

PROJETO Digital Security -UFCD 9194

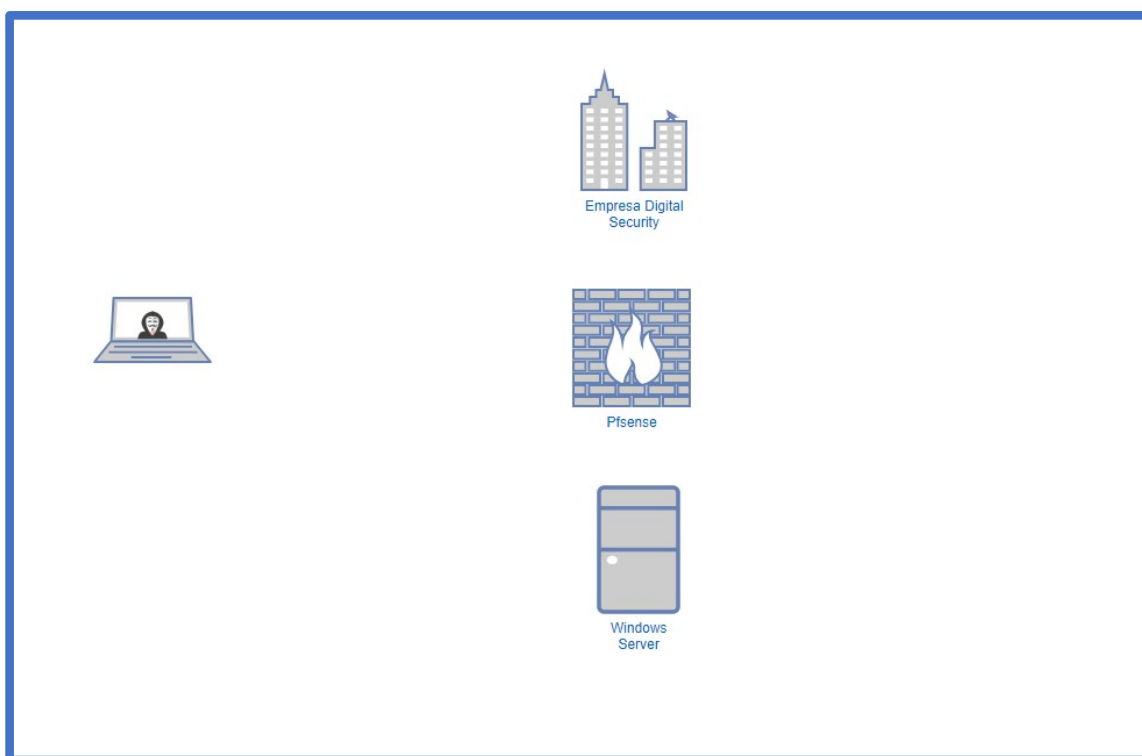
Introdução à cibersegurança e à ciberdefesa

Objetivos do projeto:

- a. Projetar e aplicar todos os conhecimentos adquiridos ao nível de redes, sistemas operativos e segurança;

Topologia de Rede:

No que concerne à parte de servidores e serviços pede-se que sejam instalados e configurados de acordo com o seguinte diagrama:



Endereçamento:

Rede: 192.168.30.0/24

Windows Server: 192.168.30.1

PfSense Bruxelas: 192.168.30.254

Kali Linux: DHCP

Domínio: digitalsecurity.pt

Considerações iniciais e instruções:

- a. Cada formando projeta e configura a topologia apresentada de acordo com as diretrizes definidas nos pontos seguintes.
- b. Qualquer situação omissa que não tenha sido mencionada neste enunciado, deve ser colocada ao formador, para posteriormente ser esclarecida/comunicada a todos os formandos.
 - i. Deve ser enviado ao formador um Pdf com um printscreen de todas as configurações feitas.

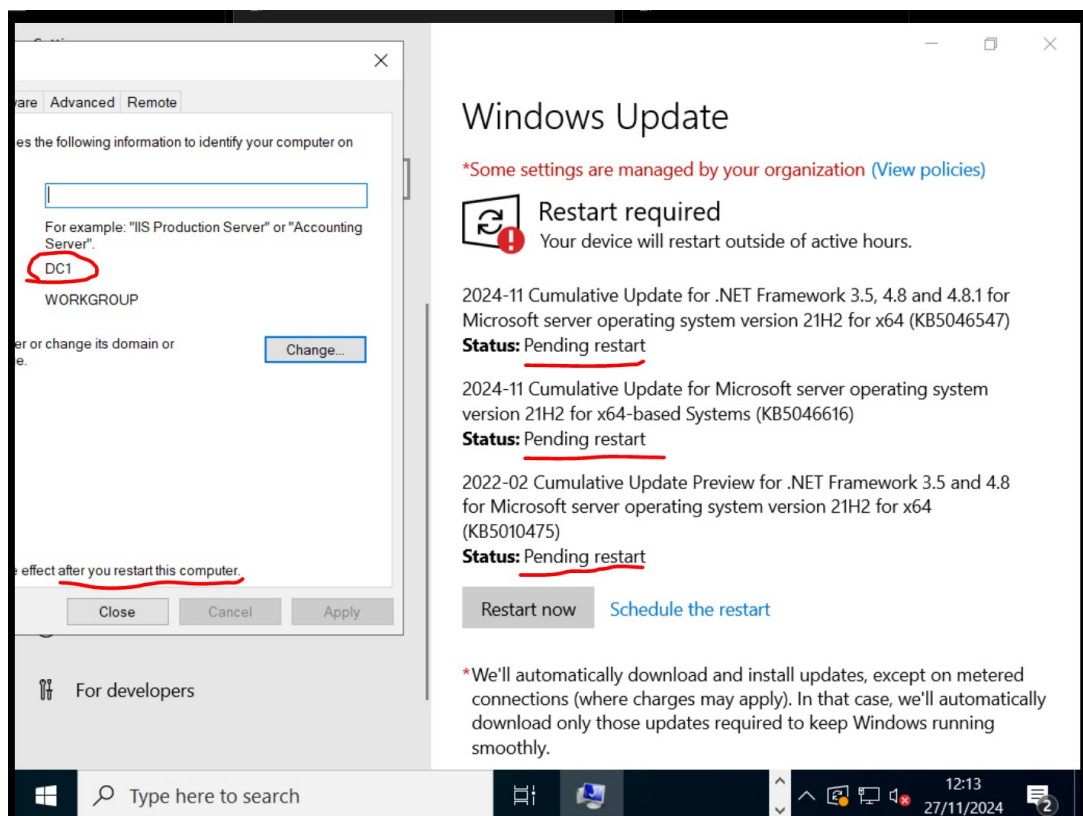
Serviços abordados

1. DNS - Domain Name System
2. DHCP - Dynamic Host Configuration Protocol
3. AD DS - Active Directory Domain Services
4. Certificados

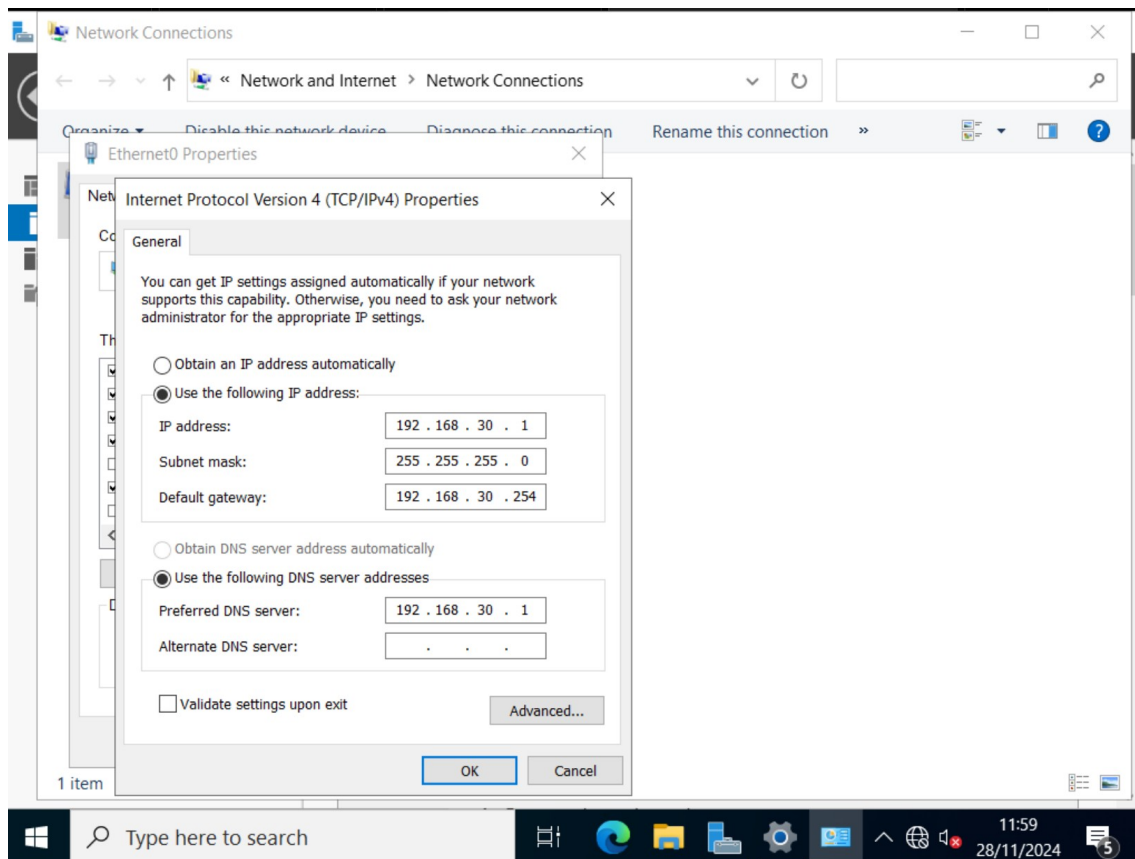
Windows Server

Ações a desenvolver:

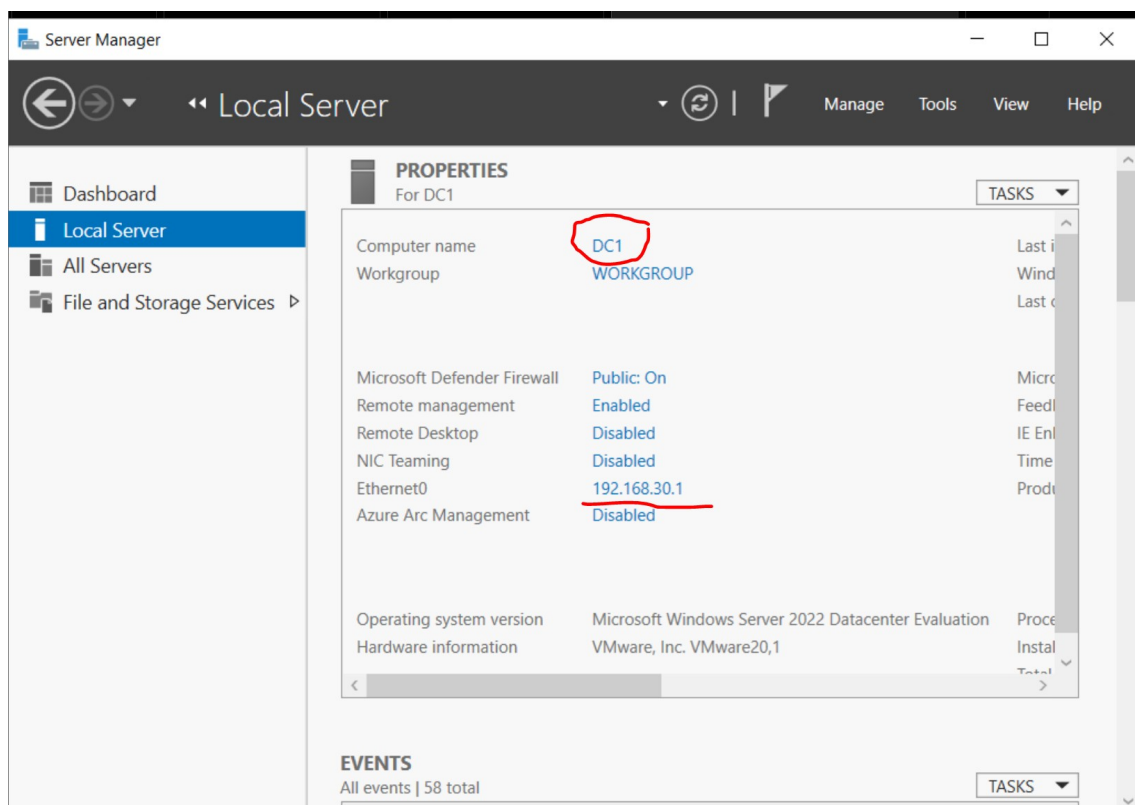
- Instalar o Windows Server



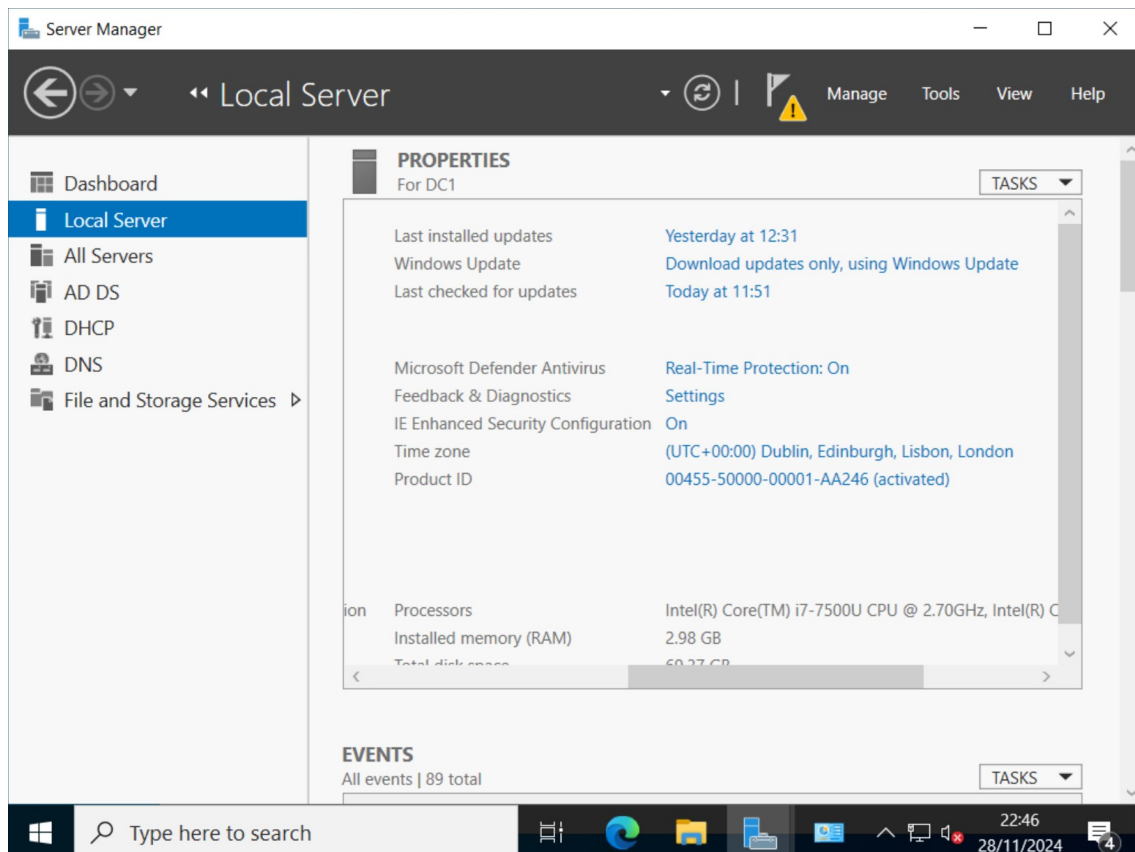
- Colocar IP estático no Windows Server



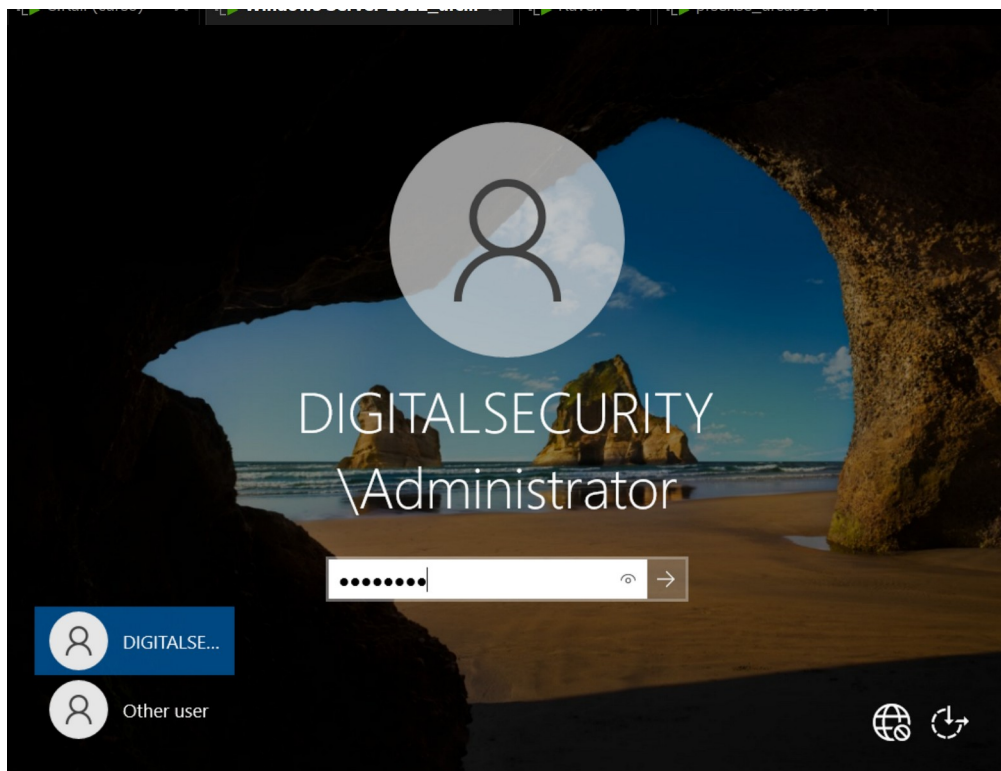
- Mudar o nome da máquina para DC1



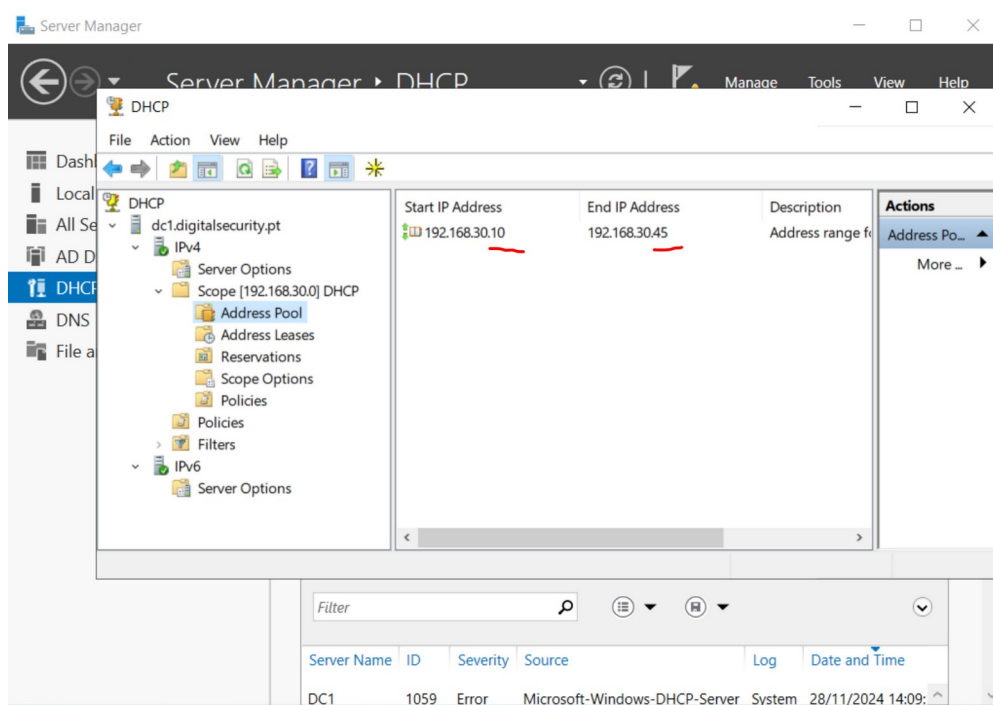
- Mudar o timezone



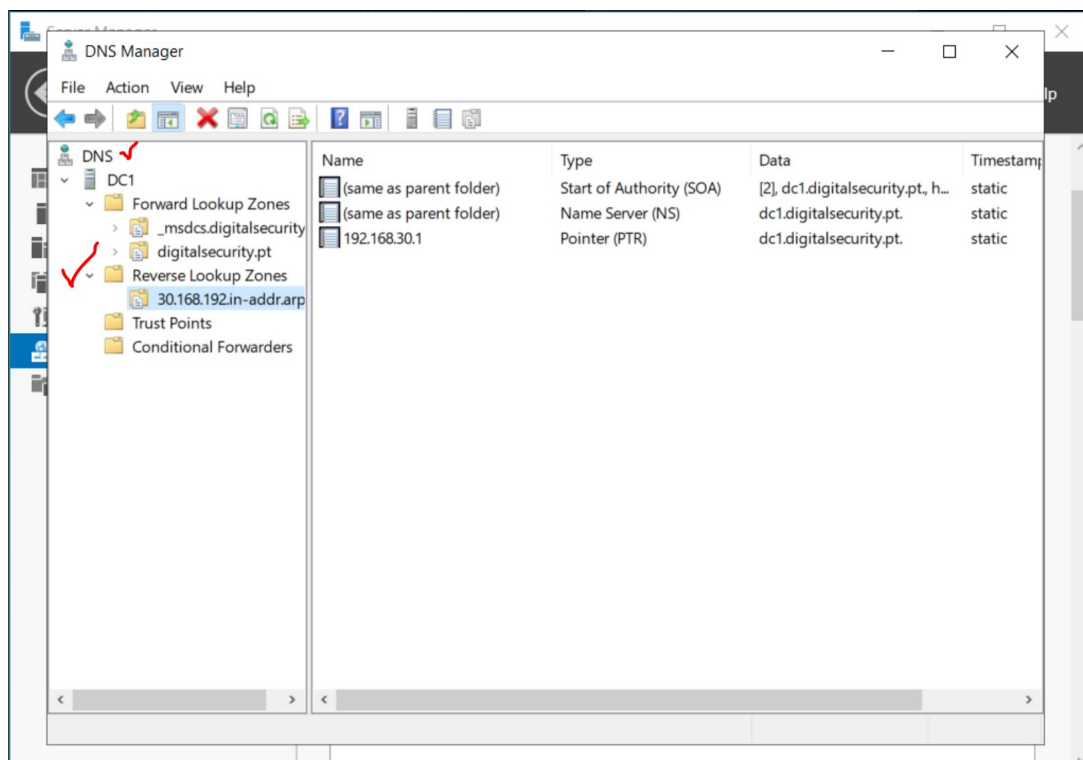
- Instalar a AD DS, DHCP e DNS



- Instalar e configurar o serviço de DHCP (range de IP: 10 – 45)



- Instalar e configurar o serviço de DNS



Pfsense

Ações a desenvolver:

- Instalar a pfsense



```
Windows Server 2022_ufcd_9... x pfSense_ufcd9194 x

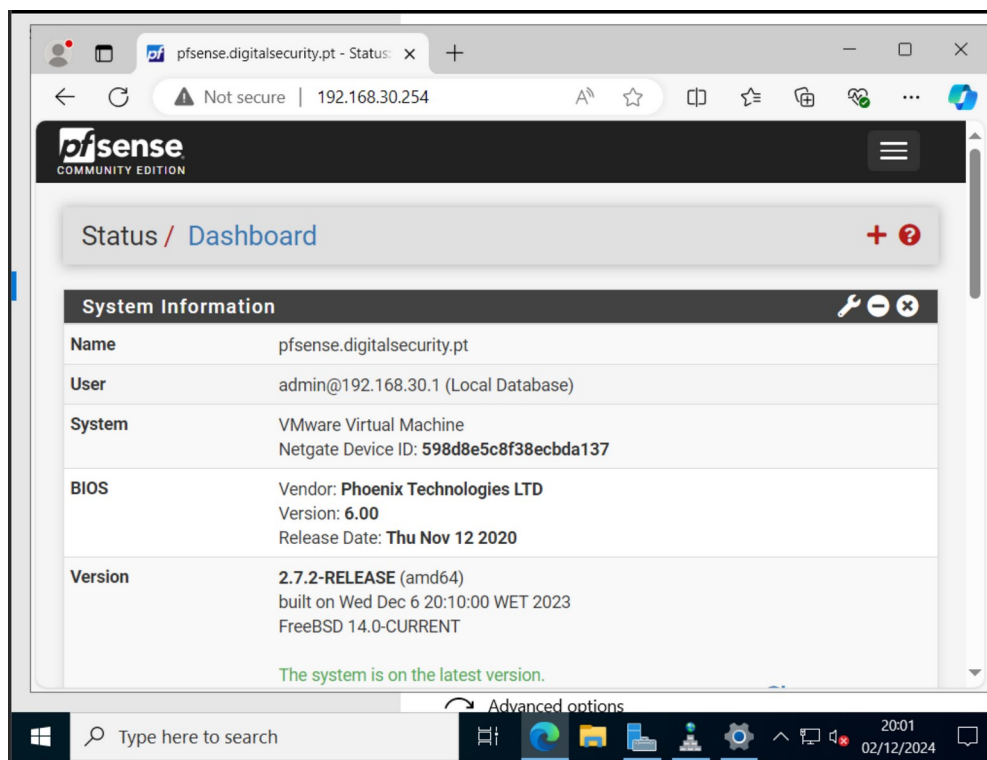
WAN (wan) -> em0 -> v4/DHCP4: 192.168.48.136/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24

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 (ssh)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

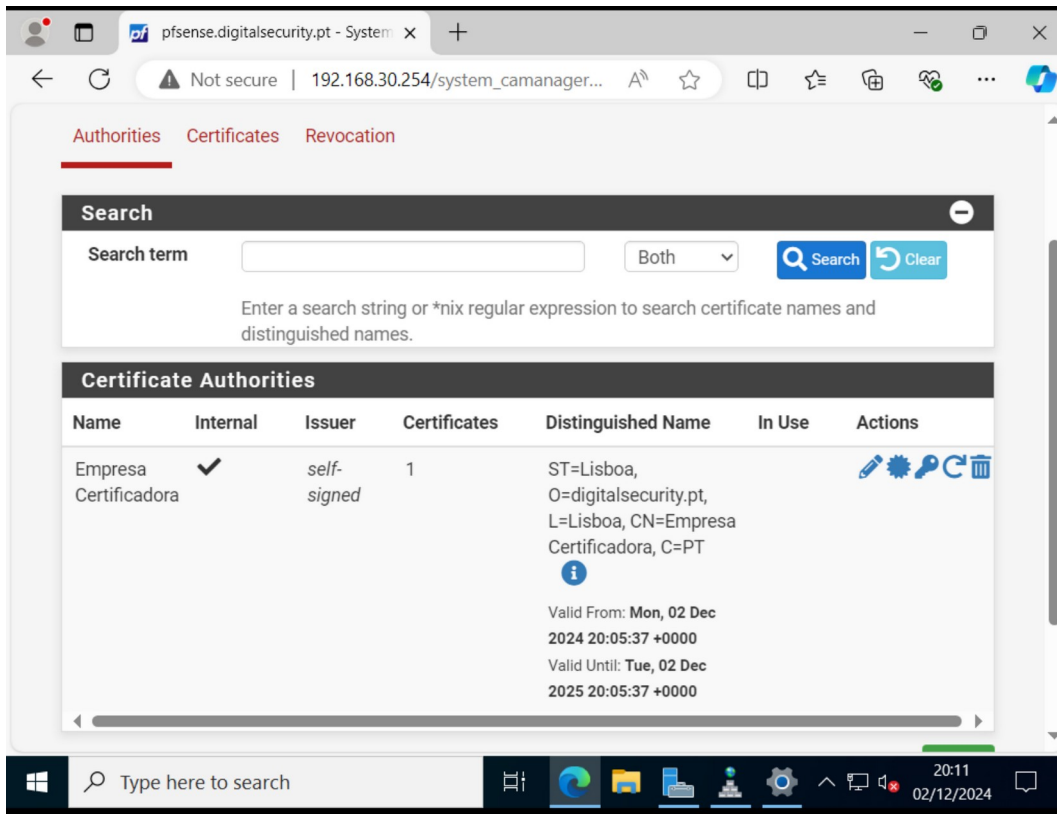
Enter an option: 8

[2.7.2-RELEASE][root@pfsense.home.arpa]: root: ping google.com
PING google.com (172.217.168.174): 56 data bytes
64 bytes from 172.217.168.174: icmp_seq=0 ttl=128 time=38.873 ms
64 bytes from 172.217.168.174: icmp_seq=1 ttl=128 time=39.958 ms
64 bytes from 172.217.168.174: icmp_seq=2 ttl=128 time=22.921 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 22.921/31.248/39.958/6.957 ms
[2.7.2-RELEASE][root@pfsense.home.arpa]: root: █
```

- Mudar o nome da máquina para pfsense (faz-se no setup wizard da pfsense)



- Criar uma CA (Autoridade Certificadora)







Authorities Certificates Revocation

Search

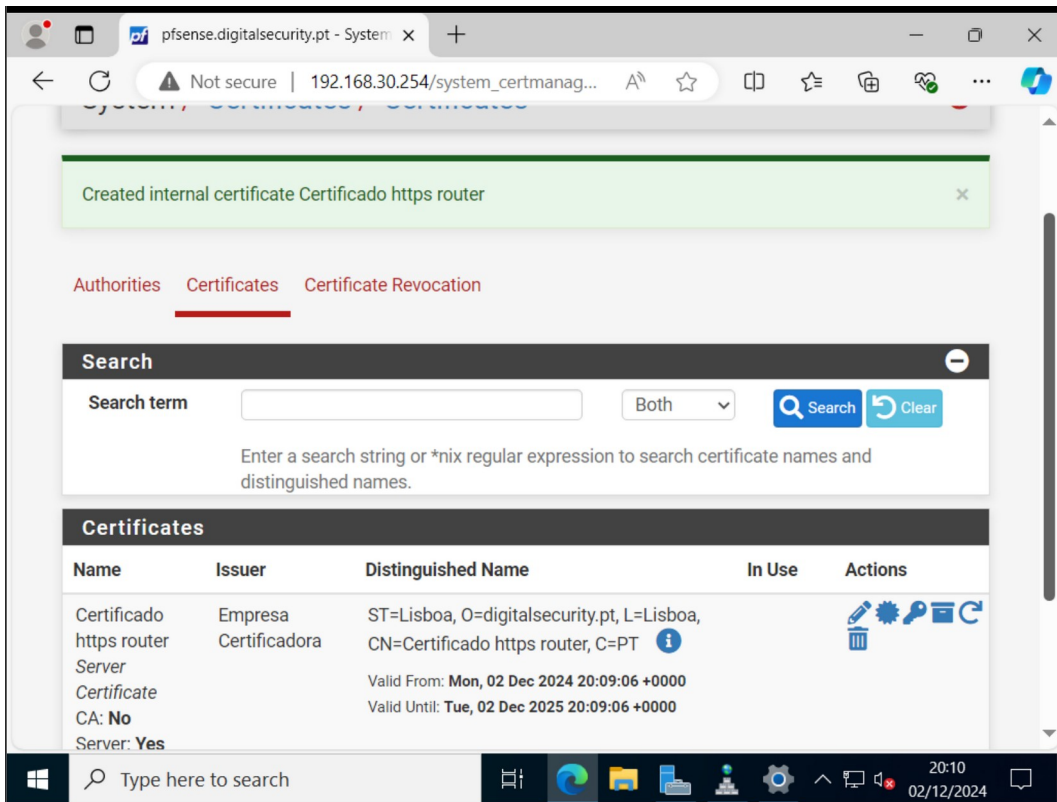
Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Empresa Certificadora	✓	self-signed	1	ST=Lisboa, O=digitalsecurity.pt, L=Lisboa, CN=Empresa Certificadora, C=PT Valid From: Mon, 02 Dec 2024 20:05:37 +0000 Valid Until: Tue, 02 Dec 2025 20:05:37 +0000		   

- Criar um certificado HTTPS para o router







Authorities Certificates Certificate Revocation

Search

Search term Both

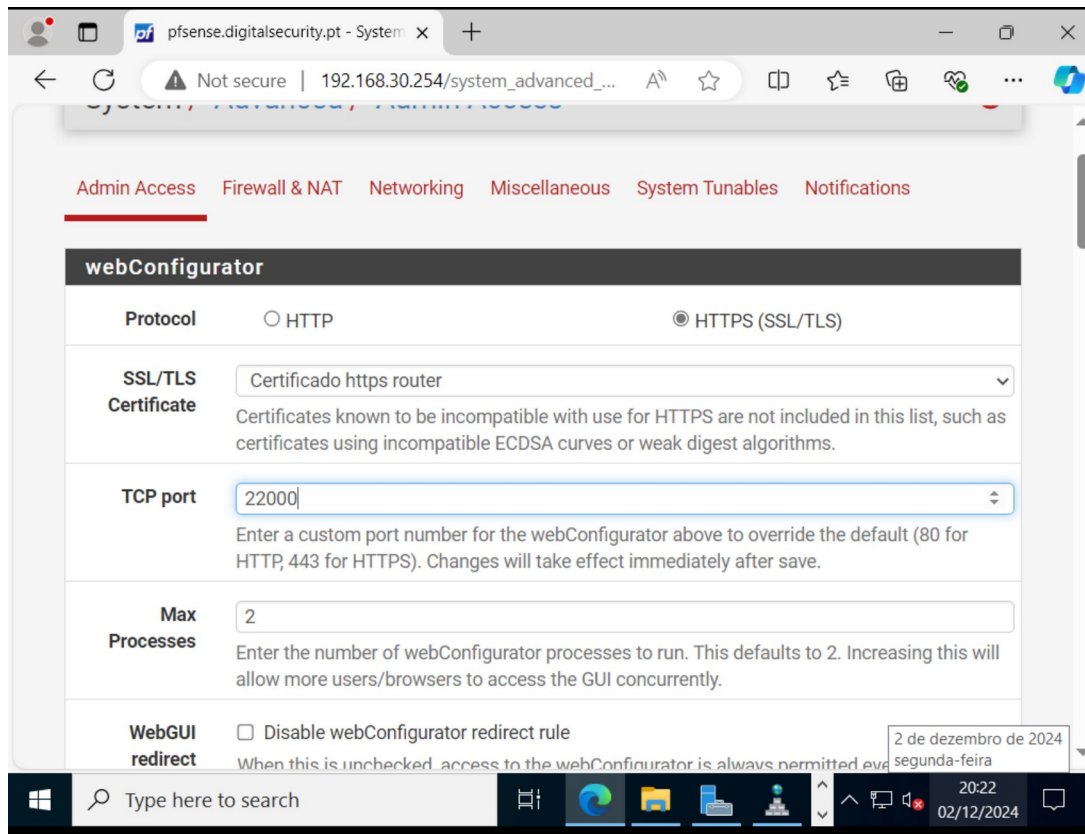
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

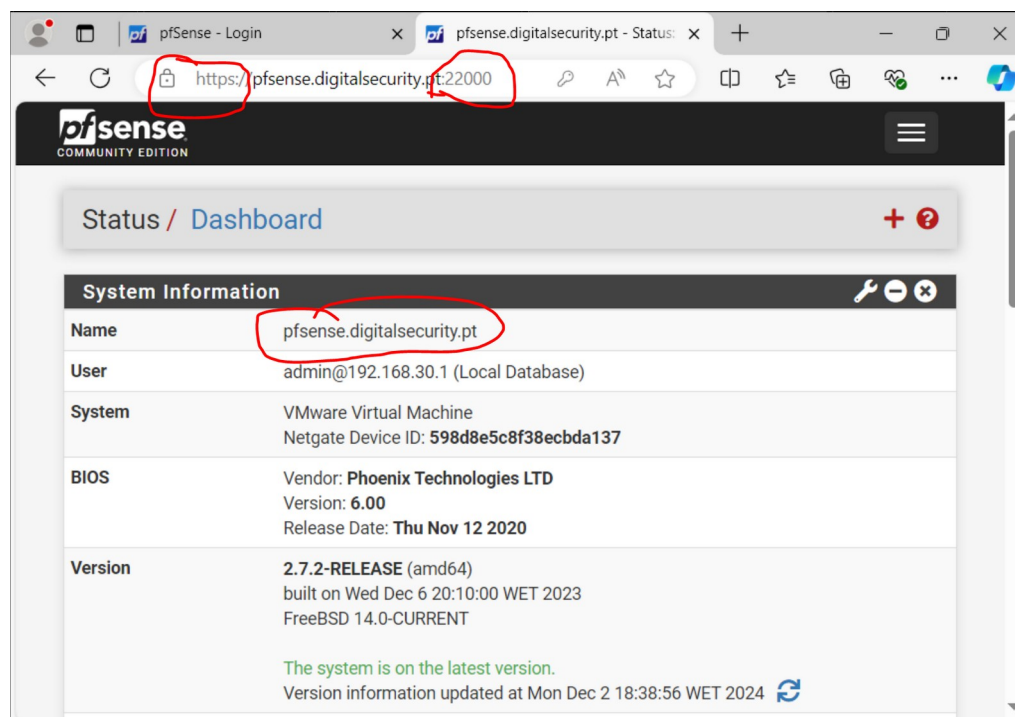
Name	Issuer	Distinguished Name	In Use	Actions
Certificado https router Server Certificate CA: No Server: Yes	Empresa Certificadora	ST=Lisboa, O=digitalsecurity.pt, L=Lisboa, CN=Certificado https router, C=PT Valid From: Mon, 02 Dec 2024 20:09:06 +0000 Valid Until: Tue, 02 Dec 2025 20:09:06 +0000		   

- Mudar o acesso do router para a porta 22000

Este passo é realizado quando mudamos a configuração da pfsense de HTTP para HTTPS.







e



- Instalar e configurar o IDS/IPS Snort

The screenshot displays the pfSense web interface, specifically the 'Services / Snort / Interfaces' configuration page. The browser's address bar shows the URL 'https://pfsense.digitalsecurity.pt:22000/sn...'. The pfSense header includes navigation links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The breadcrumb trail is 'Services / Snort / Interfaces'. Below the breadcrumb, there are tabs for 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. The 'Snort Interfaces' tab is active, showing the 'Interface Settings Overview' table.

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)	 	AC-BNFA	LEGACY MODE	Internet	 

Below the table, there are '+ Add' and 'Delete' buttons. At the bottom of the interface, a footer states 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.' The Windows taskbar at the bottom shows the search bar, taskbar icons, and the system clock displaying 22:04 on 02/12/2024.

Kali Linux

Ações a desenvolver:

- Colocar o Kali em LAN para testar o DHCP (fazer o comando ip a e verificar se tem IP)

```
root@kali: /home/morim
File Actions Edit View Help
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2c:03:65 brd ff:ff:ff:ff:ff:ff
    inet 192.168.48.132/24 brd 192.168.48.255 scope global dynamic noprefixroute eth0
        valid_lft 934sec preferred_lft 934sec
    inet6 fe80::20c:29ff:fe2c:365/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(root@kali)-[/home/morim]
# ping 192.168.30.254
PING 192.168.30.254 (192.168.30.254) 56(84) bytes of data.
^C
  192.168.30.254 ping statistics —
  21 packets transmitted, 0 received, 100% packet loss, time 20483ms

(root@kali)-[/home/morim]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2c:03:65 brd ff:ff:ff:ff:ff:ff
    inet 192.168.30.10/24 brd 192.168.30.255 scope global dynamic noprefixroute eth0
        valid_lft 863994sec preferred_lft 863994sec
    inet6 fe80::20c:29ff:fe2c:365/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(root@kali)-[/home/morim]
```

NAT

LAN DHCP configurado.

- Colocar o Kali em LAN para testar o DNS (fazer um ping e um nslookup ao domínio)

```
root@kali: /home/morim
File Actions Edit View Help
Name: dc1.digitalsecurity.pt
Address: 192.168.30.1

(root@kali)-[/home/morim]
# ping dc1
PING dc1.digitalsecurity.pt (192.168.30.1) 56(84) bytes of data.
64 bytes from 192.168.30.1: icmp_seq=1 ttl=128 time=0.284 ms
64 bytes from 192.168.30.1: icmp_seq=2 ttl=128 time=1.31 ms
64 bytes from 192.168.30.1: icmp_seq=3 ttl=128 time=0.935 ms
^C
  dc1.digitalsecurity.pt ping statistics —
  3 packets transmitted, 3 received, 0% packet loss, time 2004ms
  rtt min/avg/max/mdev = 0.284/0.842/1.307/0.422 ms

(root@kali)-[/home/morim]
# nslookup digitalsecurity.pt
Server:      192.168.30.1
Address:     192.168.30.1#53

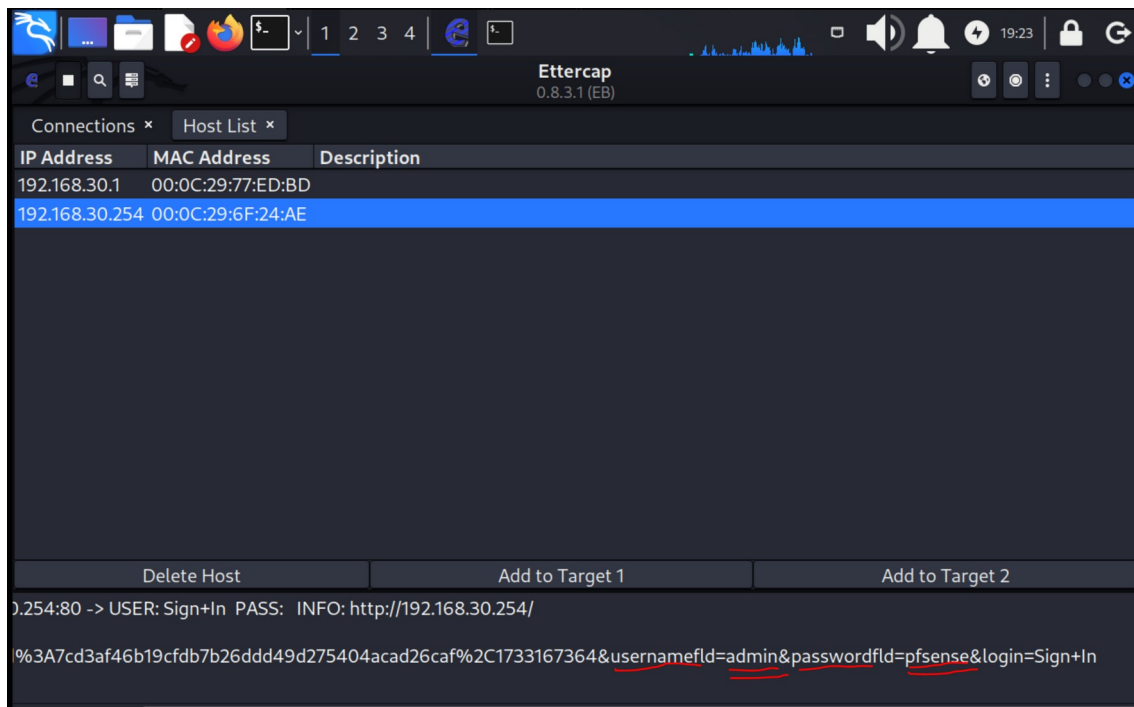
Name:   digitalsecurity.pt
Address: 192.168.30.1

(root@kali)-[/home/morim]
# ping digitalsecurity.pt
PING digitalsecurity.pt (192.168.30.1) 56(84) bytes of data.
64 bytes from dc1.digitalsecurity.pt (192.168.30.1): icmp_seq=1 ttl=128 time=0.323 ms
64 bytes from dc1.digitalsecurity.pt (192.168.30.1): icmp_seq=2 ttl=128 time=0.728 ms
64 bytes from dc1.digitalsecurity.pt (192.168.30.1): icmp_seq=3 ttl=128 time=0.962 ms
^X^C
  digitalsecurity.pt ping statistics —
  3 packets transmitted, 3 received, 0% packet loss, time 2032ms
  rtt min/avg/max/mdev = 0.323/0.671/0.962/0.263 ms

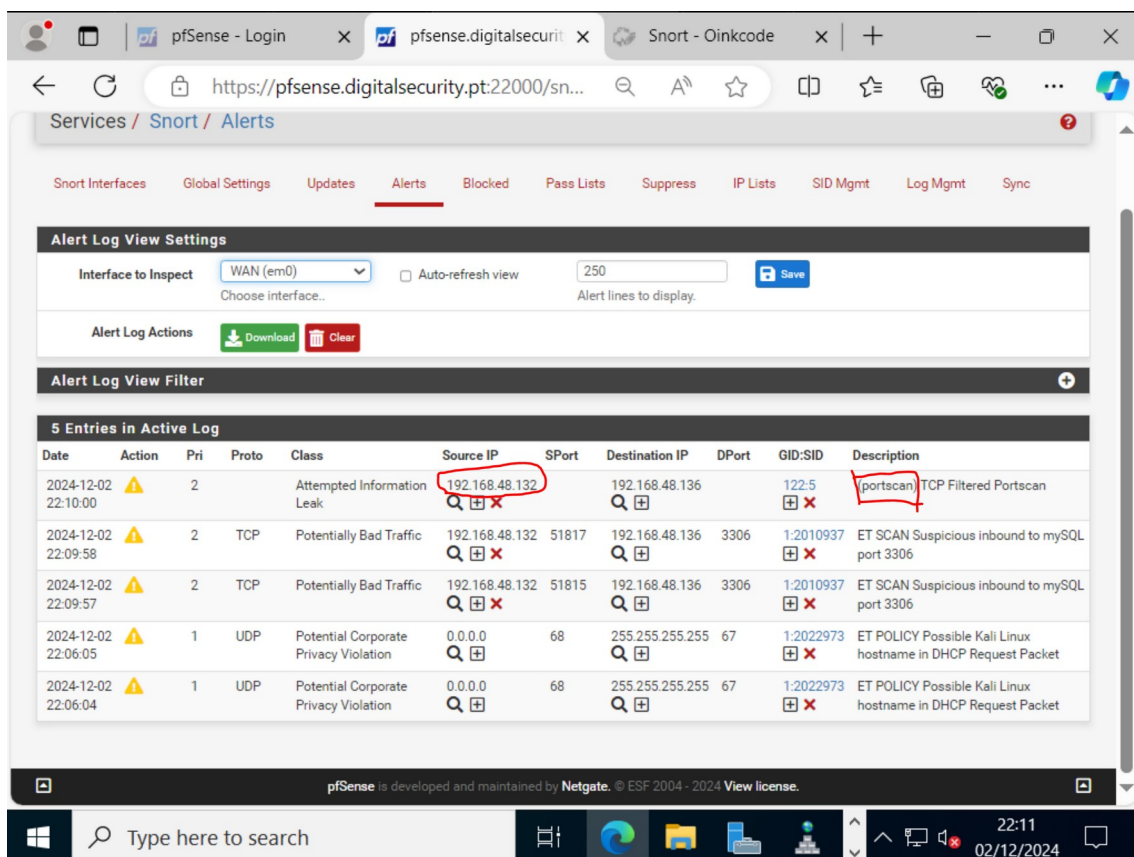
(root@kali)-[/home/morim]
```

DNS configurado.

- Colocar o Kali em LAN e fazer um ataque de MITM usando a aplicação ettercap



- Colocar o Kali em NAT e fazer um scan ao IP da WAN da pfSense e verificar se fica bloqueado no IDS/IPS



2. Cotações:

<i>Tarefa</i>	<i>Valorização</i>
Instalar o Windows Server	1 valor
Colocar IP estático no Windows Server	1 valor
Mudar o nome da máquina para DC1	1 valor
Mudar o timezone	1 valor
Instalar a AD DS, DHCP e DNS	1 valor
Instalar e configurar o serviço de DHCP	1 valor
Instalar e configurar o serviço de DNS	1 valor
Instalar a pfsense	1 valor
Mudar o nome da máquina para pfsense	1 valor
Criar uma CA (Autoridade Certificadora)	2 valores
Criar um certificado HTTPS para o router	3 valores
Mudar o acesso do router para a porta 22000	1 valor
Instalar e configurar o IDS/IPS	1 valor
Kali em LAN para testar o DHCP	1 valor
Kali em LAN para testar o DNS	1 valor
Kali em LAN e fazer um ataque de MITM	1 valor
Kali em NAT e fazer um scan ao IP da WAN	1 valor
Total	20,00 Valores

Data de entrega: 07 de Dezembro de 2024.

Bom trabalho 😊

Obrigado pela dedicação em sala e pelas elucidações sempre muito completas!
Aprendemos muito.