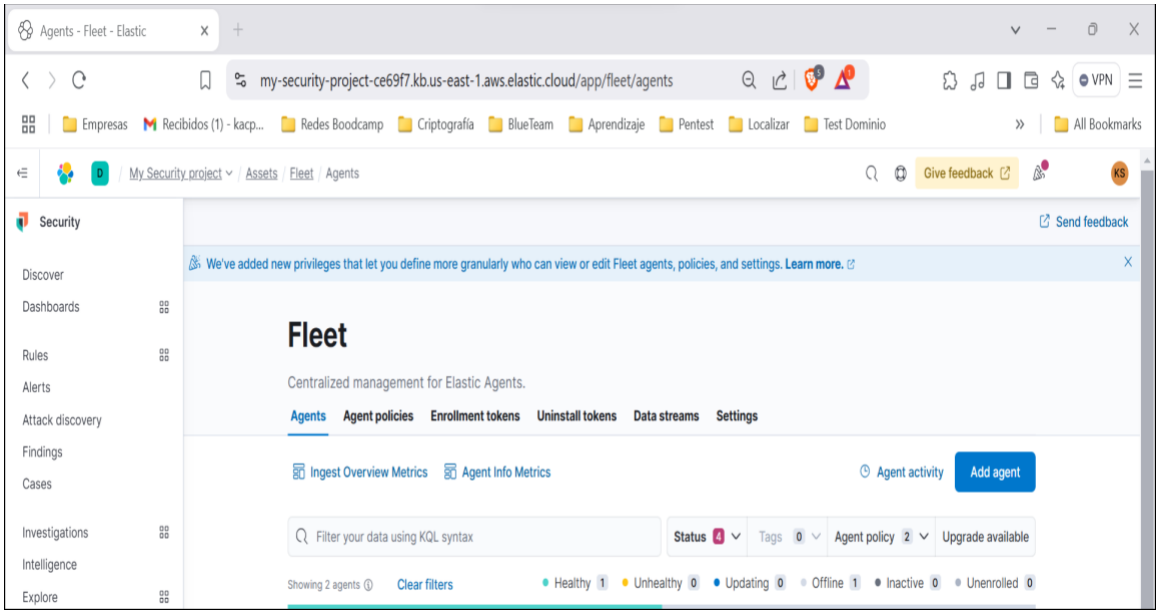
```
  "verified"
],
"event.dataset": [
  "generic"
],
"event.ingested": [
  "2025-01-19T16:50:54.000Z"
],
"host.architecture": [
  "x86_64"
],
"host.containerized": [
  false
],
"host.hostname": [
  "kali"
],
"host.id": [
  "55e5305955694ed3b6c7506b1268fad8"
],
"host.ip": [
  "192.168.1.38",
  "fe80::910f:4a21:3bcc:f90b",
  "172.17.0.1",
  "fe80::42:e0ff:fe05:163f",
  "fe80::20a5:2eff:fe7f:36",
```

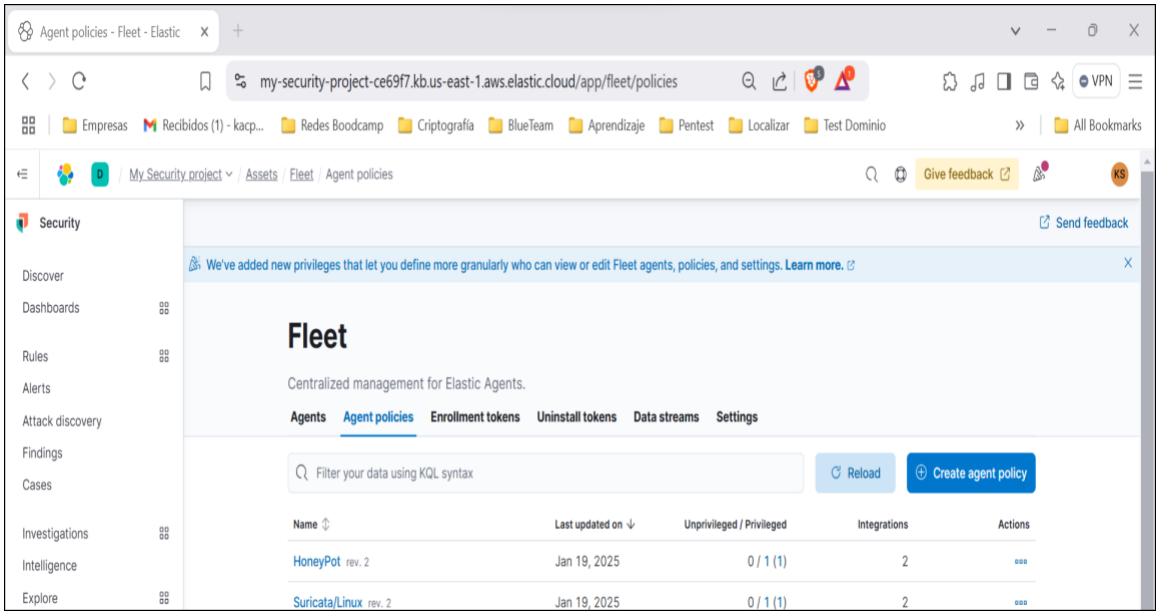
```
  "fe80::7489:baff:feb1:47ed"
],
"host.mac": [
  "02-42-E0-05-16-3F",
  "08-00-27-5A-39-D3",
  "22-A5-2E-7F-00-36",
  "76-89-BA-B1-47-ED"
],
"host.name": [
  "kali"
],
"host.os.codename": [
  "kali-rolling"
],
"host.os.family": [
  "debian"
],
"host.os.kernel": [
  "6.11.2-amd64"
],
"host.os.name": [
  "Kali GNU/Linux"
],
"host.os.name.text": [
  "Kali GNU/Linux"
],
```

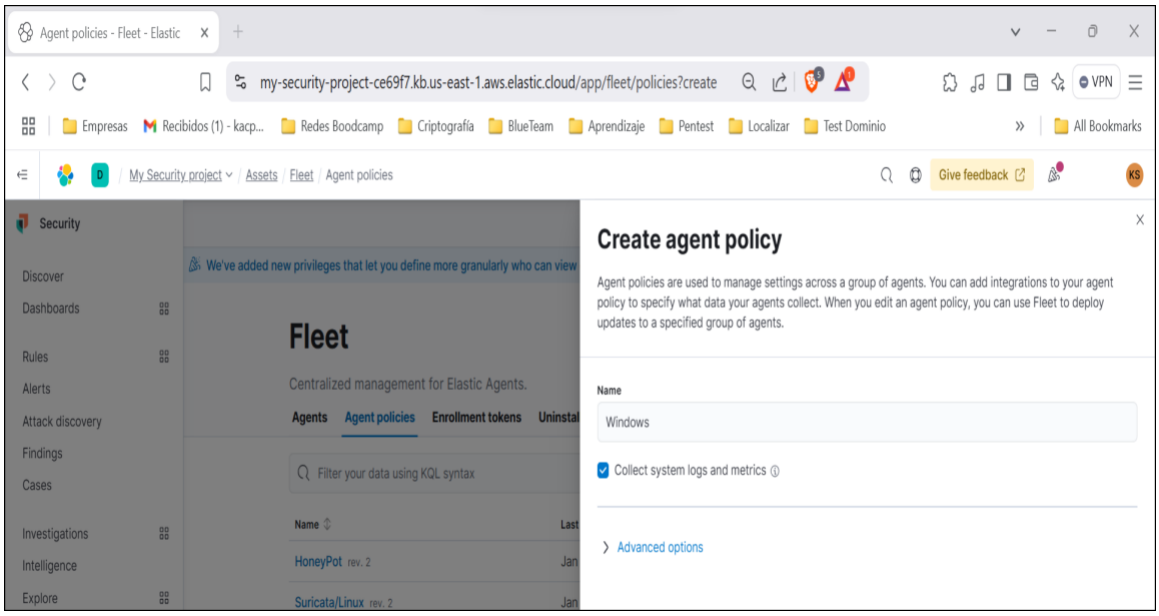
```
"host.os.platform": [
  "kali"
],
"host.os.type": [
  "linux"
],
"host.os.version": [
  "2024.4"
],
"input.type": [
  "log"
],
"log.file.path": [
  "/home/kali/Desktop/honey"
],
"log.file.path.text": [
  "/home/kali/Desktop/honey"
],
"log.offset": [
  718
],
"message": [
  "2025-01-19T16:21:57.442331Z,domain:,username:,password:,hostname:KK"
],
"_id": "AZR_ebR0sttFzmZ8Ty3r",
"_index": ".ds-logs-generic-default-2025.01.19-000001",
```

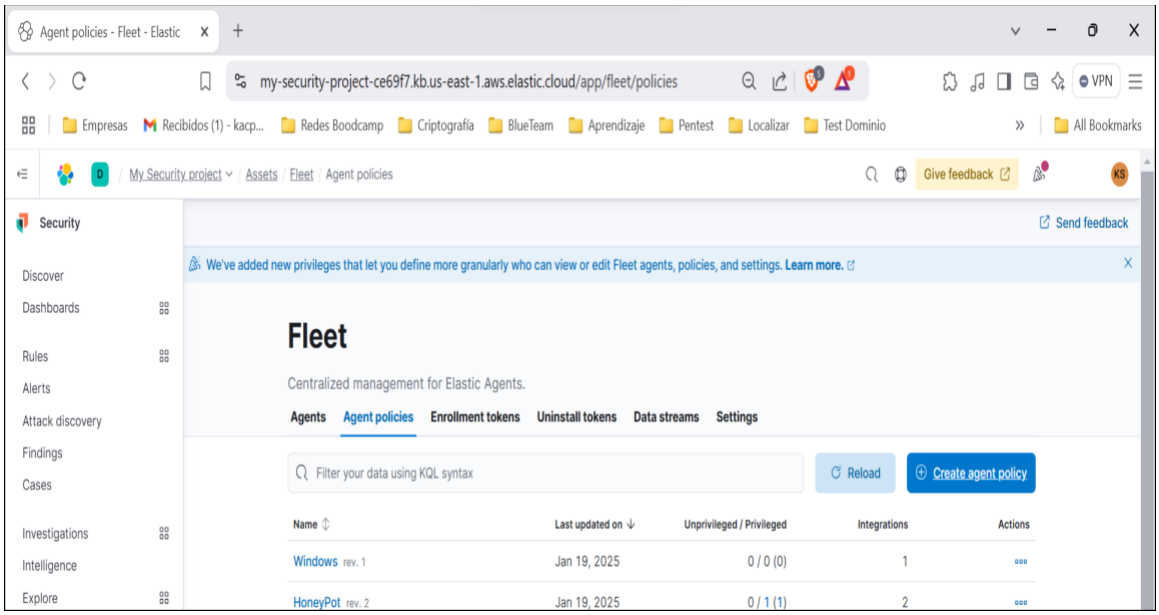
"_score": null
}

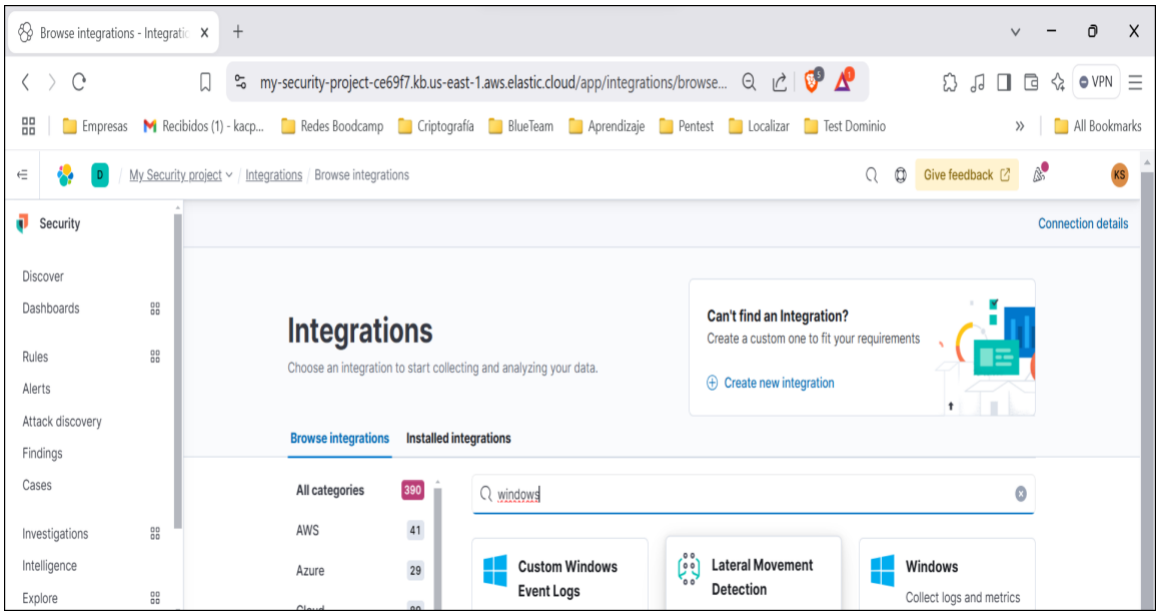
4.3. Windows

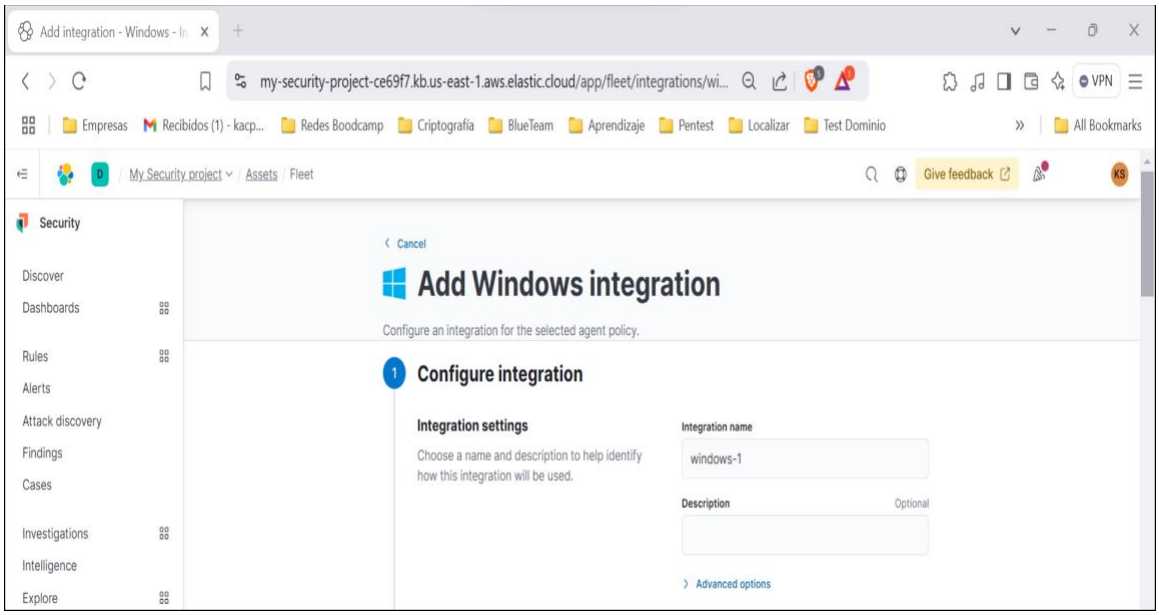


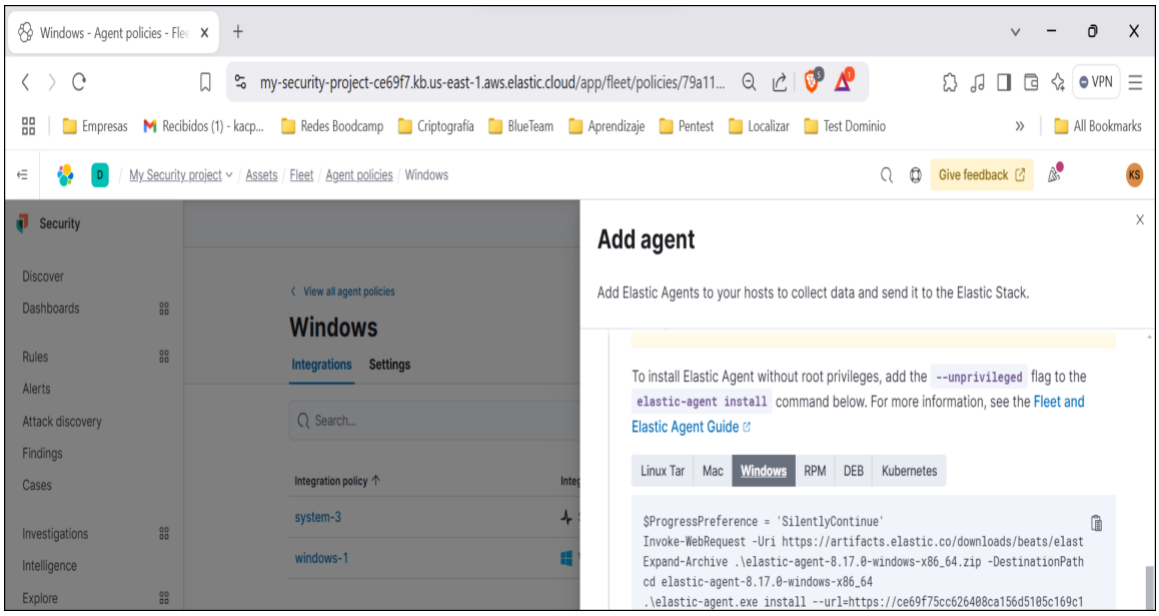


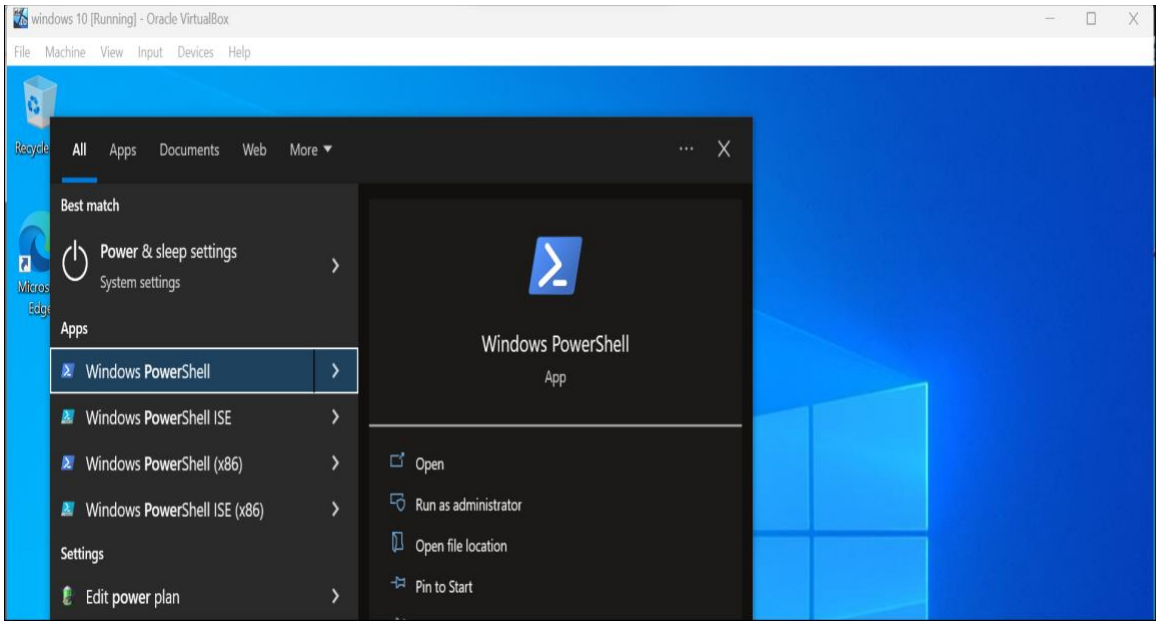

Agent policies - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies?create
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agent policies
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
We've added new privileges that let you define more granularly who can view
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Filter your data using KQL syntax
Name
HoneyPot rev. 2
Suricata/Linux rev. 2
Create agent policy
Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.
Name
Windows
Collect system logs and metrics
Advanced options

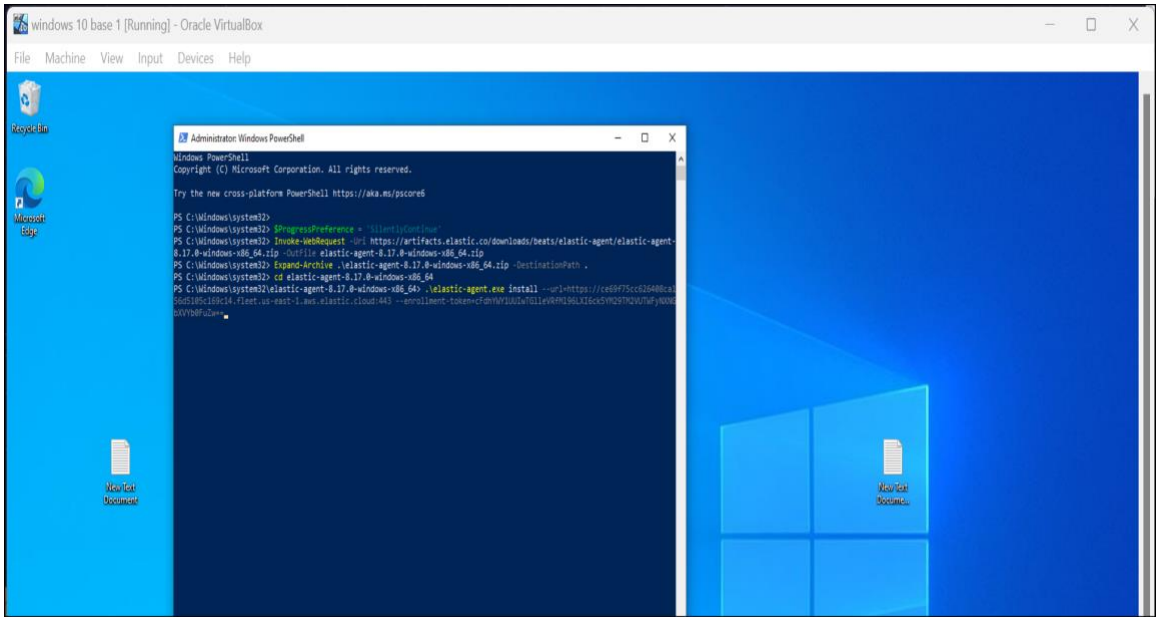

Agent policies - Fleet - Elastic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agent policies
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Send feedback
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Filter your data using KQL syntax
Reload
Create agent policy
Name
Last updated on
Unprivileged / Privileged
Integrations
Actions
Windows rev. 1
Jan 19, 2025
0 / 0 (0)
1
HoneyPot rev. 2
Jan 19, 2025
0 / 1 (1)
2

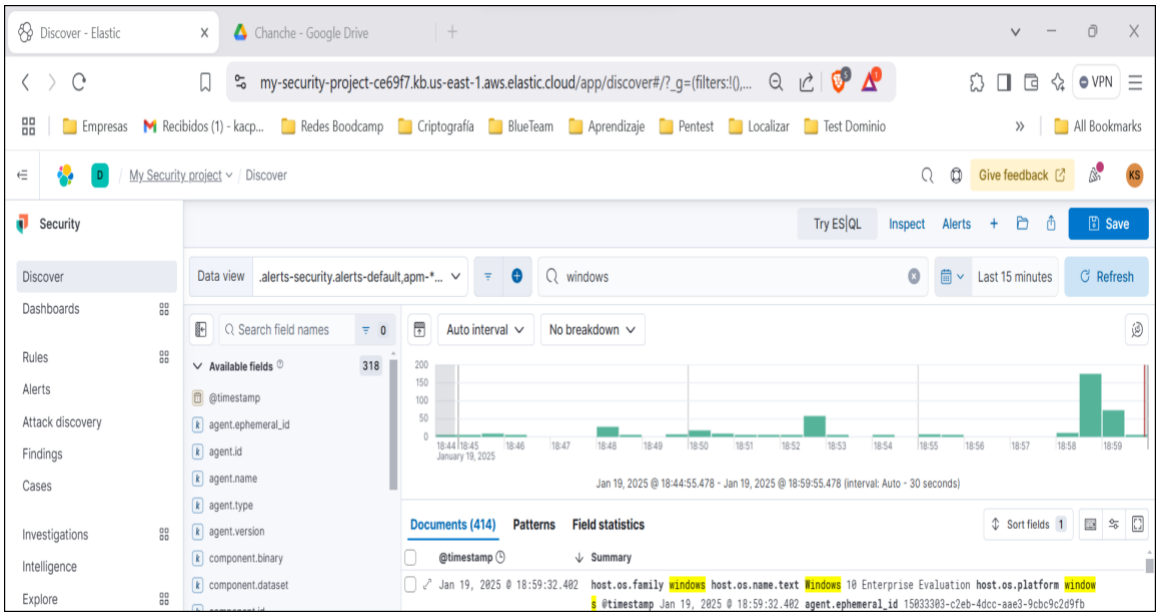

Browse integrations - Integratic
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/browse...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Integrations
Browse integrations
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Connection details
Integrations
Choose an integration to start collecting and analyzing your data.
Can't find an Integration?
Create a custom one to fit your requirements
Create new integration
Browse integrations
Installed integrations
All categories
390
AWS
41
Azure
29
windows
Custom Windows Event Logs
Lateral Movement Detection
Windows
Collect logs and metrics


Add integration - Windows - In
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/wi...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Cancel
Add Windows integration
Configure an integration for the selected agent policy.
1
Configure integration
Integration settings
Choose a name and description to help identify how this integration will be used.
Integration name
windows-1
Description
Optional
Advanced options


Windows - Agent policies - Flee
my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/79a11...
Empresas
Recibidos (1) - kacp...
Redes Boodcamp
Criptografía
BlueTeam
Aprendizaje
Pentest
Localizar
Test Dominio
All Bookmarks
My Security project
Assets
Fleet
Agent policies
Windows
Give feedback
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
View all agent policies
Windows
Integrations
Settings
Search...
Integration policy
system-3
windows-1
Add agent
Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.
To install Elastic Agent without root privileges, add the --unprivileged flag to the elastic-agent install command below. For more information, see the Fleet and Elastic Agent Guide
Linux Tar
Mac
Windows
RPM
DEB
Kubernetes
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elast
Expand-Archive .\elastic-agent-8.17.0-windows-x86_64.zip -DestinationPath
cd elastic-agent-8.17.0-windows-x86_64
.\elastic-agent.exe install --url=https://ce69f75cc626408ca156d5105c169c1


windows 10 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
All
Apps
Documents
Web
More
Best match
Power & sleep settings
System settings
Apps
Windows PowerShell
Windows PowerShell ISE
Windows PowerShell (x86)
Windows PowerShell ISE (x86)
Settings
Edit power plan
Windows PowerShell
App
Open
Run as administrator
Open file location
Pin to Start





Ejemplo:

{

"@timestamp": [

"2025-01-19T17:59:32.402Z"

],

"agent.ephemeral_id": [

"15033303-c2eb-4dcc-aae3-9cbc9c2d9fbf"

```
],
"agent.id": [
  "0a37e4d3-4dd5-498b-9eeb-1fcba2615353"
],
"agent.name": [
  "windows10"
],
"agent.type": [
  "filebeat"
],
"agent.version": [
  "8.17.0"
],
"component.binary": [
  "metricbeat"
],
"component.dataset": [
  "elastic_agent.metricbeat"
],
"component.id": [
  "system/metrics-default"
],
"component.type": [
  "system/metrics"
],
"data_stream.dataset": [
```

```
  "elastic_agent.metricbeat"
],
"data_stream.namespace": [
  "default"
],
"data_stream.type": [
  "logs"
],
"ecs.version": [
  "8.0.0"
],
"elastic_agent.id": [
  "0a37e4d3-4dd5-498b-9eeb-1fcba2615353"
],
"elastic_agent.snapshot": [
  false
],
"elastic_agent.version": [
  "8.17.0"
],
"event.agent_id_status": [
  "verified"
],
"event.dataset": [
  "elastic_agent.metricbeat"
],
```

```
"event.ingested": [
  "2025-01-19T17:59:42.000Z"
],
"host.architecture": [
  "x86_64"
],
"host.hostname": [
  "windows10"
],
"host.id": [
  "42c8fb83-0f6d-4214-8878-04bab8c5bc99"
],
"host.ip": [
  "fe80::850:7465:91b7:2eeb",
  "192.168.1.41"
],
"host.mac": [
  "08-00-27-30-A2-6A"
],
"host.name": [
  "windows10"
],
"host.os.build": [
  "19045.2006"
],
"host.os.family": [
```

```
  "windows"
],
"host.os.kernel": [
  "10.0.19041.2006 (WinBuild.160101.0800)"
],
"host.os.name": [
  "Windows 10 Enterprise Evaluation"
],
"host.os.name.text": [
  "Windows 10 Enterprise Evaluation"
],
"host.os.platform": [
  "windows"
],
"host.os.type": [
  "windows"
],
"host.os.version": [
  "10.0"
],
"input.type": [
  "filestream"
],
"log.file.idxhi": [
  "262144"
],
```

```
 "log.file.idxlo": [
  "114720"
 ],
 "log.file.path": [
  "C:\\Program Files\\Elastic\\Agent\\data\\elastic-agent-8.17.0-96f2b9\\logs\\elastic-agent-20250119-1.ndjson"
 ],
 "log.file.vol": [
  "1324036786"
 ],
 "log.level": [
  "error"
 ],
 "log.offset": [
  200651
 ],
 "log.origin.file.line": [
  324
 ],
 "log.origin.file.name": [
  "module/wrapper.go"
 ],
 "log.origin.function": [
"github.com/elastic/beats/v7/metricbeat/mb/module.(*metricSetWrapper).handleFetchError"
 ],
```

```
 "log.source": [
  "system/metrics-default"
 ],
 "message": [
  "Error fetching data for metricset system.process: Not enough privileges to fetch information: Not enough privileges to fetch information: GetInfoForPid: could not get all information for PID 0: error fetching name: OpenProcess failed for pid=0: The parameter is incorrect.\nerror fetching status: OpenProcess failed for pid=0: The parameter is incorrect.\nGetInfoForPid: could not get all information for PID 4: error fetching name: GetProcessImageFileName failed for pid=4: GetProcessImageFileName failed: invalid argument\nnon fatal error fetching PID some info for 92, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 340, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 428, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 500, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 512, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 608, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 1780, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 2884, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 3588, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 5644, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 5828, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 5840, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 6952, metrics are valid, but partial:
```

FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 5360, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 3832, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied."

],

"service.name": [

"metricbeat"

],

"_id": "AZR_uLR0sttFzmZzVV9g",

"_index": ".ds-logs-elastic_agent.metricbeat-default-2025.01.19-000001",

"_score": null

}

5. Propuesta de mejora

Podemos mejorar la siguiente infraestructura al reforzar la segmentación de las redes utilizando VLANs y aplicando reglas estrictas en el firewall PfSense, como limitando solamente el tránsito de los logs hacia Elastic, y encriptando todo tipo de información sensible con ChaCha20-Poly1305.

Tambien habría que separar y eliminar la interacción bilateral entre las redes internas DMZ2 y LAN, tal como ya se hizo con la red DMZ con el honeypot para que solo sea accesible desde la WAN. Además, se habilitaría un sistema de detección y prevención de intrusos (IDS/IPS) como Suricata en el firewall, así como listas blancas para controlar el tráfico permitido y listas negras dinámicas para bloquear direcciones IP maliciosas conocidas.

Además, los logs generados deben segregarse y analizarse mediante herramientas especializadas, configurando alertas en tiempo real para detectar actividad sospechosa como intentos de explotación o conexiones no autorizadas.

Por último, habría que implementar un sistema de copias de seguridad automáticas y periódicas de todos los datos críticos, asegurándose de que las copias sean almacenadas en una ubicación segura y aislada de la red principal.