

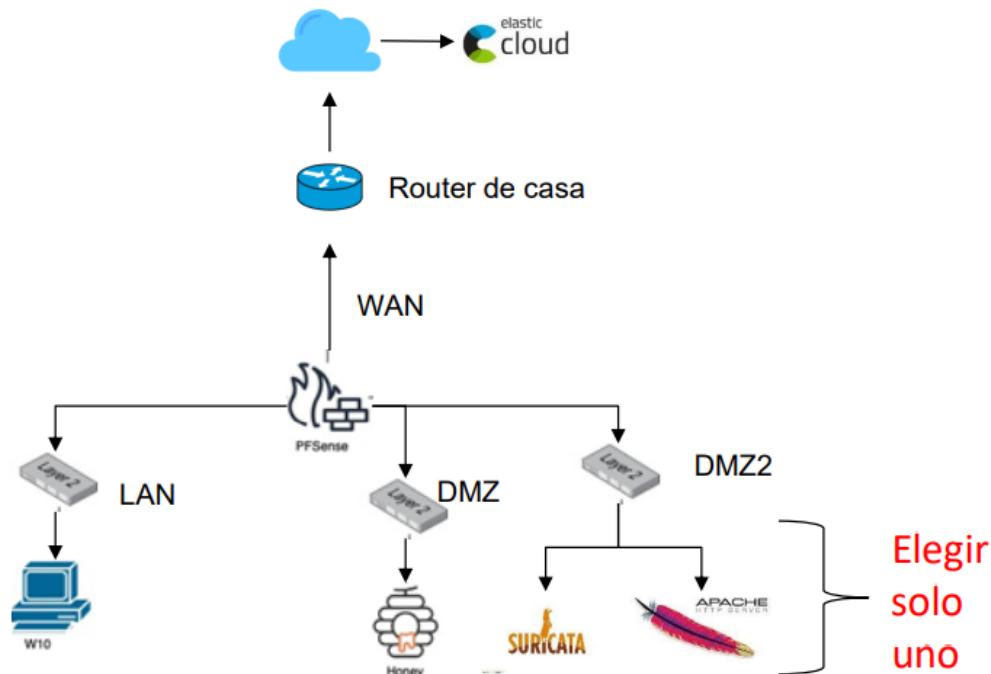
Blue Team Report

By Monica Licea Castro

We have been asked to create the following infrastructure:

Enunciado

Queremos montar la siguiente infraestructura:



Los requisitos que debe cumplir son los siguientes:

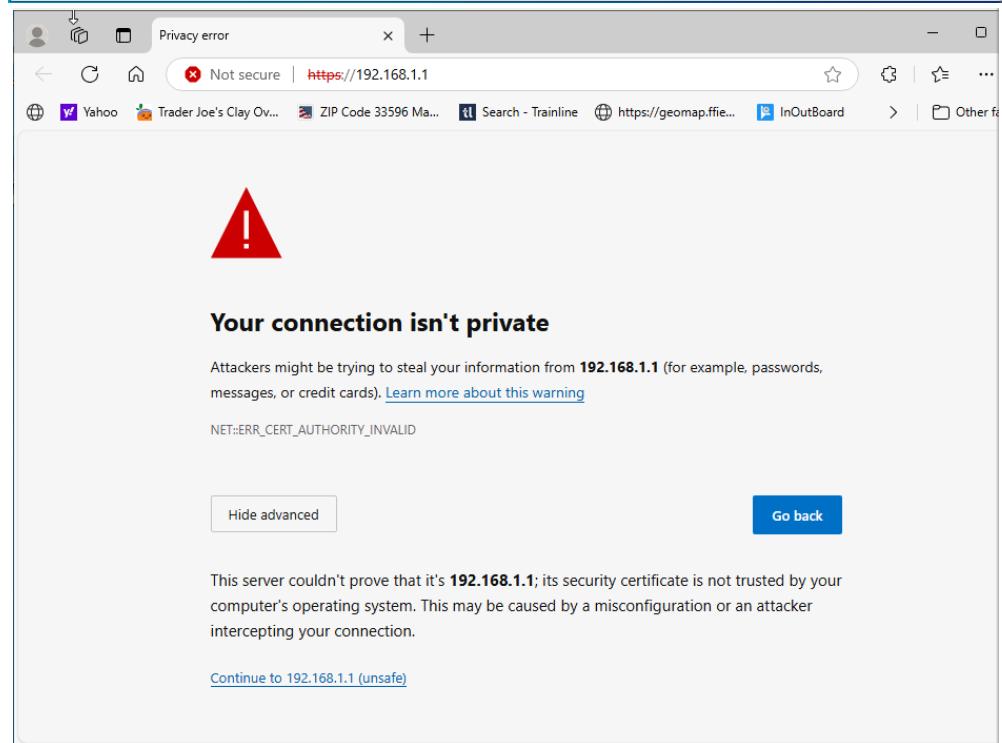
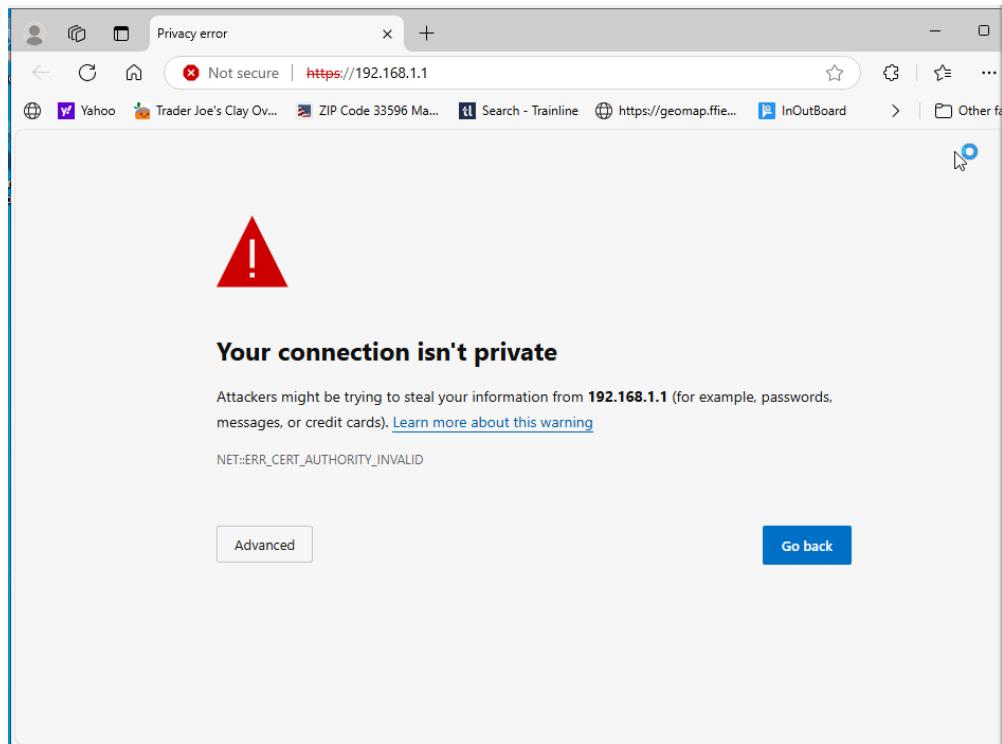
1. Debe tener un Pfsense en que se interconecten las redes LAN, DMZ y DMZ2
2. En la red LAN debe haber un equipo Windows 11 que envíe logs al servidor de Elastic.
3. En la red DMZ debe haber un honeypot que envíe los logs al servidor de Elastic.
 1. Este honeypot no debe tener acceso a ninguna red interna (LAN, DMZ2...) y debe ser accesible desde el exterior (red WAN) en ambos sentidos.
4. En la red DMZ2 debe haber otra fuente diferente de logs a las dos mencionadas anteriormente. Se propone Suricata o Apache Server como posibles fuentes, pero se deja a elección del alumno.
5. El servidor de Elastic debe recibir, almacenar y poder visualizar los logs del honeypot, el Windows 11 y la fuente elegida ubicada en la DMZ2.

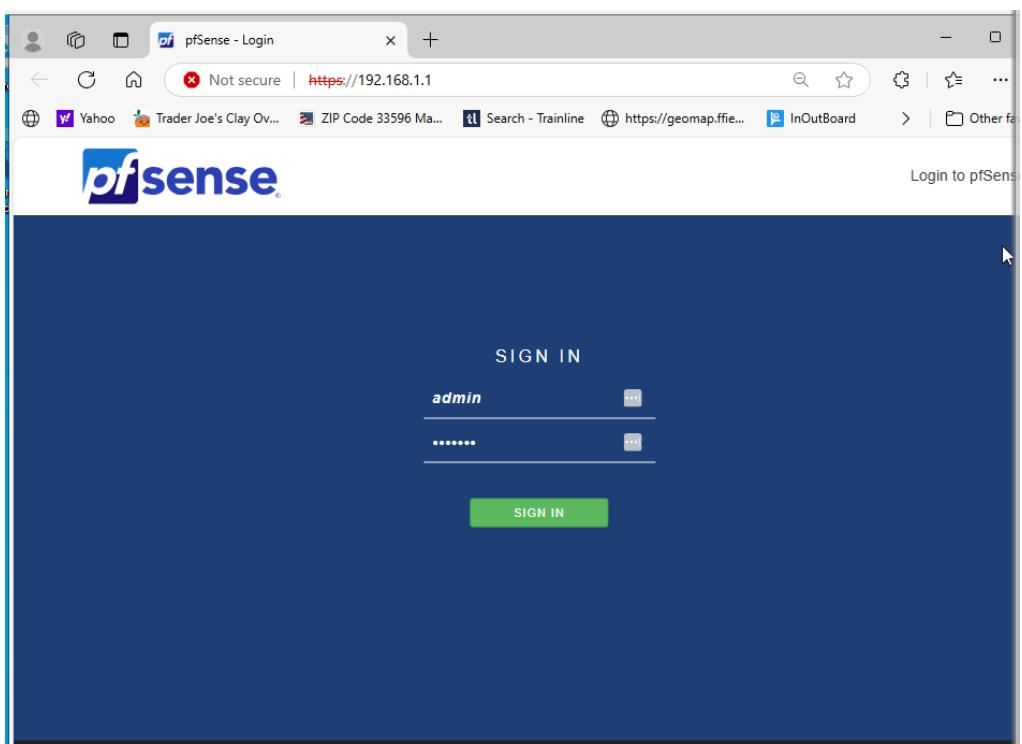
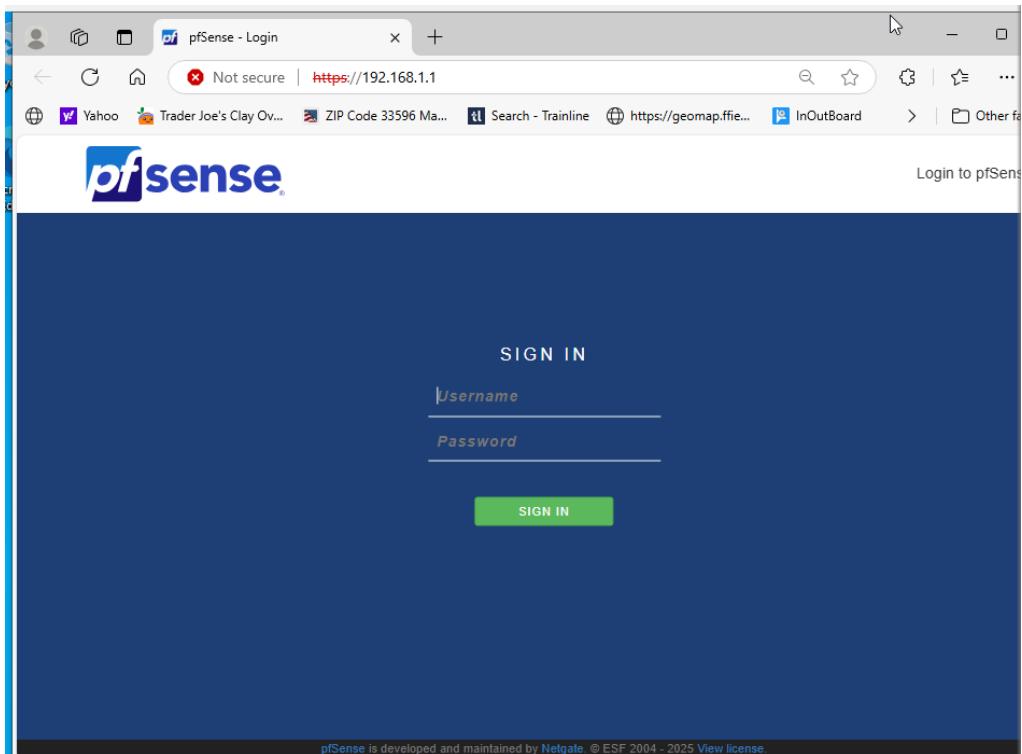
Criterios de evaluación de la memoria:

1. Debe contener evidencias y explicaciones que demuestren la correcta creación de la infraestructura de red en el Pfsense.
2. Debe contener explicación y captura de las reglas de firewall elegidas para cada red (WAN, NAT, LAN, DMZ y DMZ2)
3. Debe contener evidencias de las políticas e integraciones asignadas a cada agente del SIEM (Elastic)
4. Debe contener evidencias que demuestren la correcta recepción de los logs, de todas las fuentes especificadas en el enunciado, en el SIEM (Elastic).

PFSense Configuration

LAN v4: 192.168.1.1





The screenshot shows the pfSense Status / Dashboard page. On the left, there's a 'System Information' panel with details like Name (pfSense.home.arpa), User (admin@192.168.1.102), System (VirtualBox Virtual Machine, Netgate Device ID: f510a30ced97d5736ca1), BIOS (Vendor: innotech GmbH, Version: VirtualBox, Release Date: Fri Dec 1 2006), Version (2.7.2-RELEASE (amd64), built on Wed Dec 6 20:10:00 UTC 2023, FreeBSD 14.0-CURRENT), CPU Type (12th Gen Intel(R) Core(TM) i7-12700H, 2 CPUs: 1 package(s) x 2 cache groups x 1 core(s)), and Hardware crypto (Inactive). The right side features a 'Netgate Services And Support' panel with sections for Contract type (Community Support, Community Support Only), NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES, and a note about purchasing support. It also lists upgrade options like 'Upgrade Your Support' and 'Community Support Resources'.

The screenshot shows the pfSense web interface running on a VirtualBox machine. The title bar says 'UTM Blue Team [Running] - Oracle VirtualBox'. The main window displays the pfSense command-line menu:

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: f510a30ced97d5736ca1

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.207/24
                           v6/DHCP6: 2a0c:5a87:8401:e500:a00:27ff:febf:32
60/64
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: 
```

We now proceed with the pfSense Setup (establishing the domain and the DNS Servers)

The screenshot shows the initial welcome screen of the pfSense Setup Wizard. The title bar reads "pfSense.home.arpa - Wizard: pfSense". The main content area says "Welcome to pfSense® software! This wizard will provide guidance through the initial configuration of pfSense. The wizard may be stopped at any time by clicking the logo image at the top of the screen. pfSense® software is developed and maintained by Netgate®". A "Learn more" button is visible, and a "Next" button is at the bottom.

The screenshot shows the "General Information" step of the wizard. The title bar reads "pfSense.home.arpa - Wizard: pfSense". The main content area is titled "General Information" and says "Step 2 of 9". It contains fields for "Hostname" (set to "UTM") and "Domain" (set to "keepcoding.local"). Below these fields are explanatory notes and examples. At the bottom, there is a note about DNS resolver behavior and sections for "Primary DNS Server" (127.0.0.1), "Secondary DNS Server" (1.1.1.1), and "Override DNS" (with a checked checkbox).

The screenshot shows the 'Time Server Information' step of the pfSense setup wizard. The page title is 'Wizard / pfSense Setup / Time Server Information'. It indicates 'Step 3 of 9'. A sub-section titled 'Time Server Information' asks for the time, date and time zone. A field for 'Time server hostname' contains '2.pfsense.pool.ntp.org', with a note below it: 'Enter the hostname (FQDN) of the time server.' A dropdown menu for 'Timezone' is set to 'Europe/Madrid'. A blue 'Next' button is at the bottom.

WAN Interface Configuration

The screenshot shows the 'Configure WAN Interface' step of the pfSense setup wizard. The page title is 'Wizard / pfSense Setup / Configure WAN Interface'. It indicates 'Step 4 of 9'. A sub-section titled 'Configure WAN Interface' says 'On this screen the Wide Area Network information will be configured.' A dropdown for 'SelectedType' is set to 'DHCP'. Below, under 'General configuration', there are fields for 'MAC Address' (with a note about spoofing), 'MTU' (with a note about connection types), and 'MSS' (with a note about TCP connections). Under 'Static IP Configuration', there is a field for 'IP Address'. A note at the bottom right of the configuration section states: '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 this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.'

The screenshot shows the pfSense setup wizard at Step 5 of 9. The main configuration section is for PPTP settings, including fields for PPTP Local IP Address (set to 32), PPTP Remote IP Address, and PPTP Dial on demand (with a checkbox for Enable Dial-On-Demand mode). Below this is a section for RFC1918 Networks, which includes options to Block RFC1918 Private Networks and Block bogon networks. Both sections have checkboxes and explanatory text. At the bottom right is a blue 'Next' button.

LAN Interface Configuration (we now select a different IP to give 192.168.1.1 back to the router)

The screenshot shows the pfSense setup wizard at Step 5 of 9. The main configuration section is for the LAN interface, titled 'Configure LAN Interface'. It states that Local Area Network information will be configured. The LAN IP Address is set to 192.168.100.1, and the Subnet Mask is set to 24. A note indicates that if DHCP is used, the address should be typed as 'dhcp'. At the bottom right is a blue 'Next' button.

pfSense.home.arpa - Wizard: pfSe X

Not secure | https://192.168.1.1/wizard.php?xml=setup_wizard.xml

Yahoo Trader Joe's Clay Ov... ZIP Code 33596 Ma... Search - Trainline https://geomap.ifie... InOutBoard Other favorites

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

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:

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#).

pfSense.home.arpa - Wizard: pfSe X

Not secure | https://192.168.1.1/wizard.php?xml=setup_wizard.xml

Yahoo Trader Joe's Clay Ov... ZIP Code 33596 Ma... Search - Trainline https://geomap.ifie... InOutBoard Other favorites

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Wizard / pfSense Setup / Reload configuration

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#).

pfSense.home.arpa - Wizard: pfSe X

Not secure | https://192.168.1.1/wizard.php?xml=setup_wizard.xml

Yahoo Trader Joe's Clay Ov... ZIP Code 33596 Ma... Search - Trainline https://geomap.ffie... InOutBoard Other favorites

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Wizard / pfSense Setup / Reload in progress

Step 8 of 9

Reload in progress

A reload is now in progress. Please wait.

The wizard will redirect to the next step once the reload is completed.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#).

Privacy error

Not secure | <https://192.168.100.1>

Yahoo Trader Joe's Clay Ov... ZIP Code 33596 Ma... Search - Trainline https://geomap.ffie... InOutBoard Other favorites

!

Your connection isn't private

Attackers might be trying to steal your information from **192.168.100.1** (for example, passwords, messages, or credit cards). [Learn more about this warning](#)

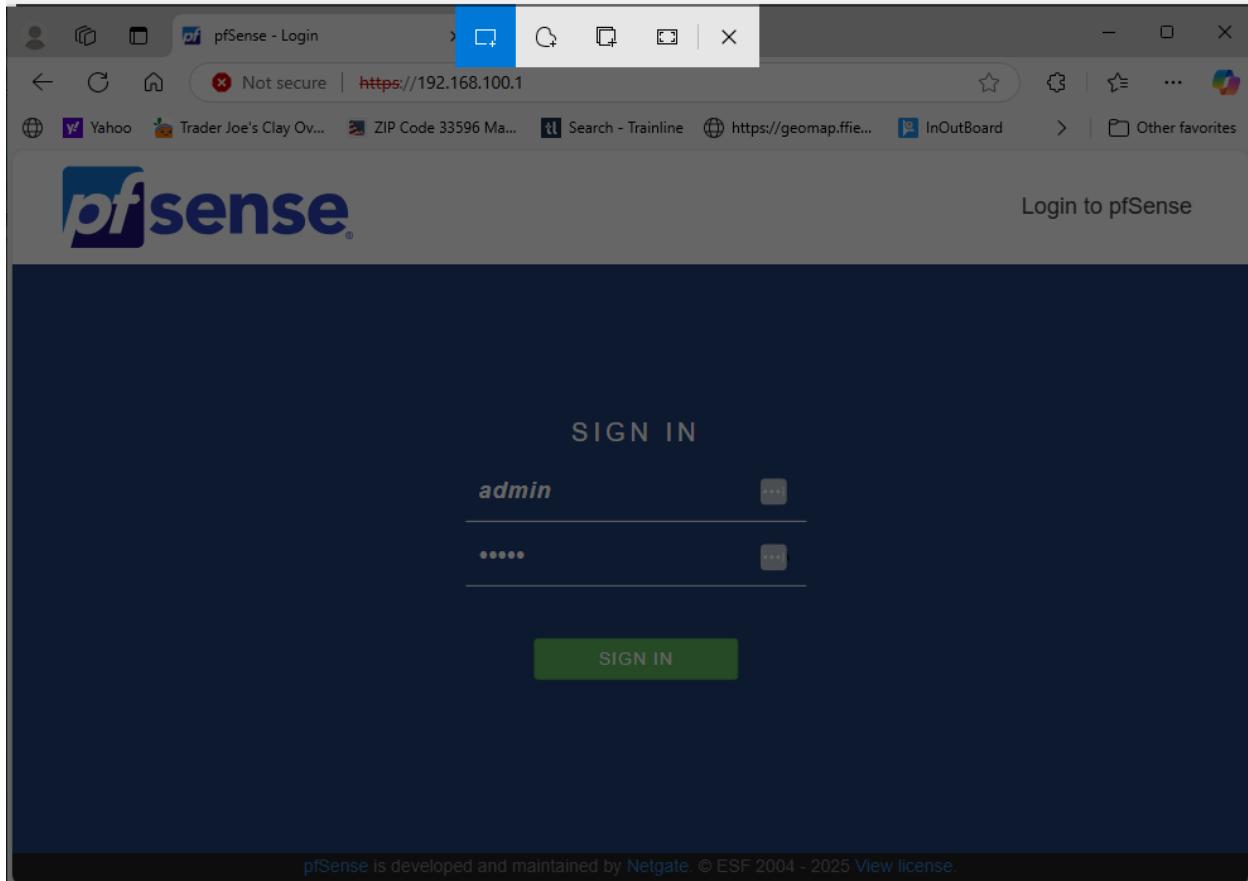
NET::ERR_CERT_AUTHORITY_INVALID

[Hide advanced](#) [Go back](#)

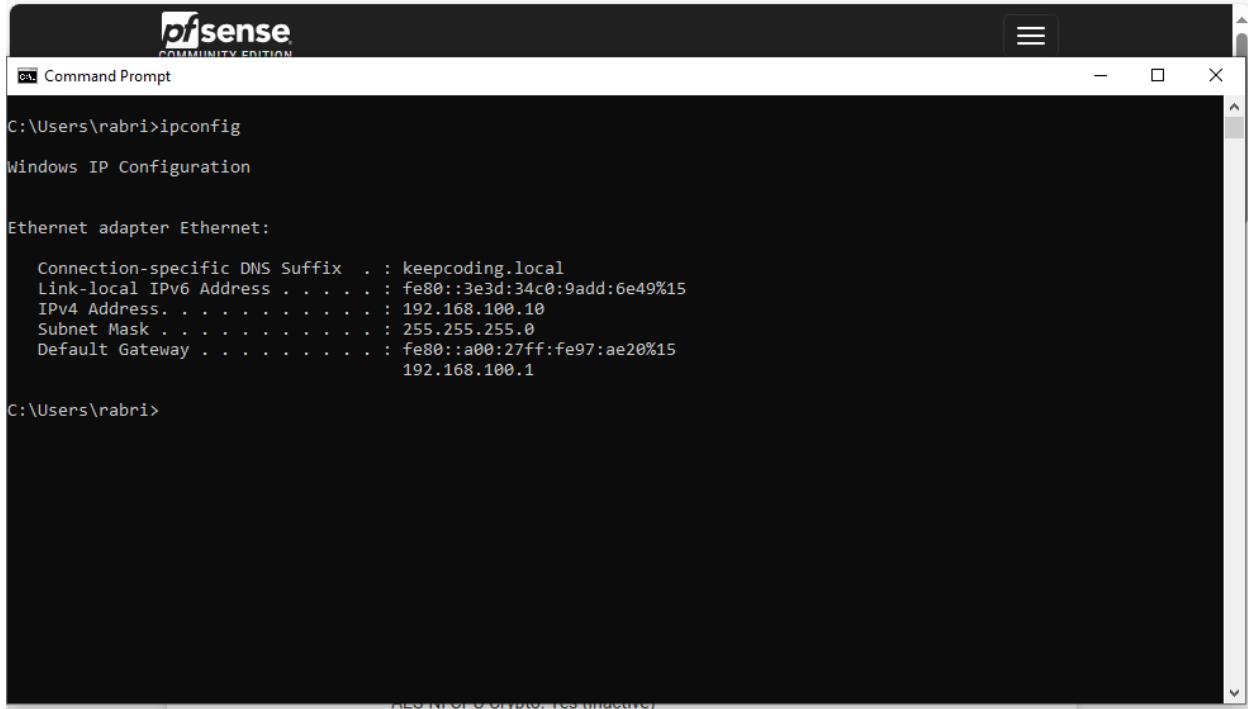
This server couldn't prove that it's **192.168.100.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Continue to 192.168.100.1 \(unsafe\)](#)

Log back in to pfSense with the newly-assigned IP address

A screenshot of a web browser showing the pfSense Status / Dashboard page. The URL in the address bar is https://192.168.100.1. The page title is "Status / Dashboard". A "System Information" table is displayed, containing the following data:

System Information	
Name	UTM.keepcoding.local
User	admin@192.168.100.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: f510a30ced97d5736ca1
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT
The system is on the latest version. Version information updated at Sat Jan 11 16:38:44 CET 2025	
CPU Type	12th Gen Intel(R) Core(TM) i7-12700H 2 CPUs: 1 package(s) x 2 cache groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No



pfSense
COMMUNITY EDITION

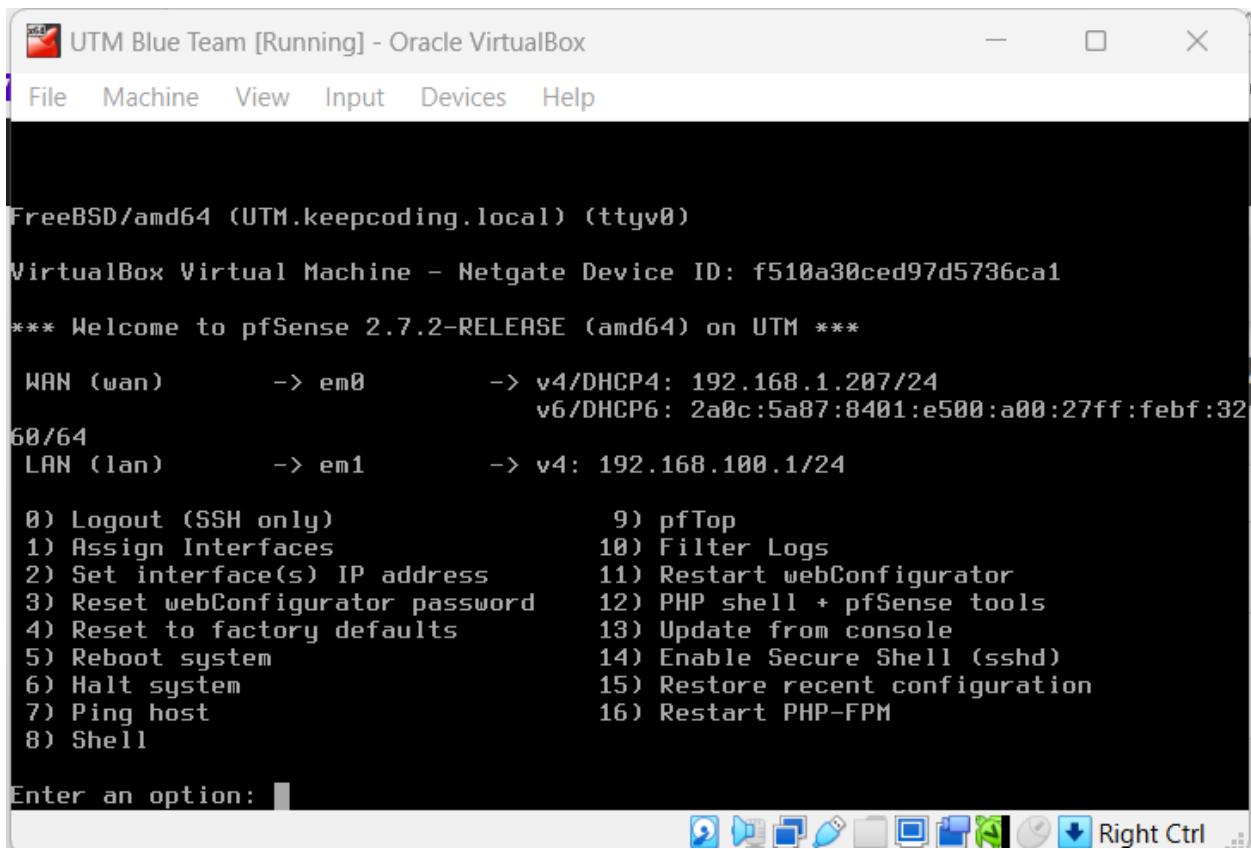
Command Prompt

```
C:\Users\rabri>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . : keepcoding.local
  Link-local IPv6 Address . . . . . : fe80::3e3d:34c0:9add:6e49%15
    IPv4 Address. . . . . : 192.168.100.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::a00:27ff:fe97:ae20%15
                                         192.168.100.1

C:\Users\rabri>
```



UTM Blue Team [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: f510a30ced97d5736ca1

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.207/24
                           v6/DHCP6: 2a0c:5a87:8401:e500:a00:27ff:febf:32
60/64
LAN (lan)      -> em1          -> v4: 192.168.100.1/24

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

Enter an option: ■
```

DNS Resolver settings

The screenshot shows the pfSense web interface under the 'Services' section, specifically the 'DNS Resolver' settings. The title bar says 'Services / DNS Resolver / General Settings'. A yellow warning box at the top states: '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.' Below the warning, there are three tabs: 'General Settings' (selected), 'Advanced Settings', and 'Access Lists'. The main content area is titled 'General DNS Resolver Options'. It includes the following sections:

- Enable**: A checked checkbox labeled 'Enable DNS resolver'.
- Listen Port**: A text input field containing '53'. A note below it says: '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.'
- SSL/TLS Service**: An unchecked checkbox labeled 'Respond to incoming SSL/TLS queries from local clients'. A note below it says: 'Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.'

This screenshot shows the same pfSense DNS Resolver settings page, but with several options expanded to show more detail. The expanded sections are:

- Strict Outgoing Network Interface Binding**: An unchecked checkbox with a note explaining that by default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.
- Domain Local Zone Type**: A dropdown menu set to 'Transparent'. A note explains that this is the local-zone type used for the pfSense system domain.
- DNSSEC**: An unchecked checkbox for enabling DNSSEC Support.
- Python Module**: An unchecked checkbox for enabling the Python Module.
- DNS Query Forwarding**: An unchecked checkbox for enabling Forwarding Mode. A note explains that if set, DNS queries will be forwarded to upstream DNS servers defined in System > General Setup or via dynamic interfaces like DHCP, PPP, or OpenVPN.
- DHCP Registration**: An unchecked checkbox for registering DHCP leases in the DNS Resolver. A note explains that if set, machines specifying their hostname during IPv4 DHCP requests will have their leases registered.
- Use SSL/TLS for outgoing DNS Queries to Forwarding Servers**: An unchecked checkbox. A note explains that when combined with DNS Query Forwarding, queries to upstream forwarding DNS servers will be sent using SSL/TLS on port 853, requiring support from all configured servers.

Internet Accessibility

The screenshot shows the MARCA website homepage. At the top, there's a navigation bar with links to 'La portada de hoy', 'Radio MARCA', 'CuidatePlus', and the main 'MARCA' logo. Below the logo is a red banner with the text '(+) Escucha en directo Radio MARCA'. The main content area displays a section titled 'LALIGA EA SPORTS' showing football scores: Alavés 0 - Girona 1 (Finalizado). It also shows a 'DESCANSO DAZN' section with Valladolid 0 - Betis 0 (1: 4.75 - X: 3.5 - 2: 1.72) and a '10:30 Movistar LaLiga' section with Espanyol 0 - Leganés 0 (1: 2.1 - X: 2.95 - 2: 3.8). To the right, there's a 'Ver todo >' link. Below this, there's a video thumbnail of a football match and a news snippet about Valverde.

DHCP Server / LAN Configuration

The screenshot shows the pfSense web interface under the 'Services / DHCP Server / LAN' tab. A yellow warning message at the top states: '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.' The 'LAN' tab is selected. In the 'General DHCP Options' section, the 'DHCP Backend' is set to 'ISC DHCP'. Under 'Enable', the checkbox 'Enable DHCP server on LAN interface' is checked. Under 'BOOTP', the checkbox 'Ignore BOOTP queries' is unchecked. Under 'Deny Unknown Clients', the dropdown menu is set to 'Allow all clients'. A detailed description below explains the options: 'When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.' At the bottom, there's an 'Innore Denied' section with a checkbox and a note: 'Innore denied clients rather than reject'. The bottom of the screen shows a Windows taskbar with various icons and system status.

We assign a range of IP addresses to LAN and establish the DNS Servers

The screenshot shows a web browser window with the URL https://192.168.100.1/services_dhcp.php. The page displays the configuration for a Primary Address Pool and Server Options.

Primary Address Pool:

- Subnet: 192.168.100.0/24
- Subnet Range: 192.168.100.1 - 192.168.100.254
- Address Pool Range: From 192.168.100.100 To 192.168.100.200
- A note states: "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
- A note below says: "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

Previous IP Address: 192.168.100.10

The screenshot shows a terminal window on pfSense with the title "Command Prompt".

```
Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : keepcoding.local
Link-local IPv6 Address . . . . . : fe80::3e3d:34c0:9add:6e49%15
IPv4 Address . . . . . : 192.168.100.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::a00:27ff:fe97:ae20%15
                                         192.168.100.1

C:\Users\rabri>ping marca.com
Ping request could not find host marca.com. Please check the name and try again.

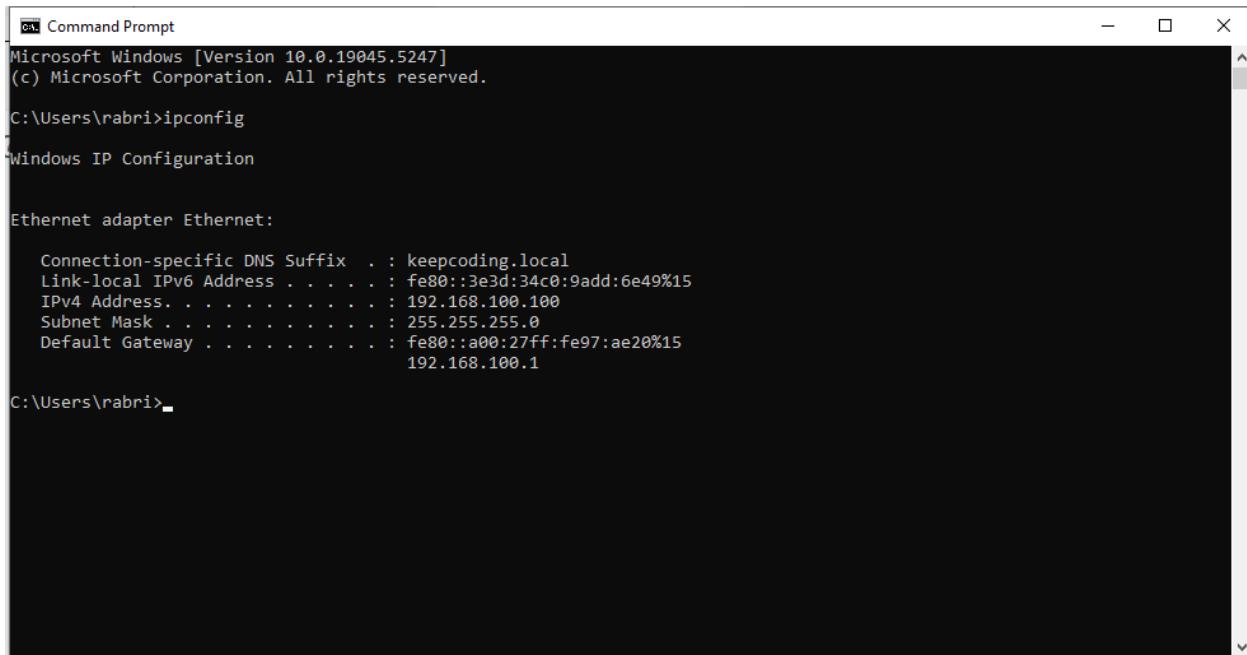
C:\Users\rabri>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : keepcoding.local
Link-local IPv6 Address . . . . . : fe80::3e3d:34c0:9add:6e49%15
IPv4 Address . . . . . : 192.168.100.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::a00:27ff:fe97:ae20%15
                                         192.168.100.1
```

New IP Address: 192.168.100.100



```
Windows Command Prompt
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Users\rabri>ipconfig

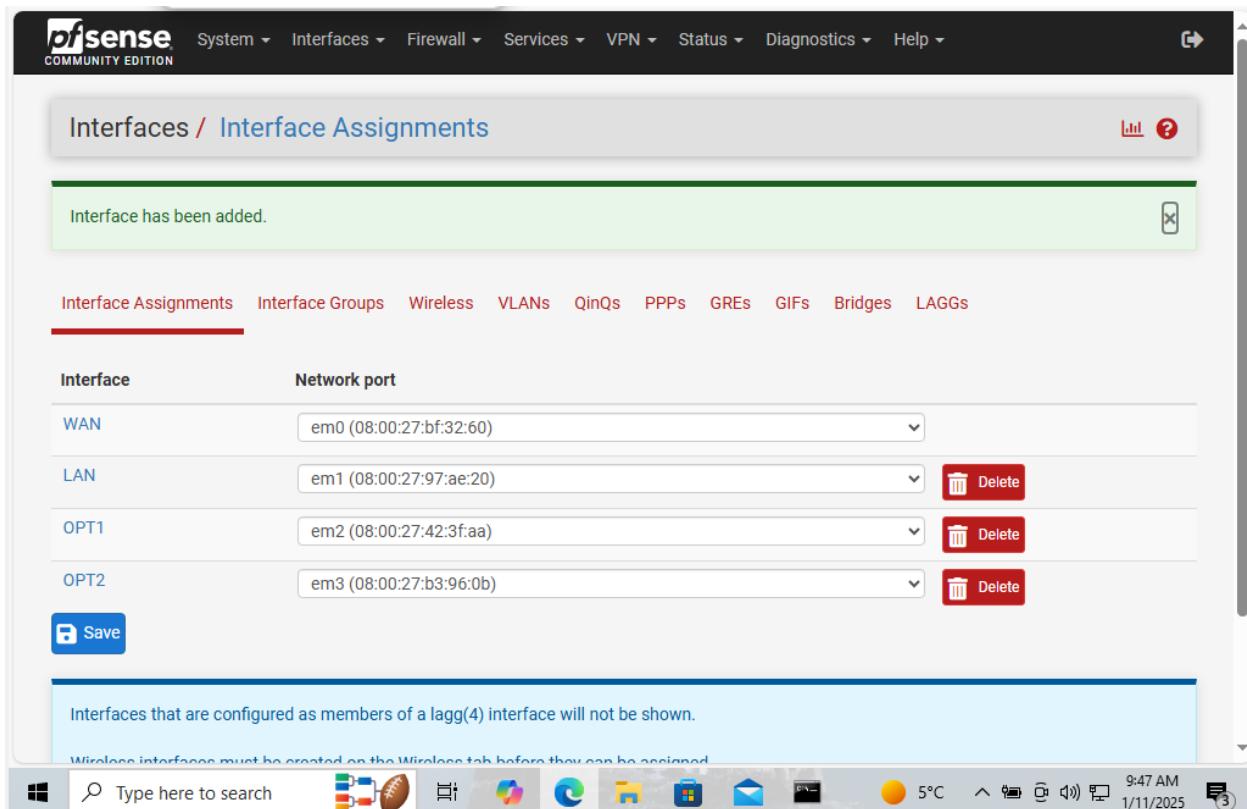
Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : keepcoding.local
Link-local IPv6 Address . . . . . : fe80::3e3d:34c0:9add:6e49%15
IPv4 Address. . . . . : 192.168.100.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::a00:27ff:fe97:ae20%15
                           192.168.100.1

C:\Users\rabri>
```

Interface Assignments to configure WAN, LAN, DMZ and DMZ2



The screenshot shows the pfSense interface assignments configuration page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main title is "Interfaces / Interface Assignments". A green message box at the top states "Interface has been added." Below the title, there are tabs for Interface Assignments, Interface Groups, Wireless, VLANs, QinQs, PPPs, GREs, GIFs, Bridges, and LAGGs. The "Interface Assignments" tab is selected. The main table lists four interfaces: WAN, LAN, OPT1, and OPT2, each associated with a network port (em0, em1, em2, em3). Each row includes a "Delete" button. At the bottom left is a "Save" button. A note below the table states: "Interfaces that are configured as members of a lagg(4) interface will not be shown." Another note at the bottom says: "Wireless interfaces must be created on the Wireless tab before they can be assigned." The bottom of the screen shows the Windows taskbar with various icons and the system tray.

Establishing OPT1 Interface as DMZ and assignment of a static IPv4

The screenshot shows the pfSense web interface under the 'Interfaces' section for the 'OPT1 (em2)' interface. The 'General Configuration' tab is selected.

General Configuration

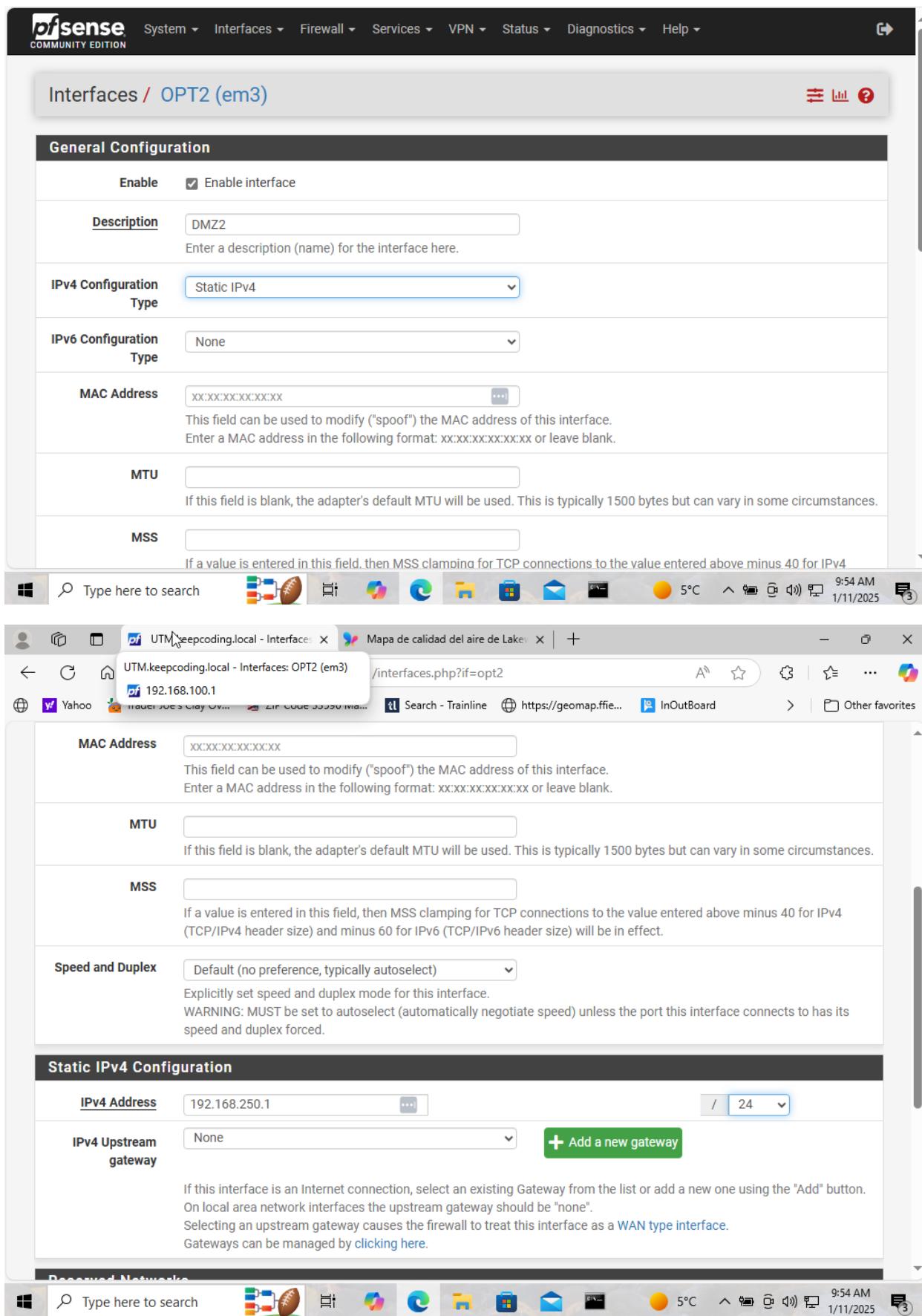
- Enable:** Enable interface
- Description:** DMZ
Enter a description (name) for the interface here.
- IPv4 Configuration Type:** Static IPv4
- IPv6 Configuration Type:** None
- MAC Address:** XX:XX:XX:XX:XX:XX
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: XX:XX:XX:XX:XX or leave blank.
- MTU:** (Blank)
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:** (Blank)
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4

The screenshot shows the pfSense web interface under the 'Static IPv4 Configuration' section for the 'OPT1 (em2)' interface.

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

Establishing OPT2 Interface as DMZ2 and assignment of a static IPv4



The image shows two side-by-side screenshots for configuring an interface on a pfSense system.

Top Screenshot (pfSense Web Interface):

- General Configuration:**
 - Enable:** Checked
 - Description:** DMZ2
 - IPv4 Configuration Type:** Static IPv4
 - IPv6 Configuration Type:** None
 - MAC Address:** XX:XX:XX:XX:XX:XX
 - MTU:** (Blank)
 - MSS:** (Blank)
- Bottom Screenshot (Browser Comparison):**
 - MAC Address:** XX:XX:XX:XX:XX:XX
 - MTU:** (Blank)
 - MSS:** (Blank)
 - Speed and Duplex:** Default (no preference, typically autoselect)

Static IPv4 Configuration:

- IPv4 Address:** 192.168.250.1 / 24
- IPv4 Upstream gateway:** None

Bottom Screenshot (Browser Comparison):

- MAC Address:** XX:XX:XX:XX:XX:XX
- MTU:** (Blank)
- MSS:** (Blank)
- Speed and Duplex:** Default (no preference, typically autoselect)

Checking the Configuration and IPs of WAN, LAN, DMZ and DMZ2

UTM Blue Team [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: f510a30ced97d5736ca1

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.207/24
                           v6/DHCP6: 2a0c:5a87:8401:e500:a00:27ff:febf:32
60/64
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
DMZ (opt1)      -> em2      -> v4: 192.168.200.1/24
DMZ2 (opt2)     -> em3      -> v4: 192.168.250.1/24

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

Enter an option: [
```

Icons at the bottom include: question mark, magnifying glass, file, folder, network, user, download, right control.

Configuration of the DHCP Server on DMZ, Assignment of a Specific IP Range and the DNS Servers

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / DHCP Server / DMZ

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.

LAN DMZ **DMZ2**

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on DMZ interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="button" value="Allow all clients"/> When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied	<input type="checkbox"/> Ignore denied clients rather than reject

Primary Address Pool	
Subnet	192.168.200.0/24
Subnet Range	192.168.200.1 - 192.168.200.254
Address Pool Range	<input type="text" value="192.168.200.100"/> From <input type="text" value="192.168.200.150"/> 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	<input type="text" value="WINS Server 1"/> <input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.200.1"/> <input type="text" value="1.1.1.1"/> <input type="text" value="8.8.8.8"/>
Other DHCP Options	
Gateway	<input type="text" value="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	<input type="text" value="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	<input type="text" value="example.com;sub.example.com"/>
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.	
Default Lease Time	<input type="text" value="7200"/>
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.	
Maximum Lease Time	<input type="text" value="86400"/>
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.	
Failover peer	

Configuration of the DHCP Server on DMZ2, Assignment of a Specific IP Range and the DNS Servers

The screenshot shows the pfSense web interface for managing the DHCP Server. The top navigation bar includes the pfSense logo and a menu icon. The main title is "Services / DHCP Server / DMZ2". A yellow warning message states: "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." Below the title, there are tabs for LAN, DMZ, and DMZ2, with DMZ2 selected. The "General DHCP Options" section shows the following settings:

- DHCP Backend:** ISC DHCP
- Enable:** Enable DHCP server on DMZ2 interface
- BOOTP:** Ignore BOOTP queries
- Deny Unknown Clients:** Allow all clients (dropdown menu)
- A note below states: "When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC

The "Server Options" section lists the following DNS servers:

- WINS Servers: WINS Server 1, WINS Server 2
- DNS Servers: 192.168.250.1, 1.1.1.1, 8.8.8.8 (highlighted with a blue border), DNS Server 4

The "OMAPI" section includes:

- OMAPI Port:** OMAPI Port (text input field)
- A note: "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 (text input field)
- Generate New Key:** Generate New Key (checkbox)
- A note: "Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint." and "Generate a new key based on the selected algorithm."

Establishing LAN rules regarding Web Ports on the Firewall (80 and 443)

The screenshot shows the 'Aliases' configuration page in pfSense. The 'Properties' section is displayed, with the 'Name' set to 'Web'. The 'Description' field contains 'Puertos para trafico web'. The 'Type' is set to 'Port(s)'. In the 'Port(s)' section, two entries are listed: port 80 mapped to HTTP and port 443 mapped to HTTPS.

Port	Protocol	Action
80	HTTP	Delete
443	HTTPS	Delete

The screenshot shows the 'Rules / LAN' configuration page in pfSense. The 'LAN' tab is selected. The 'Rules (Drag to Change Order)' table lists three rules:

Index	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1	4/33.04 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
2	23/108.78 MiB	IPv4	*	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	
3	0/0 B	IPv6	*	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	

At the bottom, there are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Establishing DMZ Rules Regarding Web Traffic on the Firewall with the Newly Created Rule

The screenshot shows the pfSense Firewall Rules / DMZ interface. The top navigation bar includes links for Floating, WAN, LAN, DMZ, and DMZ2. The main content area is titled "Rules (Drag to Change Order)" and displays a message: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." Below this message are several action buttons: Add (green), Add (green), Delete (red), Toggle (blue), Copy (blue), Save (blue), and Separator (orange). A small information icon is visible at the bottom left.

The screenshot shows the pfSense Firewall Rules / Edit interface for a newly created rule. The top navigation bar includes links for Floating, WAN, LAN, DMZ, and DMZ2. The main content area is titled "Edit Firewall Rule". The "Action" dropdown is set to "Pass". The "Disabled" section contains a checkbox labeled "Disable this rule" with the note: "Set this option to disable this rule without removing it from the list." The "Interface" dropdown is set to "DMZ". The "Address Family" dropdown is set to "IPv4". The "Protocol" dropdown is set to "TCP". At the bottom of the page, there is a search bar and a taskbar with various icons.

UTM.keepcoding.local - Firewall: +

Not secure | https://192.168.100.1/firewall_rules_edit.php?id=2

Yahoo Trader Joe's Clay Ov... ZIP Code 33596 Ma... Search - Trainline https://geomap.ffe... InOutBoard Other favorites

Source

Source Invert match Any Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination Invert match Any Destination Address /

Destination Port Range (other) From Custom (other) To Custom Web Web

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Type here to search

3:57 AM 1/12/2025

Destination

Destination Invert match Any Destination Address /

Destination Port Range (other) From Custom (other) To Custom Web Web

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description Regla trafico web

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options **Display Advanced**

Establishing DMZ Rules Regarding DNSs on the Firewall

The screenshot shows the pfSense Firewall Rule editor interface. The top navigation bar includes the pfSense logo, a menu icon, and tabs for Firewall, Rules, and Edit. Below the navigation is the title "Edit Firewall Rule".

Action: Pass (selected from a dropdown). Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule. Set this option to disable this rule without removing it from the list.

Interface: DMZ (selected from a dropdown). Choose the interface from which packets must come to match this rule.

Address Family: IPv4 (selected from a dropdown). Select the Internet Protocol version this rule applies to.

Protocol: UDP (selected from a dropdown). Choose which IP protocol this rule should match.

Source:

Source: Invert match. Any (dropdown). Source Address (dropdown).

Display Advanced (button)

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination:

Destination: Invert match. Any (dropdown). Destination Address (dropdown).

Destination Port Range: DNS (53) (dropdown). From (dropdown). Custom (button). To (dropdown). Custom (button).

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options:

Log: Log packets that are handled by this rule. Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings link).

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Regla trafico DNS

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

[Display Advanced](#)

Rule Information

Tracking ID 1736679768

Created 1/12/25 12:02:48 by admin@192.168.100.100 (Local Database)

Updated 1/12/25 12:02:48 by admin@192.168.100.100 (Local Database)

Establishing DMZ Rules Regarding ICMP Protocol on the Firewall

The screenshot shows the pfSense Firewall Rules Edit interface. The top navigation bar includes the pfSense logo, a menu icon, and tabs for Firewall, Rules, and Edit. Below the navigation is a toolbar with icons for list, search, and help. The main area is titled "Edit Firewall Rule".

Action: Pass (selected from a dropdown menu). Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule. Set this option to disable this rule without removing it from the list.

Interface: DMZ (selected from a dropdown menu). Choose the interface from which packets must come to match this rule.

Address Family: IPv4 (selected from a dropdown menu). Select the Internet Protocol version this rule applies to.

Protocol: ICMP (selected from a dropdown menu). Choose which IP protocol this rule should match.

silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

DMZ

Choose the interface from which packets must come to match this rule.

Address

IPv4

Family

Select the Internet Protocol version this rule applies to.

Protocol

ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes

Alternate Host

Datagram conversion error

Echo reply

Echo request

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source

Invert
match

Any

Source Address

/

▼

Destination

Destination

Invert
match

Any

Destination Address

/

▼

Extra Options

Log

Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Regla ICMP request

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

 [Display Advanced](#)

Rule Information

Tracking ID 1736679996

Created 1/12/25 12:06:36 by admin@192.168.100.100 (Local Database)

Updated 1/12/25 12:09:35 by admin@192.168.100.100 (Local Database)

DMZ Firewall Rules

Firewall / Rules / DMZ

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

Floating WAN LAN DMZ **DMZ2**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP	*	*	*	*	*	none		Regla ICMP request	
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla trafico DNS	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	Web	*	none		Regla trafico web	

Establishing DMZ2 Rules Regarding Web Traffic on the Firewall with the Newly Created Port Rule

Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	DMZ2 Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	TCP Choose which IP protocol this rule should match.

Destination

Destination	<input type="checkbox"/> Invert match	Any	Destination Address /	
Destination Port Range	(other)	Web	(other)	Web
From	Custom	To	Custom	
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.				

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).	
Description	Regla trafico web
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	Display Advanced

Establishing DMZ2 Rules Regarding DNSs on the Firewall

Firewall / Rules / Edit

[☰](#) [List](#) [New](#) [?](#)

Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule
Set this option to disable this rule without removing it from the list.	
Interface	DMZ2
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	UDP
Choose which IP protocol this rule should match.	
Source	
-	Any
-	Source Address /

Destination

<u>Destination</u>	<input type="checkbox"/> Invert match	Any	Destination Address /
<u>Destination Port Range</u>	DNS (53) From	Custom	DNS (53) To
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			

Extra Options

<u>Log</u>	<input type="checkbox"/> Log packets that are handled by this rule <small>Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).</small>
<u>Description</u>	Regla tráfico DNS
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
<u>Advanced Options</u>	Display Advanced
 Save	

Establishing DMZ Rules Regarding ICMP Protocol on the Firewall

Firewall / Rules / Edit

Edit Firewall Rule		List	New	?
<u>Action</u>	Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.		
<u>Disabled</u>	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.		
<u>Interface</u>	DMZ2	Choose the interface from which packets must come to match this rule.		
<u>Address Family</u>	IPv4	Select the Internet Protocol version this rule applies to.		
<u>Protocol</u>	ICMP	Choose which IP protocol this rule should match.		
<u>ICMP Subtypes</u>	Datagram conversion error Echo reply Echo request			

<u>Source</u>	<input type="checkbox"/> Invert match	Any	/	Source Address	/
Destination					
<u>Destination</u>	<input type="checkbox"/> Invert match	Any	/	Destination Address	/
Extra Options					
Log	<input type="checkbox"/> Log packets that are handled by this rule	Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).			
Description	Regla ICMP Request				
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.					
Advanced Options	Display Advanced				
Save					

DMZ Firewall Rules

Firewall / Rules / DMZ2											
The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.											
Floating	WAN	LAN	DMZ	DMZ2							
Rules (Drag to Change Order)											
□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4	*	*	*	*	*	none		Regla ICMP Request	  
<input type="checkbox"/>	✓ 0/0 B	IPv4	*	*	*	53	*	none		Regla trafico DNS	  
<input type="checkbox"/>	✓ 0/0 B	IPv4	*	*	*	Web	*	none		Regla trafico web	  
↑ Add ↓ Add Delete Toggle Copy Save + Separator											

DHCP Status

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

Enter a search string or *nix regular expression to filter entries.

Leases

IP Address	MAC Address	Hostname	Description	Start	End	Actions
192.168.100.100	08:00:27:b7:5c:2e	DESKTOP-8CEQE17		2025/01/12 11:39:53	2025/01/12 13:39:53	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Lease Utilization

Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	192.168.100.100	192.168.100.200	1	101	0% of 101

Port Forward Configuration on WAN for NAT on the Firewall

pfSense COMMUNITY EDITION

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPt

Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>									

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#).

Firewall / NAT / Port Forward / Edit

?

Edit Redirect Entry

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule

This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface

WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address

IPv4

Family

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source
Display Advanced
Interface

WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address

IPv4

Family

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source
Display Advanced
Destination
 Invert
match.

WAN address

/
/
/

Type

Address/mask

Destination

Other

80

Other

80

port range

From port

Custom

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect

Address or Alias

/
/
/

Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4

UTM.keepcoding.local - Firewall: +

Not secure | https://192.168.100.1/firewall_nat_edit.php?after=-1

Yahoo | Trader Joe's Clay Ov... | ZIP Code 33596 Ma... | Search - Trainline | https://geomap.ffie... | InOutBoard | Other favorites

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)	
<u>Redirect target port</u>	Port
Other	80
Custom	
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.	
<u>Description</u>	Servidor Apache
A description may be entered here for administrative reference (not parsed).	
<u>No XMLRPC Sync</u>	<input type="checkbox"/> Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
<u>NAT reflection</u>	Use system default
<u>Filter rule association</u>	Add associated filter rule The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.
Save	

Blocking DMZ2 from Accessing DMZ

pfSense COMMUNITY EDITION

Firewall / Rules / Edit

Edit Firewall Rule

<u>Action</u>	Block	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
<u>Disabled</u>	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.	
<u>Interface</u>	DMZ	Choose the interface from which packets must come to match this rule.	
<u>Address Family</u>	IPv4	Select the Internet Protocol version this rule applies to.	
<u>Protocol</u>	Any	Choose which IP protocol this rule should match.	
Source			
<u>Source</u>	<input type="checkbox"/> Invert match	DMZ subnets	Source Address
Destination			
<u>Destination</u>	<input type="checkbox"/> Invert match	DMZ2 subnets	Destination Address
Extra Options			
<u>Log</u>	<input checked="" type="checkbox"/> Log packets that are handled by this rule	Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).	

Blocking LAN from Accessing DMZ

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' is set to 'Block'. The 'Disabled' checkbox is unchecked. The 'Interface' is set to 'DMZ'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'Any'. Under the 'Source' section, the 'Source' dropdown is set to 'DMZ subnets'. Under the 'Destination' section, the 'Destination' dropdown is set to 'LAN subnets'. In the 'Extra Options' section, the 'Log' checkbox is checked.

Edit Firewall Rule

Action: Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: DMZ
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source

Source: Invert match DMZ subnets Source Address /

Destination

Destination: Invert match LAN subnets Destination Address /

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Blocking DMZ from Accessing DMZ2

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' is set to 'Block'. The 'Disabled' checkbox is unchecked. The 'Interface' is set to 'DMZ2'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'Any'. Under the 'Source' section, the 'Source' dropdown is set to 'DMZ2 subnets'. Under the 'Destination' section, the 'Destination' dropdown is set to 'DMZ subnets'. In the 'Extra Options' section, the 'Log' checkbox is checked.

Edit Firewall Rule

Action: Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: DMZ2
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source

Source: Invert match DMZ2 subnets Source Address /

Destination

Destination: Invert match DMZ subnets Destination Address /

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

DMZ Rules

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / DMZ

Floating WAN LAN **DMZ** DMZ2

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/4 KiB	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Block LAN	
0/0 B	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		Block DMZ2	
0/0 B	IPv4 *	DMZ subnets	*	WAN subnets	*	*	none		Allow WAN	
0/0 B	IPv4 ICMP echoreq	*	*	*	*	*	*	none	Regla ICMP request	
10/110 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla trafico DNS	
15/22.32 MiB	IPv4 TCP	*	*	*	Web	*	none		Regla trafico web	

Add Add Delete Toggle Copy Save Separator

DMZ2 Rules

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / DMZ2

Floating WAN LAN **DMZ** **DMZ2**

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none		Block DMZ	
0/0 B	IPv4 ICMP echoreq	*	*	*	*	*	*	none	Regla ICMP Request	
0/163 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla trafico DNS	
2/3.64 MiB	IPv4 TCP	*	*	*	Web	*	none		Regla trafico web	

Add Add Delete Toggle Copy Save Separator

WAN Rules

Firewall / Rules / WAN

Floating WAN LAN DMZ DMZ2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	WAN subnets	*	DMZ subnets	*	*	none		Allow WAN TO DMZ	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.100.99	80 (HTTP)	*	none		NAT Servidor Apache	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	DMZ address	222	*	none		NAT cowrie SSH port forward 222	

Add Add Delete Toggle Copy Save Separator

LAN, DMZ and DMZ2 Configuration

A Windows 10 VM on LAN

A Kali Linux VM on DMZ

A Kali Linux VM on DMZ2

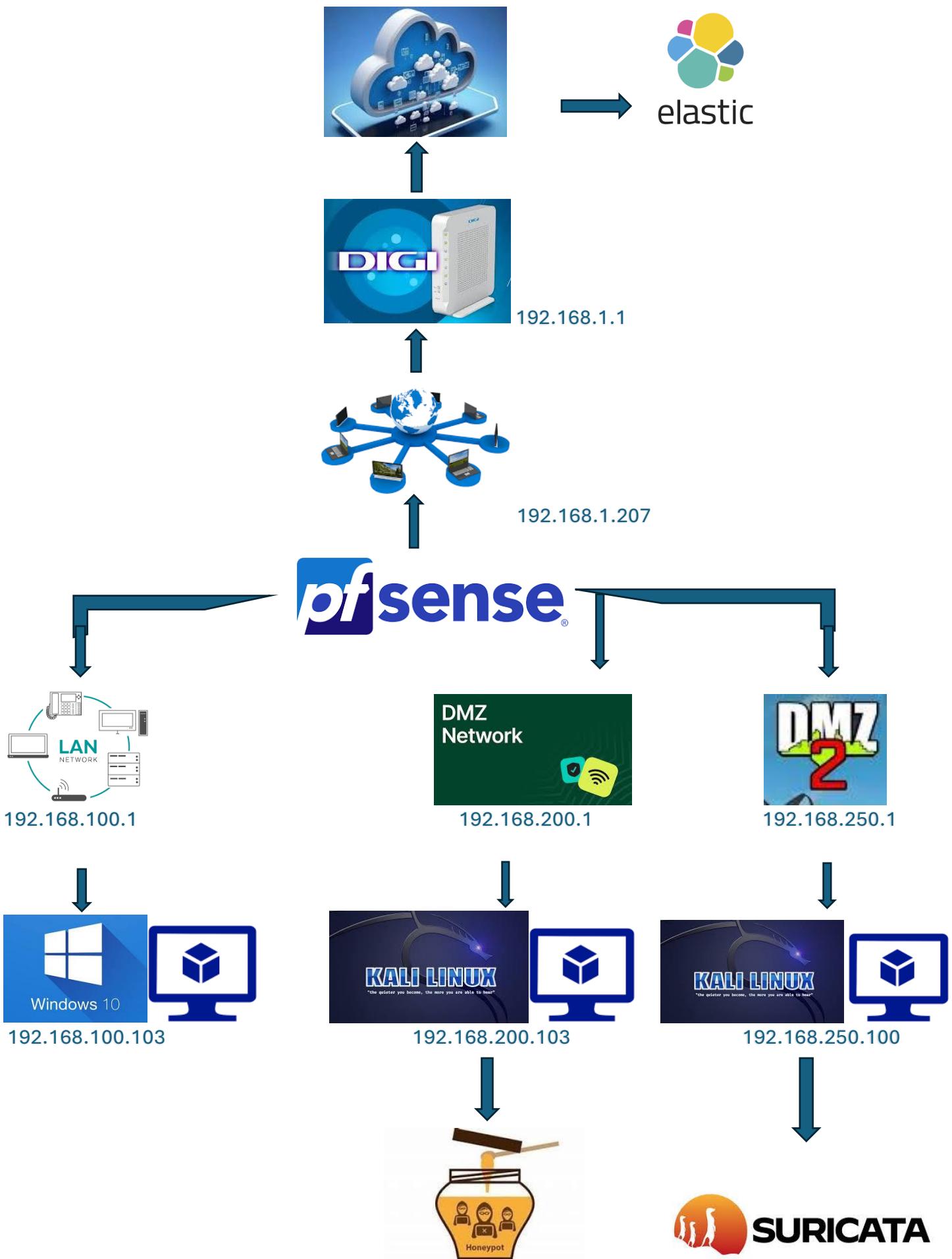
Then

A Honeypot on DMZ

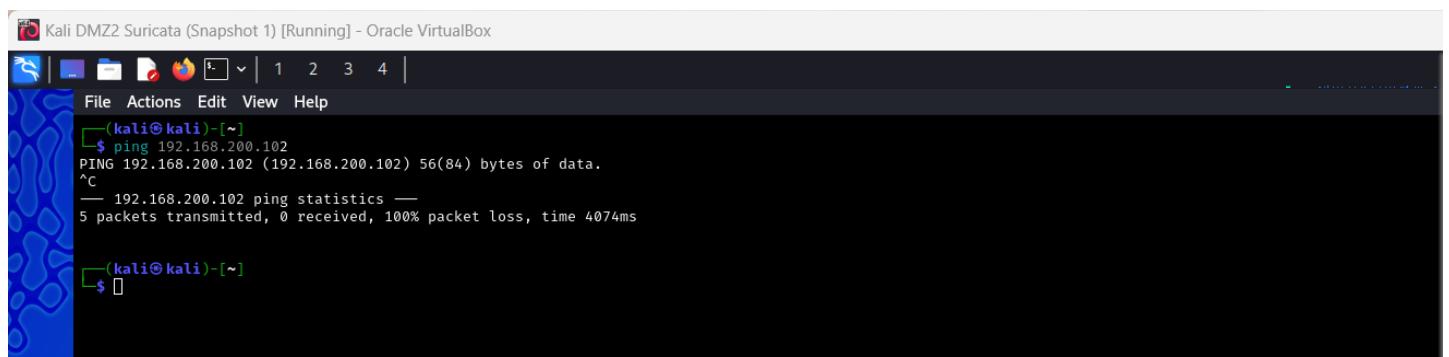
And

Suricata on DMZ2

Elastic Configuration to receive and show logs from the three virtual machines.

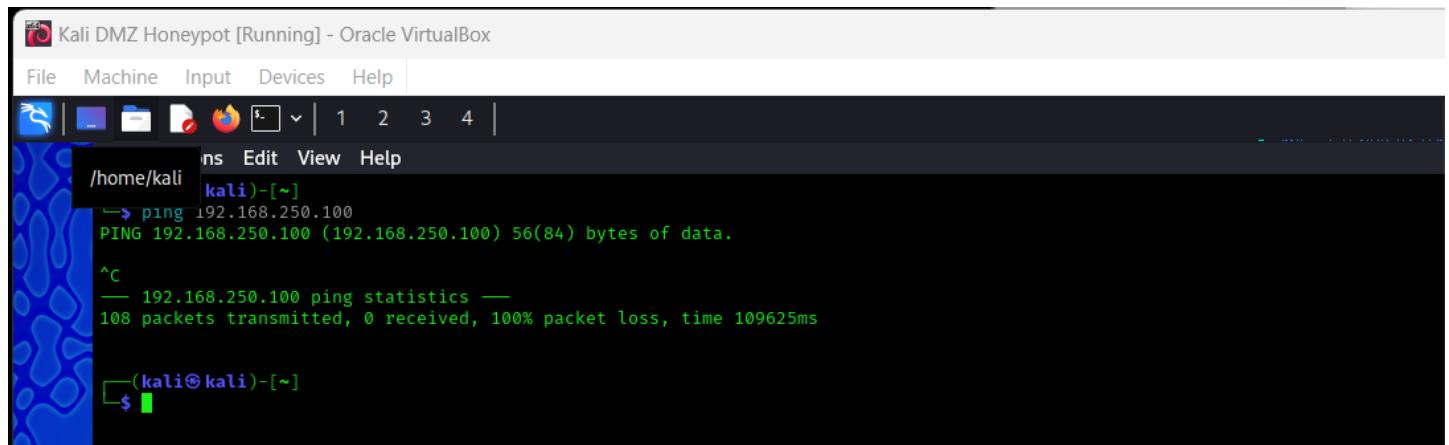


No communication between DMZ and DMZ2



```
(kali㉿kali)-[~]
$ ping 192.168.200.102
PING 192.168.200.102 (192.168.200.102) 56(84) bytes of data.
^C
--- 192.168.200.102 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4074ms

(kali㉿kali)-[~]
$
```



```
/home/kali
File Machine Input Devices Help
(kali㉿kali)-[~]
$ ping 192.168.250.100
PING 192.168.250.100 (192.168.250.100) 56(84) bytes of data.

^C
--- 192.168.250.100 ping statistics ---
108 packets transmitted, 0 received, 100% packet loss, time 109625ms

(kali㉿kali)-[~]
$
```

Elastic Cloud Configuration

Three Agent Policies: Windows with Windows Integration, Honeypot with Custom Logs Integration, and Suricata with Suricata Integration.

Agents - Fleet - Elastic

my-security-project-b39300.kb.us-east-1.aws.elastic.cloud/app/fleet/agents

Scholarships | Red R... Work Study and Stu... Levels in the Germa... My Account About | Quick Draw... Learn Japanese Log In to Your Anth... All Bookmarks

My_Security_project / Assets / Fleet / Agents

Give feedback Send feedback

Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

Ingest Overview Metrics Agent Info Metrics

Filter your data using KQL syntax Status 4 Tags 0 Agent policy 3 Upgrade available

Showing 3 agents Clear filters

Status	Host	Agent policy	CPU	Memory	Last activi...	Version	Actions
Healthy	vbox	Honeypot rev. 6	0.70 %	206 MB	1 minute ago	8.17.0	...
Healthy	kali	Suricata-Linux rev. 2	N/A	N/A	4 minutes ago	8.17.0	...
Healthy	DESKTOP-34K6US3	Windows rev. 2	N/A	N/A	29 seconds ago	8.17.0	...

Rows per page: 20

Agents - Fleet - Elastic

my-security-project / Assets / Fleet / Agent.policies / Honeypot

Give feedback Send feedback

Honeypot

Integrations Settings

View all agent policies Revision 6 Integrations 2 Agents 1 agent Last updated on Jan 18, 2025 Actions

Search... Namespace Add integration

Integration policy	Integration	Namespace	Output	Actions
log-1	Custom Logs v2.3.3	default	Default output	...
system-3	System v1.63.2	default	Default output	...

Suricata-Linux - Agent policies

my-security-project-b39300.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/e77e8ad4-3a8d-4cd2-9694-ce3a81eea210

Scholarships | Red R... Work Study and Stu... Levels in the Germa... My Account About | Quick Draw... Learn Japanese Log In to Your Anth... 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 Assets Machine learning

View all agent policies

Suricata-Linux

Integrations Settings

Search... Namespace Add integration

Integration policy ↑	Integration ↓	Namespace	Output	Actions
suricata-1	Suricata v2.21.4	default	Default output	...
system-2	System v1.63.2	default	Default output	...

Revision 2 Integrations 2 Agents 1 agent Last updated on Jan 17, 2025 Actions

Windows - Agent policies - Fleet

my-security-project-b39300.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/6b505e43-2809-4d3a-8f32-140298999117

Scholarships | Red R... Work Study and Stu... Levels in the Germa... My Account About | Quick Draw... Learn Japanese Log In to Your Anth... All Bookmarks

My_Security_project / Assets / Fleet / Agent_policies / Windows

Give feedback Send feedback

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore Assets Machine learning

View all agent policies

Windows

Integrations Settings

Search... Namespace Add integration

Integration policy ↑	Integration ↓	Namespace	Output	Actions
system-1	System v1.63.2	default	Default output	...
windows-1	Windows v2.3.6	default	Default output	...

Revision 2 Integrations 2 Agents 1 agent Last updated on Jan 17, 2025 Actions

[Honeypot Logs](#)

Documents (7) Patterns Field statistics		Sort fields 1
<input type="checkbox"/>	@timestamp ↗	↓ Summary
<input type="checkbox"/> ↗	Jan 18, 2025 @ 16:16:23.027	message 2025-01-18T10:13:37.646101Z [HoneyPotSSHTransport,2,127.0.0.1] SSH client hash fingerprint: 0babd4b68a5f3757987be75fe35ad60a @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a9206057 agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e...
<input type="checkbox"/> ↗	Jan 18, 2025 @ 16:16:23.027	message 2025-01-18T10:13:37.643112Z [HoneyPotSSHTransport,2,127.0.0.1] Remote SSH version: SSH-2.0-OpenSSH_9.9p1 Debian-3 @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a9206057 agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e...
<input type="checkbox"/> ↗	Jan 18, 2025 @ 16:16:23.026	message 2025-01-18T09:32:15.089090Z [HoneyPotSSHTransport,1,127.0.0.1] SSH client hash fingerprint: 0babd4b68a5f3757987be75fe35ad60a @timestamp Jan 18, 2025 @ 16:16:23.026 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a9206057 agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e...
<input type="checkbox"/> ↗	Jan 18, 2025 @ 16:16:23.026	message 2025-01-18T09:32:15.087587Z [HoneyPotSSHTransport,0,127.0.0.1] Remote SSH version: SSH-2.0-OpenSSH_9.9p1 Debian-3 @timestamp Jan 18, 2025 @ 16:16:23.026 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a9206057 agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e...
<input type="checkbox"/> ↗	Jan 18, 2025 @ 16:16:23.021	message 2025-01-18T09:22:08.412885Z [HoneyPotSSHTransport,0,127.0.0.1] SSH client hash fingerprint: 0babd4b68a5f3757987be75fe35ad60a @timestamp Jan 18, 2025 @ 16:16:23.021 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a9206057 agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e...
<input type="checkbox"/> ↗	Jan 18, 2025 @ 16:16:23.020	message 2025-01-18T09:18:29.373096Z [-] Ready to accept SSH connections @timestamp Jan 18, 2025 @ 16:16:23.020 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a9206057 agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 elastic_agent.snapshot false

HONEYHOT LOG (SSH)

```

{@timestamp": [
  "2025-01-18T15:16:23.027Z"
]
}
"agent.ephemeral_id": [
  "4835f548-938e-479e-98c0-98f0a9206057"
]
}
"agent.id": [
  "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
]
}
"agent.name": [
  "vbox"
]
}
"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": [
    "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
],
"elastic_agent.snapshot": [
    false
],
"elastic_agent.version": [
    "8.17.0"
],
"event.agent_id_status": [
    "verified"
],
"event.dataset": [
    "generic"
],
"event.ingested": [
    "2025-01-18T15:17:32.000Z"
],
"host.architecture": [
    "x86_64"
],
"host.containerized": [
    false
],
"host.hostname": [
    "vbox"
],
"host.id": [
    "b8a20186aff447eabf70e5019ed33327"
],
"host.ip": [
    "192.168.200.103",
    "fe80::a00:27ff:fe81:e1fb"
],
"host.mac": [
    "08-00-27-81-E1-FB"
],
"host.name": [
    "vbox"
],
"host.os.codename": [
    "Ubuntu"
]
```

```
"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/monica/cowrie/var/log/cowrie/cowrie.log"
].
"log.file.path.text": [
  "/home/monica/cowrie/var/log/cowrie/cowrie.log"
].
"log.offset": [
  8742
].
"message": [
  "2025-01-18T10:13:37.646101Z [HoneyPotSSHTransport,2,127.0.0.1] SSH client hassh fingerprint:
  0babd4b68a5f3757987be75fe35ad60a"
].
"_id": "AZR5_RMpTxFMiMikkiqg",
"_index": ".ds-logs-generic-default-2025.01.18-000001",
"_score": null
}
COWRIE LOG
```

Settings - Site settings Discover - Elastic

my-security-project-b39300.kb.us-east-1.aws.elastic.cloud/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now...)

Scholarships | Red R... Work Study and Stu... Levels in the German... My Account About | Quick Draw... Learn Japanese Log In to Your Anth...

All Bookmarks

Documents (13) Patterns Field statistics

Sort fields 1

@timestamp

Summary

Jan 19, 2025 @ 16:20:22.750 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 19, 2025 @ 16:20:22.750 agent.ephemeral_id 6a81f6ac-1ff2-46f9-a33d-fd6df7e2c agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 19, 2025 @ 16:20:22.750 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 19, 2025 @ 16:20:22.750 agent.ephemeral_id 6a81f6ac-1ff2-46f9-a33d-fd6df7e2c agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 19, 2025 @ 16:20:22.750 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 19, 2025 @ 16:20:22.750 agent.ephemeral_id 6a81f6ac-1ff2-46f9-a33d-fd6df7e2c agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 19, 2025 @ 16:20:22.749 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 19, 2025 @ 16:20:22.749 agent.ephemeral_id 6a81f6ac-1ff2-46f9-a33d-fd6df7e2c agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 19, 2025 @ 16:20:22.749 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log message 2025-01-19T10:20:21.769680Z [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 2.4.11.0 (/home/monica/cowrie/cowrie-env/bin/python3.12.8) starting up. @timestamp Jan 19, 2025 @ 16:20:22.749 agent.ephemeral_id 6a81f6ac-1ff2-46f9-a33d-fd6df7e2c agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox agent.type filebeat agent.version 8.17.0 data_stream.dataset generic...

Jan 19, 2025 @ 16:20:22.749 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 19, 2025 @ 16:20:22.749 agent.ephemeral_id 6a81f6ac-1ff2-46f9-a33d-fd6df7e2c agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 19, 2025 @ 16:20:22.749 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log message 2025-01-19T10:20:21.764854Z [-] Cowrie Version 2.6.1 @timestamp Jan 19, 2025 @ 16:20:22.749 agent.ephemeral_id 6a81f6ac-1ff2-46f9-a33d-fd6df7e2c agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 19, 2025 @ 16:20:22.749 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 19, 2025 @ 16:20:22.749 agent.ephemeral_id 6a81f6ac-1ff2-46f9-a33d-fd6df7e2c agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 19, 2025 @ 16:20:22.749 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log message 2025-01-19T10:20:21.764594Z [-] Removing stale pidfile /home/monica/cowrie/var/run/cowrie.pid @timestamp Jan 19, 2025 @ 16:20:22.749 agent.ephemeral_id 6a81f6ac-1ff2-46f9-a33d-fd6df7e2c agent.id 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dda06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Rows per page: 100

HONEYHOT LOG (COWRIE)

{

"@timestamp": [

"2025-01-19T15:20:22.750Z"

]

"agent.ephemeral_id": [

"6a81f6ac-1ff2-46f9-a33d-fd6df7e2c"

]

"agent.id": [

"73298f8b-8831-4d8c-97d3-7dda06b2e1e4"

]

"agent.name": [

"vbox"

]

"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": [
    "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
],
"elastic_agent.snapshot": [
    false
],
"elastic_agent.version": [
    "8.17.0"
],
"event.agent_id_status": [
    "verified"
],
"event.dataset": [
    "generic"
],
"event.ingested": [
    "2025-01-19T15:20:41.000Z"
],
"host.architecture": [
    "x86_64"
],
"host.containerized": [
    false
],
"host.hostname": [
    "vbox"
],
"host.id": [
    "b8a20186aff447eabf70e5019ed33327"
],
"host.ip": [
    "192.168.200.103",
    "fe80::a00:27ff:fe81:e1fb"
],
"host.mac": [

```

"08-00-27-81-E1-FB"

1.

"host.name": [

 "vbox"

1.

"host.os.codename": [

 "kali-rolling"

1.

"host.os.family": [

 "debian"

1.

"host.os.kernel": [

 "6.11.2-amd64"

1.

"host.os.name": [

 "Kali GNU/Linux"

1.

"host.os.name.text": [

 "Kali GNU/Linux"

1.

"host.os.platform": [

 "kali"

1.

"host.os.type": [

 "linux"

1.

"host.os.version": [

 "2024.4"

1.

"input.type": [

 "log"

1.

"log.file.path": [

 "/home/monica/cowrie/var/log/cowrie/cowrie.log"

1.

"log.file.path.text": [

 "/home/monica/cowrie/var/log/cowrie/cowrie.log"

1.

"log.offset": [

 972

1.

"message": [

 "2025-01-19T10:20:21.820728Z [-] Ready to accept SSH connections"

1.

```
"_id": "AZR_JhMpTxFMiMjevX6A",
"_index": ".ds-logs-generic-default-2025.01.18-000001",
"_score": null
}
```

LOG

```
{
  "@timestamp": [
    "2025-01-19T12:12:37.017Z"
  ],
  "agent.ephemeral_id": [
    "c306da15-d257-4eff-9786-2770ed2f8f9c"
  ],
  "agent.id": [
    "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
  ],
  "agent.name": [
    "vbox"
  ],
  "agent.type": [
    "filebeat"
  ],
  "agent.version": [
    "8.17.0"
  ],
  "component.binary": [
    "filebeat"
  ],
  "component.dataset": [
    "elastic_agent.filebeat"
  ],
  "component.id": [
    "log-default"
  ],
  "component.type": [
    "log"
  ],
  "data_stream.dataset": [
    "elastic_agent.filebeat"
  ],
  "data_stream.namespace": [
    "default"
  ],
  "data_stream.type": [
    "log"
  ]
}
```

```
"logs"
  [
    {
      "ecs.version": [
        "8.0.0"
      ],
      "elastic_agent.id": [
        "73298f8b-8831-4d8c-97d3-7dda06b2e1e4"
      ],
      "elastic_agent.snapshot": [
        false
      ],
      "elastic_agent.version": [
        "8.17.0"
      ],
      "event.agent_id_status": [
        "verified"
      ],
      "event.dataset": [
        "elastic_agent.filebeat"
      ],
      "event.ingested": [
        "2025-01-19T12:12:58.000Z"
      ],
      "host.architecture": [
        "x86_64"
      ],
      "host.containerized": [
        false
      ],
      "host.hostname": [
        "vbox"
      ],
      "host.id": [
        "b8a20186aff447eabf70e5019ed33327"
      ],
      "host.ip": [
        "192.168.200.103",
        "fe80::a00:27ff:fe81:e1fb"
      ],
      "host.mac": [
        "08-00-27-81-E1-FB"
      ],
      "host.name": [
        "vbox"
      ]
    }
  ]
}
```

```
1.
"host.os.codename": [
    "kali-rolling"
1.
"host.os.family": [
    "debian"
1.
"host.os.kernel": [
    "6.11.2-amd64"
1.
"host.os.name": [
    "Kali GNU/Linux"
1.
"host.os.name.text": [
    "Kali GNU/Linux"
1.
"host.os.platform": [
    "kali"
1.
"host.os.type": [
    "linux"
1.
"host.os.version": [
    "2024.4"
1.
"input.type": [
    "filestream"
1.
"input_id": [
    "cfb5c92f-eb75-42ca-aa73-233b83186800"
1.
"log.file.device_id": [
    "2049"
1.
"log.file.inode": [
    "1204044"
1.
"log.file.path": [
    "/opt/Elastic/Agent/data/elastic-agent-8.17.0-96f2b9/logs/elastic-agent-20250119.ndjson"
1.
"log.level": [
    "info"
1.
"log.logger": [
```

```
"input"
  [
    "log.offset": [
      80155
    ],
    "log.origin.file.line": [
      179
    ],
    "log.origin.file.name": [
      "log/input.go"
    ],
    "log.origin.function": [
      "github.com/elastic/beats/v7/filebeat/input/log.NewInput"
    ],
    "log.source": [
      "log-default"
    ],
    "message": [
      "Configured paths: [/home/monica/cowrie/var/log/cowrie/*.log]"
    ],
    "service.name": [
      "filebeat"
    ],
    "_id": "AZR-exMpTxFMiMgBp7dL",
    "_index": ".ds-logs-elastic_agent.filebeat-default-2025.01.17-000001",
    "_score": null
  ]
}
```

SURICATA LOGS

Documents (1,859)		Patterns	Field statistics	
<input type="checkbox"/>	@timestamp	<input type="button" value="Summary"/>		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.980	@timestamp Jan 19, 2025 @ 16:09:01.980 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 3.229.246.159 destination.as.number 14,618 destination.as.organization.name AMAZON-AES destination.domain b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.759	@timestamp Jan 19, 2025 @ 16:09:01.759 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 3.229.246.159 destination.as.number 14,618 destination.as.organization.name AMAZON-AES destination.domain b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.685	@timestamp Jan 19, 2025 @ 16:09:01.685 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.25.0.1 destination.ip 192.168.250.1 destination.port 53 dns.answers.data [prd-awsuse1-cp-app-6d.us-east-1.aws.elastic.cloud, ingress-proxy-us-east-1d-80f6eda6036]		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.685	@timestamp Jan 19, 2025 @ 16:09:01.685 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.25.0.1 destination.ip 192.168.250.1 destination.port 53 dns.answers.data [prd-awsuse1-cp-app-6d.us-east-1.aws.elastic.cloud, ingress-proxy-us-east-1d-80f6eda6036]		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.684	@timestamp Jan 19, 2025 @ 16:09:01.684 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.25.0.1 destination.ip 192.168.250.1 destination.port 53 dns.question.name b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.684	@timestamp Jan 19, 2025 @ 16:09:01.684 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.25.0.1 destination.ip 192.168.250.1 destination.port 53 dns.question.name b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.673	@timestamp Jan 19, 2025 @ 16:09:01.673 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 3.229.246.159 destination.as.number 14,618 destination.as.organization.name AMAZON-AES destination.domain b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.498	@timestamp Jan 19, 2025 @ 16:09:01.498 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.25.0.1 destination.ip 192.168.250.1 destination.port 53 dns.answers.data [prd-awsuse1-cp-app-6d.us-east-1.aws.elastic.cloud, ingress-proxy-us-east-1d-80f6eda6036]		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.498	@timestamp Jan 19, 2025 @ 16:09:01.498 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.25.0.1 destination.ip 192.168.250.1 destination.port 53 dns.answers.data [prd-awsuse1-cp-app-6d.us-east-1.aws.elastic.cloud, ingress-proxy-us-east-1d-80f6eda6036]		
<input type="checkbox"/>	Jan 19, 2025 @ 16:09:01.497	@timestamp Jan 19, 2025 @ 16:09:01.497 agent.ephemeral_id 0becd8f7-07c7-4699-bc03-f65bbb632e01 agent.id 04c9f0e3-05a9-449c-8be5-40e5824fa3ac agent.name kali agent.type filebeat agent.version 8.17.0 data_stream.dataset suricata.eve data_stream.namespace default data_stream.type logs destination.address 192.168.25.0.1 destination.ip 192.168.250.1 destination.port 53 dns.question.name b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud		

Rows per page: 100 < 1 2 3 4 5 >

SURICATA LOG

{

"@timestamp": [

"2025-01-19T15:09:01.980Z"

]

"agent.ephemeral_id": [

"0becd8f7-07c7-4699-bc03-f65bbb632e01"

]

"agent.id": [

"04c9f0e3-05a9-449c-8be5-40e5824fa3ac"

]

"agent.name": [

"kali"

]

"agent.type": [

"filebeat"

]

"agent.version": [

"8.17.0"

]

"data_stream.dataset": [

"suricata.eve"

]

```
"data_stream.namespace": [
    "default"
],
"data_stream.type": [
    "logs"
],
"destination.address": [
    "3.229.246.159"
],
"destination.as.number": [
    14618
],
"destination.as.organization.name": [
    "AMAZON-AES"
],
"destination.as.organization.name.text": [
    "AMAZON-AES"
],
"destination.domain": [
    "b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud"
],
"destination.geo.city_name": [
    "Ashburn"
],
"destination.geo.continent_name": [
    "North America"
],
"destination.geo.country_iso_code": [
    "US"
],
"destination.geo.country_name": [
    "United States"
],
"destination.geo.location": [
    {
        "coordinates": [
            -77.49030003324151,
            39.046899997629225
        ],
        "type": "Point"
    }
],
"destination.geo.region_iso_code": [
    "US-VA"
]
```

```
1.
"destination.geo.region_name": [
    "Virginia"
1.
"destination.ip": [
    "3.229.246.159"
1.
"destination.port": [
    443
1.
"ecs.version": [
    "8.11.0"
1.
"elastic_agent.id": [
    "04c9f0e3-05a9-449c-8be5-40e5824fa3ac"
1.
"elastic_agent.snapshot": [
    false
1.
"elastic_agent.version": [
    "8.17.0"
1.
"event.agent_id_status": [
    "verified"
1.
"event.category": [
    "network"
1.
"event.created": [
    "2025-01-19T15:09:02.557Z"
1.
"event.dataset": [
    "suricata.eve"
1.
"event.ingested": [
    "2025-01-19T15:09:13.000Z"
1.
"event.kind": [
    "event"
1.
"event.module": [
    "suricata"
1.
"event.type": [
```

```
"protocol"
  [
    "input.type": [
      "log"
        [
          "log.file.path": [
            "/var/log/suricata/eve.json"
          ],
          "log.offset": [
            932835
          ],
          "network.community_id": [
            "1:mIYSy0WPZDkZk0A7C4wxAWV/9rE="
          ],
          "network.protocol": [
            "tls"
          ],
          "network.transport": [
            "tcp"
          ],
          "observer.hostname": [
            "kali"
          ],
          "observer.ip": [
            "192.168.250.100",
            "fe80::c6b6:99d7:2858:f4ac",
            "172.17.0.1"
          ],
          "observer.mac": [
            "02-42-28-1D-78-B4",
            "08-00-27-CB-7E-F5"
          ],
          "observer.product": [
            "Suricata"
          ],
          "observer.type": [
            "ids"
          ],
          "observer.vendor": [
            "OISF"
          ],
          "related.hosts": [
            "b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud"
          ]
        ]
      ]
    ]
  ]
}
```

```
"related.ip": [
    "192.168.250.100",
    "3.229.246.159"
],
{
    "source.address": [
        "192.168.250.100"
    ],
    "source.ip": [
        "192.168.250.100"
    ],
    "source.port": [
        58890
    ],
    "suricata.eve.event_type": [
        "tls"
    ],
    "suricata.eve.flow_id": [
        "1538408431940806"
    ],
    "suricata.eve.in_iface": [
        "eth0"
    ],
    "suricata.eve.pkt_src": [
        "wire/pcap"
    ],
    "suricata.eve.tls.sni": [
        "b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud"
    ],
    "suricata.eve.tls.version": [
        "TLS 1.3"
    ],
    "tags": [
        "forwarded",
        "suricata-eve"
    ],
    "tls.client.server_name": [
        "b393006a79224741968d308f42f39f06.es.us-east-1.aws.elastic.cloud"
    ],
    "tls.version": [
        "1.3"
    ],
    "tls.version_protocol": [
        "tls"
    ]
}
```

```
"_id": "AZR_HBMpTxFMiMhftn7-",  
"_index": ".ds-logs-suricata.eve-default-2025.01.17-000001",  
"_score": null  
}
```

LOG

```
{  
"@timestamp": [  
"2025-01-16T13:26:35.520Z"  
],  
"agent.ephemeral_id": [  
"e6f3b52c-fe37-4357-9223-35f6c361c328"  
],  
"agent.id": [  
"f752d655-1242-4066-888a-8c1c9043f3e5"  
],  
"agent.name": [  
"kali"  
],  
"agent.type": [  
"filebeat"  
],  
"agent.version": [  
"8.17.0"  
],  
"data_stream.dataset": [  
"suricata.eve"  
],  
"data_stream.namespace": [  
"default"  
],  
"data_stream.type": [  
"logs"  
],  
"destination.address": [  
"35.193.143.25"  
],  
"destination.as.number": [  
396982  
],  
"destination.as.organization.name": [  
"GOOGLE-CLOUD-PLATFORM"  
],  
"destination.as.organization.name.text": [  
]
```

"GOOGLE-CLOUD-PLATFORM"
],
"destination.domain": [
"add9e71f48304c70804ecc975a324e3.us-central1.gcp.cloud.es.io"
],
"destination.geo.city_name": [
"Council Bluffs"
],
"destination.geo.continent_name": [
"North America"
],
"destination.geo.country_iso_code": [
"US"
],
"destination.geo.country_name": [
"United States"
],
"destination.geo.location": [
{
"coordinates": [
-95.8517,
41.2591
],
"type": "Point"
}
],
"destination.geo.region_iso_code": [
"US-IA"
],
"destination.geo.region_name": [
"Iowa"
],
"destination.ip": [
"35.193.143.25"
],
"destination.port": [
443
],
"ecs.version": [
"8.11.0"
],
"elastic_agent.id": [
"f752d655-1242-4066-888a-8c1c9043f3e5"
],

```
"elastic_agent.snapshot": [
  false
],
"elastic_agent.version": [
  "8.17.0"
],
"event.agent_id_status": [
  "verified"
],
"event.category": [
  "network"
],
"event.created": [
  "2025-01-16T13:26:35.675Z"
],
"event.dataset": [
  "suricata.eve"
],
"event.ingested": [
  "2025-01-16T13:26:49.000Z"
],
"event.kind": [
  "event"
],
"event.module": [
  "suricata"
],
"event.type": [
  "protocol"
],
"input.type": [
  "log"
],
"log.file.path": [
  "/var/log/suricata/eve.json"
],
"log.offset": [
  1430128
],
"network.community_id": [
  "1:+FxyBDIZf2ZBD4x5BsAYWnWTJyc="
],
"network.protocol": [
  "tls"
]
```

```
],
"network.transport": [
"tcp"
],
"observer.hostname": [
"kali"
],
"observer.ip": [
"172.17.0.1"
],
"observer.mac": [
"02-42-23-12-56-E6",
"08-00-27-CB-7E-F5"
],
"observer.product": [
"Suricata"
],
"observer.type": [
"ids"
],
"observer.vendor": [
"OISF"
],
"related.hosts": [
"add9e71f48304c70804ecc975a324e3.us-central1.gcp.cloud.es.io"
],
"related.ip": [
"192.168.250.100",
"35.193.143.25"
],
"source.address": [
"192.168.250.100"
],
"source.ip": [
"192.168.250.100"
],
"source.port": [
51934
],
"suricata.eve.event_type": [
"tls"
],
"suricata.eve.flow_id": [
"1121390172740121"
]
```

```
],
"suricata.eve.in_iface": [
"eth0"
],
"suricata.eve.pkt_src": [
"wire/pcap"
],
"suricata.eve.tls.sni": [
"add9e71f48304c70804ecc975a324e3.us-central1.gcp.cloud.es.io"
],
"suricata.eve.tls.version": [
"TLS 1.3"
],
"tags": [
"forwarded",
"suricata-eve"
],
"tls.client.server_name": [
"add9e71f48304c70804ecc975a324e3.us-central1.gcp.cloud.es.io"
],
"tls.version": [
"1.3"
],
"tls.version_protocol": [
"tls"
],
"_id": "UwVLb5QBo0yIF2SyjXhq",
"_index": ".ds-logs-suricata.eve-default-2025.01.15-000001",
"_score": null
}
```

WINDOWS LOGS

The screenshot shows a web browser window with the title "Discover - Elastic". The URL is "my-security-project-b39300.kb.us-east-1.aws.elastic.cloud/app/discover/?_g=(filters:!(),refreshInterval:(pause:1t,value:60000),time:(from:'202...". The page displays a table of log entries with the following columns: @timestamp, Patterns, and Field statistics. The table has 6,090 rows. The logs are primarily about Windows updates and installations, with entries like "Installation Successful: Windows successfully installed the following update: 9WZDNCRFJBH4-Microsoft.Windows.Photos" and "Update started downloading an update. @timestamp Jan 20, 2025 @ 02:02:51.221 agent.type filebeat agent.version 8.17.0 data_stream.dataset system.sys...". The logs also mention various Microsoft services and components like DESKTOP-34K6US3 and filebeat agent IDs.

WINDOWS LOG

```
{  
  "@timestamp": [  
    "2025-01-20T01:02:53.932Z"  
  ],  
  "agent.ephemeral_id": [  
    "c56c0f46-71f1-4013-bd89-d65419a96031"  
  ],  
  "agent.id": [  
    "3f2c0aa7-171b-4368-a2a2-9b9bd5052937"  
  ],  
  "agent.name": [  
    "DESKTOP-34K6US3"  
  ],  
  "agent.name.text": [  
    "DESKTOP-34K6US3"  
  ],  
  "agent.type": [  
    "filebeat"  
  ]  
}
```

```
1.
"agent.version": [
  "8.17.0"
]
1.
"data_stream.dataset": [
  "system.system"
]
1.
"data_stream.namespace": [
  "default"
]
1.
"data_stream.type": [
  "logs"
]
1.
"ecs.version": [
  "8.11.0"
]
1.
"elastic_agent.id": [
  "3f2c0aa7-171b-4368-a2a2-9b9bd5052937"
]
1.
"elastic_agent.snapshot": [
  false
]
1.
"elastic_agent.version": [
  "8.17.0"
]
1.
"event.action": [
  "Windows Update Agent"
]
1.
"event.agent_id_status": [
  "verified"
]
1.
"event.code": [
  "43"
]
1.
"event.created": [
  "2025-01-20T01:02:55.199Z"
]
1.
"event.dataset": [
  "system.system"
]
1.
"event.ingested": [
  "2025-01-19T16:03:12.000Z"
]
1.
"event.kind": [

```

```
"event"
].
"event.module": [
    "system"
].
"event.provider": [
    "Microsoft-Windows-UpdateClient"
].
"host.architecture": [
    "x86_64"
].
"host.hostname": [
    "DESKTOP-34K6US3"
].
"host.id": [
    "c5a4c4f9-536a-40b9-b44c-56f35adff986"
].
"host.ip": [
    "fe80::28d9:f8f2:b83:5f13",
    "192.168.100.103"
].
"host.mac": [
    "08-00-27-B8-8F-2B"
].
"host.name": [
    "desktop-34k6us3"
].
"host.os.build": [
    "19045.2965"
].
"host.os.family": [
    "windows"
].
"host.os.kernel": [
    "10.0.19041.2965 (WinBuild.160101.0800)"
].
"host.os.name": [
    "Windows 10 Home"
].
"host.os.name.text": [
    "Windows 10 Home"
].
"host.os.platform": [
    "windows"
]
```

```
1.
"host.os.type": [
    "windows"
1.
"host.os.version": [
    "10.0"
1.
"input.type": [
    "winlog"
1.
"log.level": [
    "information"
1.
"message": [
    "Installation Started: Windows has started installing the following update: 9NBLGGH51CLL-
Microsoft.Services.Store.Engagement"
1.
"winlog.api": [
    "wineventlog"
1.
"winlog.channel": [
    "System"
1.
"winlog.computer_name": [
    "DESKTOP-34K6US3"
1.
"winlog.event_data.updateGuid": [
    "{3f6608fd-a63e-4c0a-ac23-3d0a81a8fe70}"
1.
"winlog.event_data.updateRevisionNumber": [
    "1"
1.
"winlog.event_data.updateTitle": [
    "9NBLGGH51CLL-Microsoft.Services.Store.Engagement"
1.
"winlog.event_id": [
    "43"
1.
"winlog.keywords": [
    "Installation",
    "Started"
1.
"winlog.opcode": [
    "Installation"
```

```
1.
"winlog.process.pid": [
  4224
1.
"winlog.process.thread.id": [
  9428
1.
"winlog.provider_guid": [
  "{945a8954-c147-4acd-923f-40c45405a658}"
1.
"winlog.provider_name": [
  "Microsoft-Windows-WindowsUpdateClient"
1.
"winlog.record_id": [
  "648"
1.
"winlog.task": [
  "Windows Update Agent"
1.
"winlog.user.domain": [
  "NT AUTHORITY"
1.
"winlog.user.identifier": [
  "S-1-5-18"
1.
"winlog.user.name": [
  "SYSTEM"
1.
"winlog.user.type": [
  "User"
1.
"winlog.version": [
  1
1.
"_id": "AZR_TRMpTxFMiMjKzJPG",
"_index": ".ds-logs-system.system-default-2025.01.17-000001",
"_score": null
}
```

Discover - Elastic

my-security-project-b39300.kb.us-east-1.aws.elastic.cloud/app/discover/?_g=(filters:[],refreshInterval:(pause:1t,value:60000),time:(from:now-1h,until:now))

Scholarships | Red R... Work Study and Stu... Levels in the German... My Account About | Quick Draw... Learn Japanese Log In to Your Anth... All Bookmarks

Documents (119) Patterns Field statistics Sort fields

Summary

Jan 18, 2025 @ 17:50:09.329 message Configured paths: [/home/monica/cowrie/var/log/cowrie/*.log] @timestamp Jan 18, 2025 @ 17:50:09.329 agent.ephemeral_id 25bc7940-f9da-4980-8268-705793c0 bbad agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox agent.type filebeat agent.version 8.17.0 component.binary filebeat component.dataset elastici_agent.filebeat component.log log-default component.type log data_stream.dataset elastic_agent.filebeat data_stream.namespace default data_stream.type log...

Jan 18, 2025 @ 16:16:23.028 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 18, 2025 @ 16:16:23.028 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 18, 2025 @ 16:16:23.028 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 18, 2025 @ 16:16:23.028 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 18, 2025 @ 16:16:23.027 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 18, 2025 @ 16:16:23.027 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 18, 2025 @ 16:16:23.027 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 18, 2025 @ 16:16:23.027 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 18, 2025 @ 16:16:23.027 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 18, 2025 @ 16:16:23.027 log.message 2025-01-18T10:14:32.145447Z [HoneyPotSSHTransport,2,127.0.0.1] Closing TTY Log: var/lib/cowrie/tty/9b75b44c80ba7e5e8a2af4803b36dd99dec54be9fca111b7bfd16ae4c248a61 after 53.1 seconds @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 18, 2025 @ 16:16:23.027 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Jan 18, 2025 @ 16:16:23.027 log.file.path.text /home/monica/cowrie/var/log/cowrie/cowrie.log @timestamp Jan 18, 2025 @ 16:16:23.027 agent.ephemeral_id 4835f548-938e-479e-98c0-98f0a920605 7 agent.id 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 agent.name vbox 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 73298f8b-8831-4d8c-97d3-7dd06b2e1e4 elastic_agent.snapshot false elastic_agent.version 8.17...

Rows per page: 100

All logs were received successfully.

The rules of the project specified that DMZ2 was not allowed to access the DMZ, however...



...No rule was specified to prevent Monica from accessing the DMZ. 😊

