

Projeto

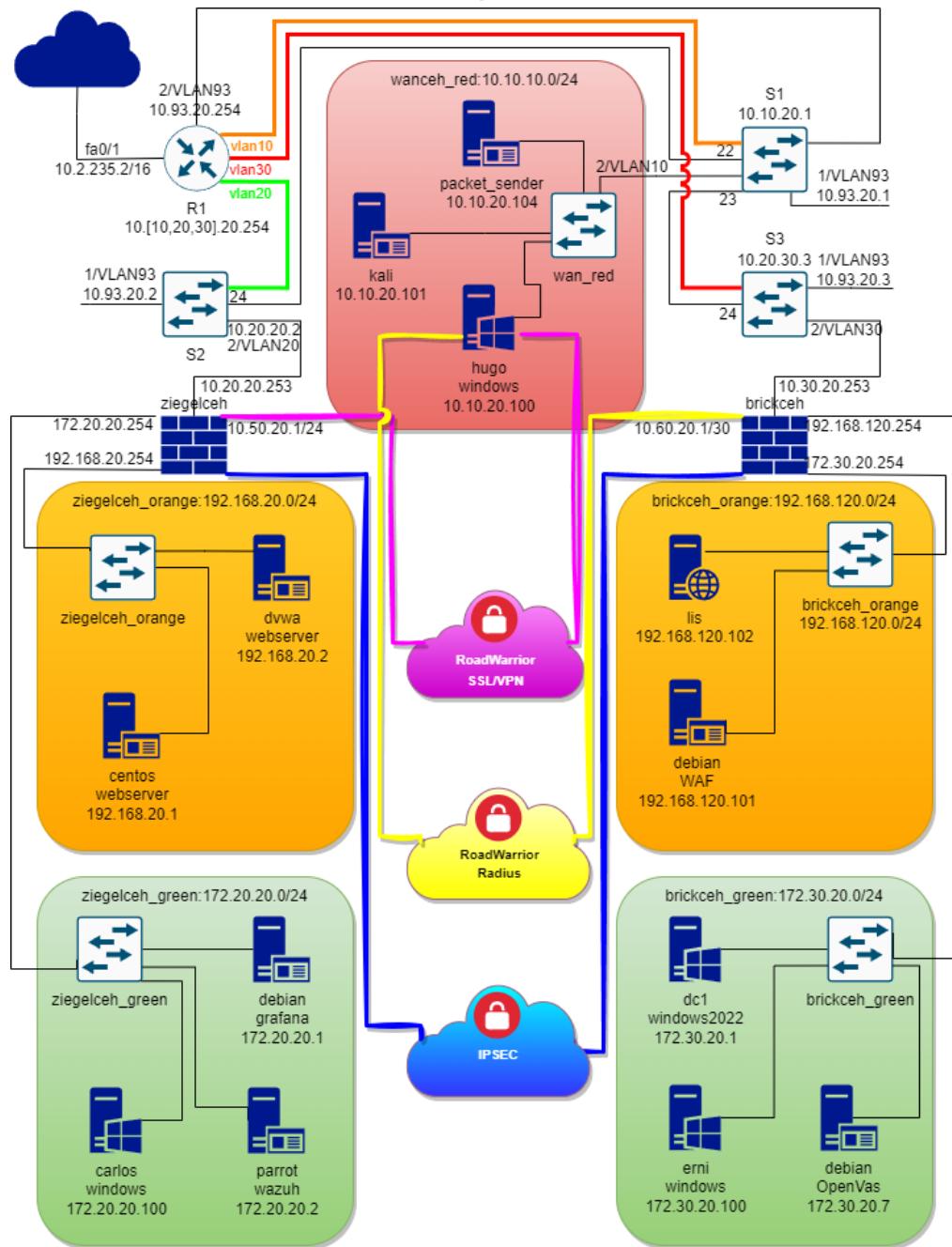


Imagen 1

Carlos Oliveira, Erni Souza, Hugo Oliveira
 9197 – Wargaming

Índice

Introdução	4
wanceh_red.....	5
Configuração Router	5
Configuração Switch	7
Switch 1.....	7
Switch 2.....	9
Switch 3.....	11
NXLog CE em máquina Windows.....	13
brickceh.....	15
Windows Server DC.....	15
DNS	15
DHCP	15
ADDS.....	19
Ubuntu Linux (WAF).....	22
Windows Server DC1 RADIUS VPN	29
Configuração VPN RoadWarrior RADIUS	32
Windows Server CORE	35
Debian Server	43
OpenVAS	43
PfSense briceh	48
Snort	48
ZenMap brickceh	52
ziegelceh.....	53
cockpit	53
Grafana, Wazuh	53
VPN IPSec	54
OpenVPN RoadWarrior.....	57
Configuração VPN SSL RoadWarrior cliente	59
Wazuh Server.....	62
Wazuh Agent.....	65
Syslog-ng Server	66
Syslog-ng Local Log.....	68
Syslog-ng Client	69

Técnico Especialista Cibersegurança - CET93

Syslog-ng a partir da OpnSense.....	70
Syslog-ng do Apache2	71
Syslog-ng do wazuh.....	72
Syslog-ng, testes.....	73
Syslog-ng no Cisco	74
Syslog-ng, no Windows (NXLog)	75
Syslog-ng da firewall.....	77
Promtail, Configuração.....	78
Grafana	79
Polystat to monitor ping	82
Install Telegraf	84
Packet Sender.....	88
CentOS	89
Suricata.....	91
DVWA Server	92
Static IP	92
SSH.....	92
Instalação do DVWA.....	93
ZenMap	95
Conclusão.....	96
Agradecimentos	97
Referências	98
Instalação do Cockpit	98
Installing the Wazuh server step by step	98
Wazuh installation assistant	98
Netplan config usando static IP	98
Ubuntu UFW	98
SQL Server Firewall Windows Server	98
Debia OpenVas GreenBone	98
Configurações Router e Switch	98
OpenVPN cliente.....	99

Introdução

O presente relatório descreve o trabalho desenvolvido no âmbito do Projeto Final do curso Técnico/a Especialista em Cibersegurança (CET93), promovido pelo CINEL - Centro de Formação Profissional da Indústria Electrónica, Energia, Telecomunicações e Tecnologias da Informação, Polo de Lisboa. Este projeto, realizado em março de 2025, foi proposto pelo formador Fernando Ruela e tem como objetivo principal a configuração e validação de uma estrutura de rede em máquinas virtuais, conforme o diagrama lógico apresentado na Figura 1 do enunciado.

Nós, Carlos, Erni e Hugo, enquanto grupo de formandos, propomo-nos a implementar e configurar uma infraestrutura de rede segura e funcional, que integre equipamentos físicos, como um router Cisco e switches, com sistemas virtualizados distribuídos em diferentes zonas de segurança. Este trabalho abrange a configuração de firewalls (PFsense e Opnsense), a criação de VPNs, a implementação de sistemas de deteção de intrusões (IDS) como Snort e Suricata, e a integração de ferramentas de monitorização e análise de segurança, como Wazuh, OpenVAS e Syslog-ng. Além disso, comprometemos-nos a desenvolver um relatório detalhado que documente todas as configurações realizadas, incluindo tabelas de IPs, redes e MACs utilizados, de forma a permitir a replicação dos resultados por outros formandos da turma.

Com este projeto, pretendemos não só cumprir os requisitos técnicos estabelecidos, mas também propor sugestões que potenciem a segurança, fiabilidade e usabilidade das soluções implementadas, contribuindo para uma avaliação prática e teórica sólida das competências adquiridas ao longo da formação.

wanceh_red

Configuração Router

Os seguintes comandos foram executados no Router:

- Alteração do hostname e adição do domínio “guardianprobe.local”

```
hostname R1
ip domain-name guardianprobe.local
```

- Configuração da interface para acesso à internet

```
int fa0/0
ip address 10.2.235.2 255.255.0.0
```

- Encapsulamento para roteamento entre VLANs (10, 20, 30 e 93)

```
interface FastEthernet0/1.10
encapsulation dot1Q 10
ip address 10.10.20.254 255.255.255.0
```

```
interface FastEthernet0/1.20
encapsulation dot1Q 20
ip address 10.20.20.254 255.255.255.0
```

```
interface FastEthernet0/1.30
encapsulation dot1Q 30
ip address 10.30.20.254 255.255.255.0
```

```
interface FastEthernet0/1.93
encapsulation dot1Q 93 native
ip address 10.93.20.254 255.255.255.0
```

- Criação de rotas estáticas

```
ip route 0.0.0.0 0.0.0.0 10.5.255.254
ip route 0.0.0.0 0.0.0.0 10.2.255.254
ip route 172.20.20.0 255.255.255.0 10.20.20.253
ip route 172.30.20.0 255.255.255.0 10.20.30.253
ip route 192.168.20.0 255.255.255.0 10.20.20.253
ip route 192.168.120.0 255.255.255.0 10.20.30.253
```

Técnico Especialista Cibersegurança - CET93

- Criação de ACL extendida para a VLAN 93 (gestão)

```
ip access-list extended DEBUG_ACL
permit ip 10.93.20.0 0.0.0.255 any
```

```
ip access-list extended DEBUG_ICMP_ACL
permit icmp 10.93.20.0 0.0.0.255 any
```

- Criação de ACL standard para as VLANs (10, 20, 30 e 93)

```
access-list 1 permit 10.93.20.0 0.0.0.255
access-list 1 permit 10.20.20.0 0.0.0.255
access-list 1 permit 10.10.20.0 0.0.0.255
access-list 1 permit 10.30.20.0 0.0.0.255
```

- Aplicar password no acesso consola e configuração

```
enable secret Passw0rd
line console 0
password Passw0rd
```

- Criação de banner informativo

```
Banner motd #
*****
ADMIN ACCESS ONLY
*****#
```

Configuração Switch

Switch 1

- Alteração do hostname, adição do domínio e aplicar password no modo acesso e configuração

```
hostname s1
ip domain-name guardianprobe.local
enable secret Passw0rd
line console 0
password Passw0rd
```

- Configuração do SSH

```
crypto key generate rsa
2048
ssh username formando privilege 15 password Passw0rd
line vty 0 4
login local
transport input ssh
```

- Criação das VLANs (10, 20, 30, 93)

```
vlan 10
name red
vlan 20
name zielger
vlan 30
name brick
vlan 93
name gestão
```

- Atribuição de IP nas VLANs e default gateway

```
interface Vlan10
ip address 10.10.20.1 255.255.255.0

interface Vlan20
ip address 10.20.20.1 255.255.255.0

interface Vlan30
ip address 10.30.20.1 255.255.255.0

interface Vlan93
ip address 10.93.20.1 255.255.255.0

ip default-gateway 10.93.20.254
```

Técnico Especialista Cibersegurança - CET93

- Port-Security e atribuição de VLAN nas respetivas interfaces a ser usadas

```
int range fa0/1-24, g0/1-2
shutdown
int range fa0/1-3
switchport port-security
switchport port-security mac-address sticky
switchport port-security shutdown
interface range fa0/23-24
switchport mode trunk
switchport trunk native vlan 93
switchport trunk allowed vlan 10,20,30,93
no shut
interface fa0/1
switchport mode access
switchport access vlan 93
no shut
interface range fa0/2-3
switchport mode access
switchport access vlan 10
no shut
```

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Gig0/1, Gig0/2
10 red	active	Fa0/2, Fa0/3
20 siegel	active	
30 brick	active	
93 gestao	active	Fa0/1
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Imagen 2

Port	Mode	Encapsulation	Status	Native vlan
Fa0/22	on	802.1q	trunking	1
Fa0/23	on	802.1q	trunking	1
Fa0/24	on	802.1q	trunking	93

Port Vlans allowed on trunk

Fa0/22 1-1005
 Fa0/23 1-1005
 Fa0/24 1-1005

Port Vlans allowed and active in management domain

Fa0/22 1,10,20,30,93
 Fa0/23 1,10,20,30,93
 Fa0/24 1,10,20,30,93

Imagen 3

Técnico Especialista Cibersegurança - CET93

- Criação de banner informativo

```
banner motd #
*****
ADMIN ACCESS ONLY
*****#
```

Switch 2

- Alteração do hostname, adição do domínio e aplicar password no modo acesso e configuração

```
hostname s2
ip domain-name guardianprobe.local
enable secret Passw0rd
lime console 0
password Passw0rd
```

- Configuração do SSH

```
crypto key generte rsa
2048
ssh username formando privilege 15 password Passw0rd
line vty 0 4
login local
transport input ssh
```

- Criação das VLANs (10, 20, 30, 93)

```
vlan 10
name red
vlan 20
name zielger
vlan 30
name brick
vlan 93
name gestão
```

- Atribuição de IP nas VLANs e default gateway

```
interface Vlan10
ip address 10.10.20.1 255.255.255.0

interface Vlan20
ip address 10.20.20.1 255.255.255.0

interface Vlan30
ip address 10.30.20.1 255.255.255.0

interface Vlan93
ip address 10.93.20.1 255.255.255.0

ip default-gateway 10.93.20.254
```

Técnico Especialista Cibersegurança - CET93

- Port-Security e atribuição de VLAN nas respetivas interfaces a ser usadas

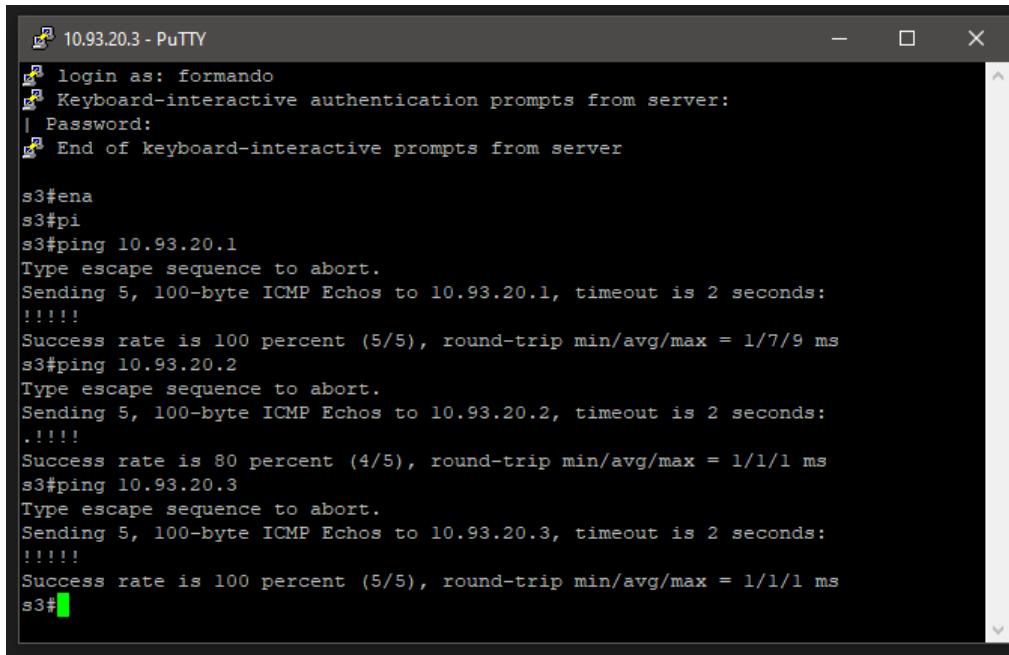
```
int range fa0/1-24, g0/1-2
shutdown
int range fa0/1-3
switchport port-security
switchport port-security mac-address sticky
switchport port-security shutdown

interface fa0/23
switchport mode trunk
switchport trunk native vlan 93
switchport trunk allowed vlan 10,20,30,93
no shut
interface fa0/1
switchport mode access
switchport access vlan 93
no shut
interface range fa0/2-3
switchport mode access
switchport access vlan 20
no shut
```

- Criação de banner informativo

```
banner motd #
*****
ADMIN ACCESS ONLY
*****#
```

Switch 3



```
10.93.20.3 - PuTTY
login as: formando
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

s3#ena
s3#pi
s3#ping 10.93.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.93.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/9 ms
s3#ping 10.93.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.93.20.2, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
s3#ping 10.93.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.93.20.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
s3#
```

Imagen 4

- Alteração do hostname, adição do domínio e aplicar password no modo acesso e configuração

```
hostname s3
ip domain-name guardianprobe.local
enable secret Passw0rd
lime console 0
password Passw0rd
```

- Configuração do SSH

```
crypto key generte rsa
2048
ssh username formando privilege 15 password Passw0rd
line vty 0 4
login local
transport input ssh
```

- Criação das VLANs (10, 20, 30, 93)

```
vlan 10
name red
vlan 20
name zielger
vlan 30
name brick
vlan 93
name gestão
```

Técnico Especialista Cibersegurança - CET93

- Atribuição de IP nas VLANs e default gateway

```
interface Vlan10
ip address 10.10.20.1 255.255.255.0

interface Vlan20
ip address 10.20.20.1 255.255.255.0

interface Vlan30
ip address 10.30.20.1 255.255.255.0

interface Vlan93
ip address 10.93.20.1 255.255.255.0

ip default-gateway 10.93.20.254
```

- Port-Security e atribuição de VLAN nas respetivas interfaces a ser usadas

```
int range fa0/1-24, g0/1-2
shutdown
int range fa0/1-3
switchport port-security
switchport port-security mac-address sticky
switchport port-security shutdown

interface fa0/24
switchport mode trunk
switchport trunk native vlan 93
switchport trunk allowed vlan 10,20,30,93
no shut
interface fa0/1
switchport mode access
switchport access vlan 93
no shut
interface range fa0/2-3
switchport mode access
switchport access vlan 30
no shut
```

- Criação de banner informativo:

```
banner motd #
*****
ADMIN ACCESS ONLY
*****#
```

Técnico Especialista Cibersegurança - CET93

NXLog CE em máquina Windows

Download do nxlog CE (Community Edition) na máquina Windows cliente

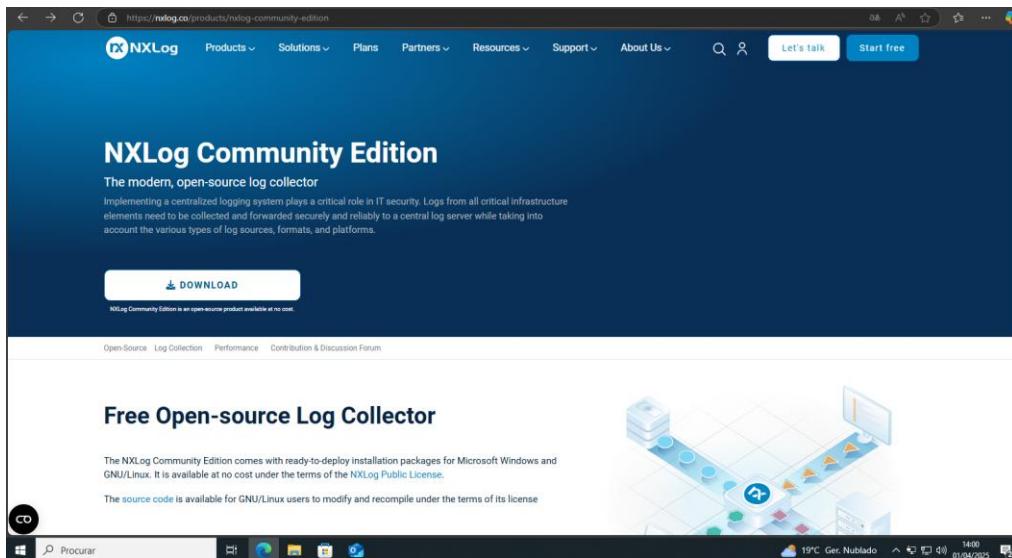


Imagen 5

Fazer a instalação

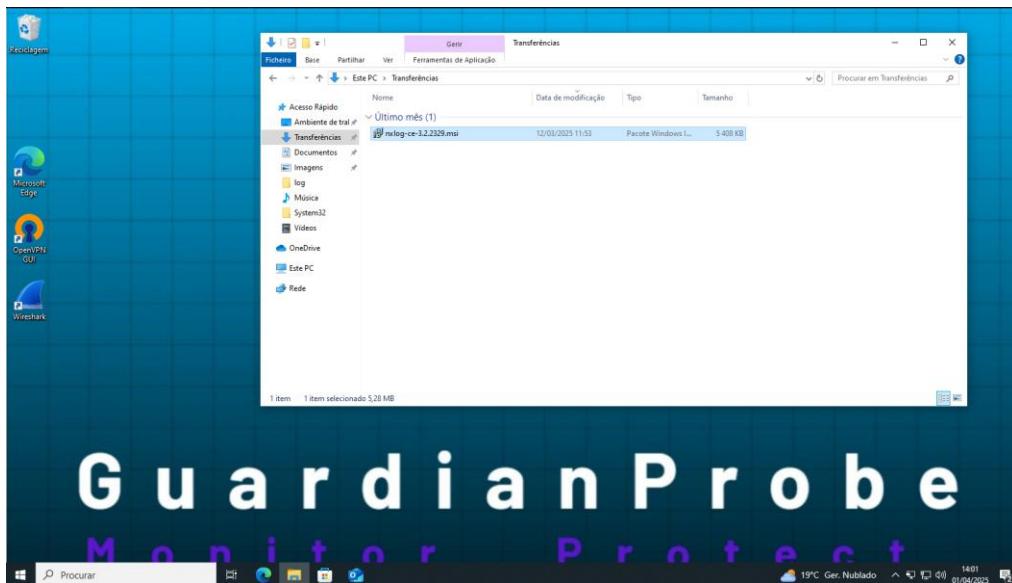


Imagen 6

Depois da instalação, não irá apresentar nenhuma interface gráfica, pelo que teremos de ir à seguinte localização para configurar o envio dos logs, abrindo o ficheiro 'nxlog.conf':

C:\Program Files\nxlog\conf

Técnico Especialista Cibersegurança - CET93

No ficheiro colocar o seguinte código:

```
# Input: Collect Windows Event Log
<Input eventlog>
    Module im_msvistalog
</Input>

# Output: Forward to syslog-ng server (UDP)
<Output syslog_out>
    Module om_udp
    Host 172.20.20.1
    Port 514
    Exec \
        # Map Windows Event Log fields to syslog format \
        $Message = "EventID=" + $EventID + " " + $Message; \
        $Hostname = hostname(); \
        $Severity = "INFO"; # Adjust based on $Level if needed \
        to_syslog_bsd();
</Output>

# Define the log routing
<Route eventlog_to_syslog>
    Path eventlog => syslog_out
</Route>
```

O resultado será o envio dos logs do Windows para a máquina do grafana.

Técnico Especialista Cibersegurança - CET93

brickceh

Windows Server DC

DNS

Install:

Server Manager: Manage > Add Roles and Features > Next > Next > Next >
Seleciona DNS Server > Add Features > Next > Next > Next > Install

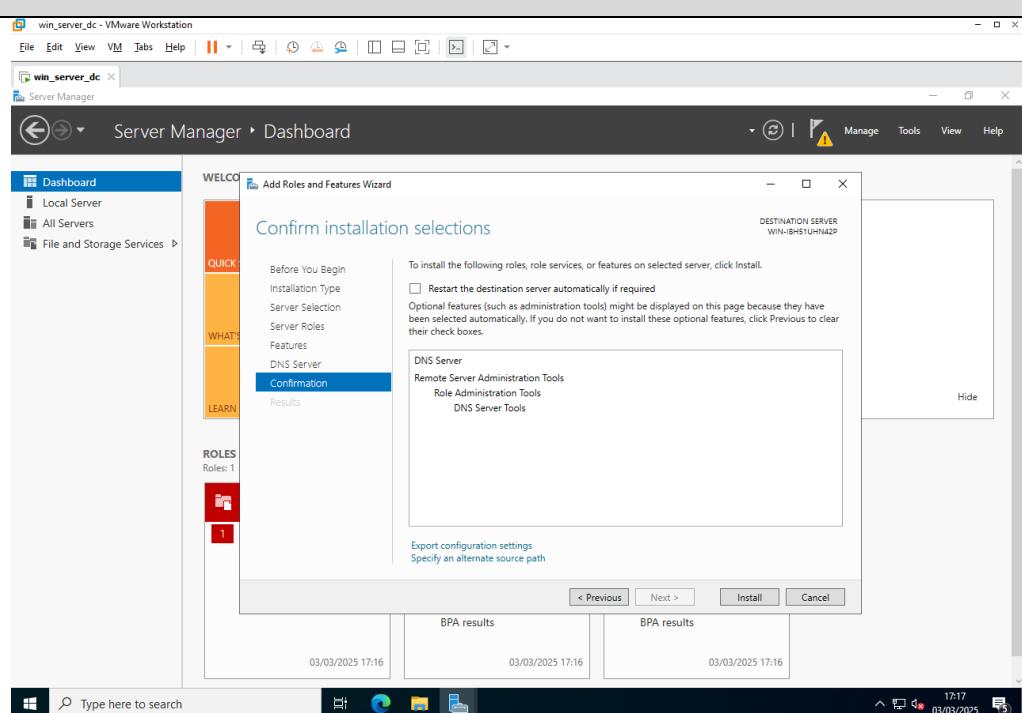


Imagen 16

DHCP

Install:

Server Manager: Manage > Add Roles and Features > Next > Next > Next >
Seleciona DHCP Server > Add Features > Next > Next > Next > Install

Técnico Especialista Cibersegurança - CET93

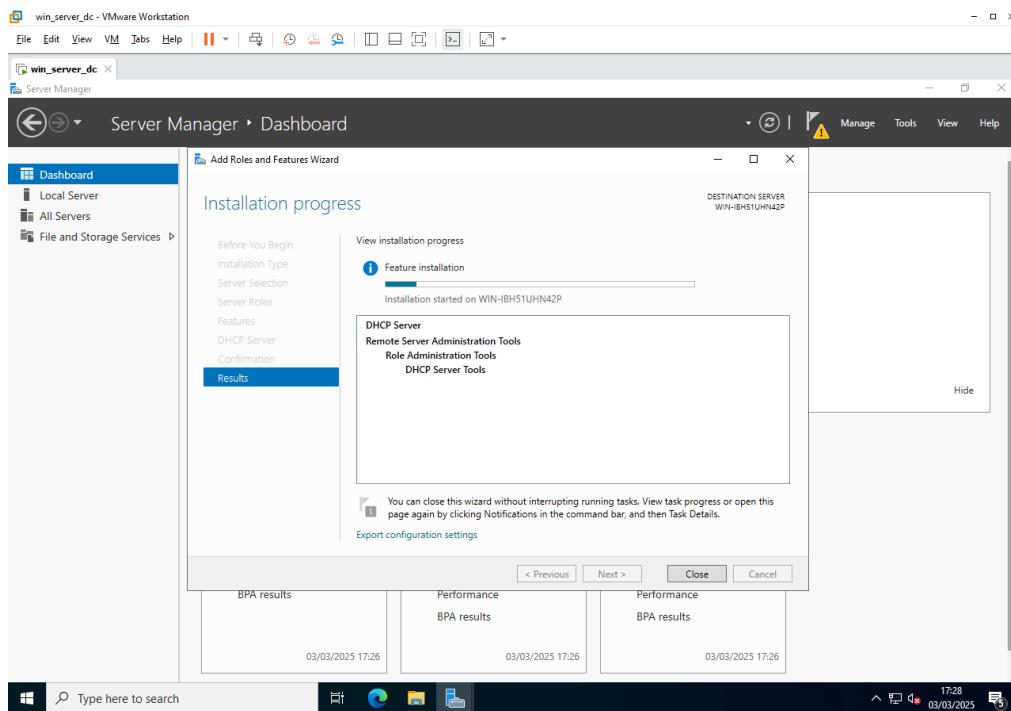


Imagen 17

Config:

Server Manager: Tools > DHCP > Selecione com o botão direito do mouse em IPv4 > New Scope...

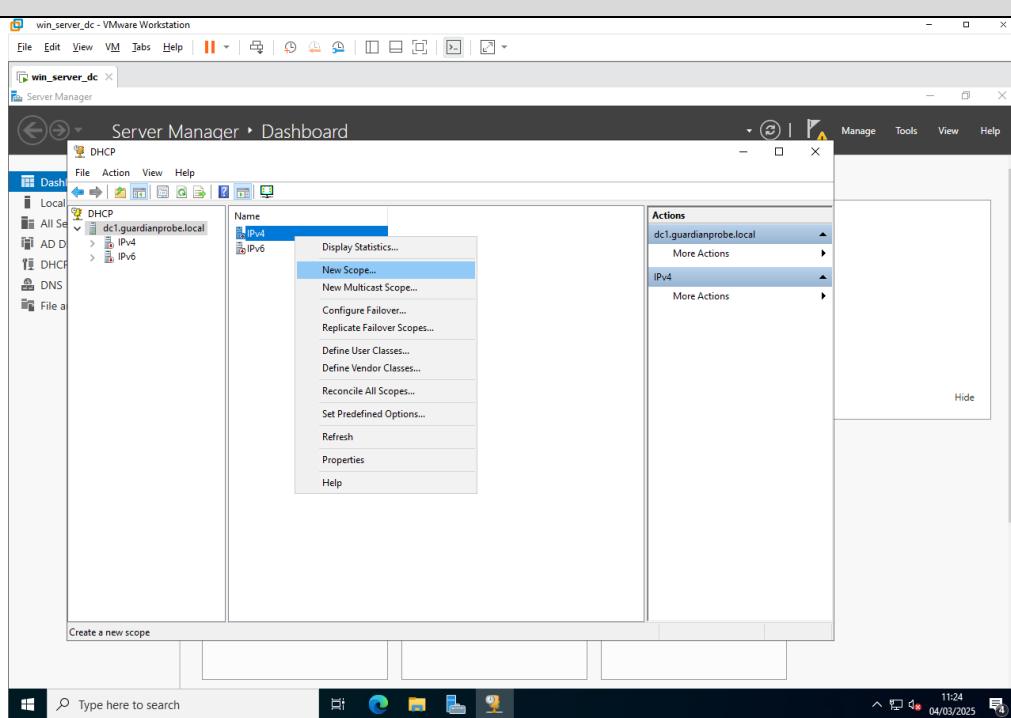


Imagen 18

Técnico Especialista Cibersegurança - CET93

Next > Especificar Name e Description > Next > Especificar Start IP, End IP addresses, Length e Subnet mask > Next > Especificar IPs para Exclusions and Delay se necessário > Next > Especificar Lease Duration se necessário > Next > Selecionar se pretende Do you want to configure the DHCP options for this scope now? > Next > Se for necessário configurar o DHCP options para o scope, especificar o Router Default Gateway > Next > Especificar Domain Name and DNS Servers > Next > Especificar WINS Servers > Next > Selecionar se pretende Activate Scope now > Next > Finish

- Authorize o server dhcp.
- Restart service.

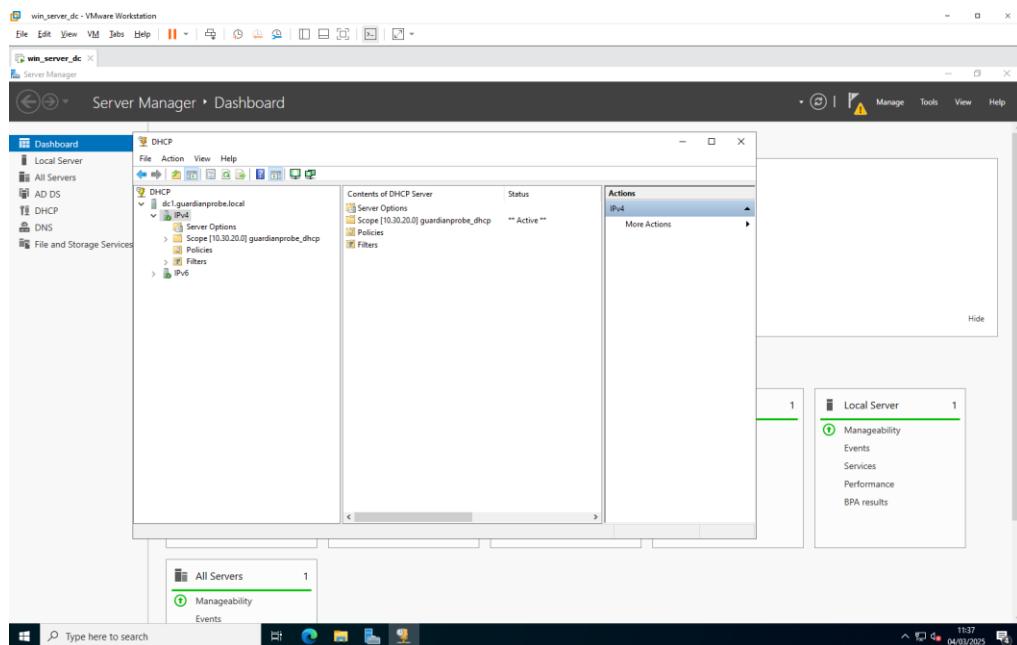


Imagen 19

Criar Reverse Lookup Zone Name.
Selezione New Zone com o botão direto do mouse em cima do Reverse Lookup Zones > Next > Next > Next > Next > Especificar o Reverse lookup zone name > Next > Next > Finish

Técnico Especialista Cibersegurança - CET93

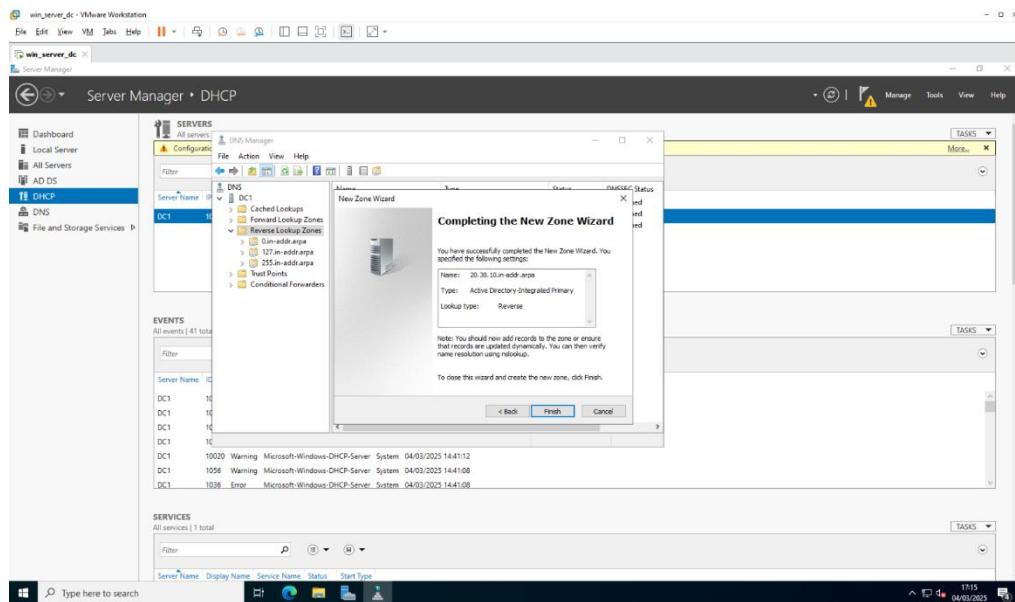


Imagen 20

Técnico Especialista Cibersegurança - CET93

ADDS

Install:

Server Manager: Manage > Add Roles and Features > Next > Next > Next >
Selecione Active Directory Domain Services > Add Features > Next > Next > Next
> Install

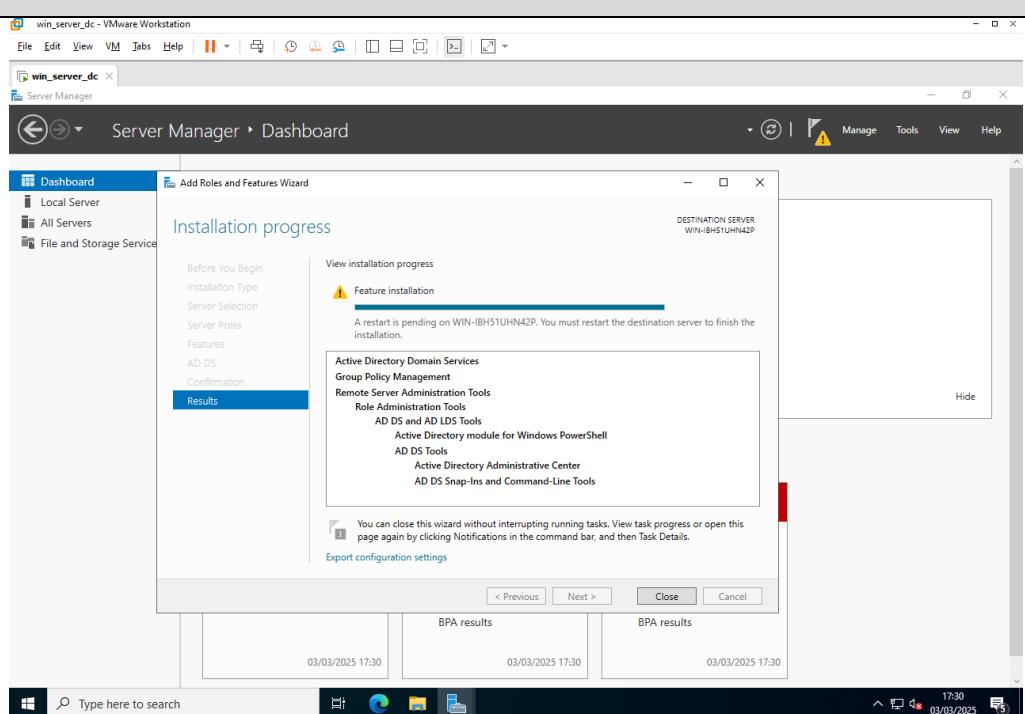


Imagen 21

Config:

Server Manager > AD DS > Selecione More... na mensagem de alerta para promover o server ao domain > Selecione Promote this server to a domain controller.

Técnico Especialista Cibersegurança - CET93

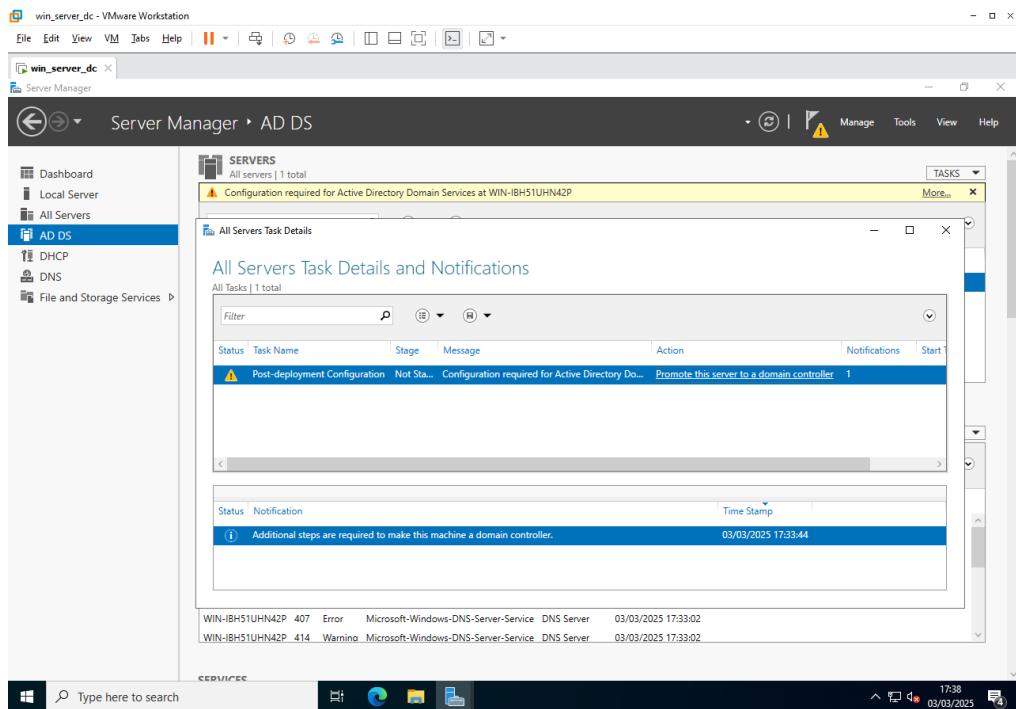


Imagen 22

Add a new forest > Especifique o Root domain name > Next > Digite Password e Confirm Password para o Type the Directory Services Restore Mode (DSRM) password > Next > Next > Next > Next > Install.

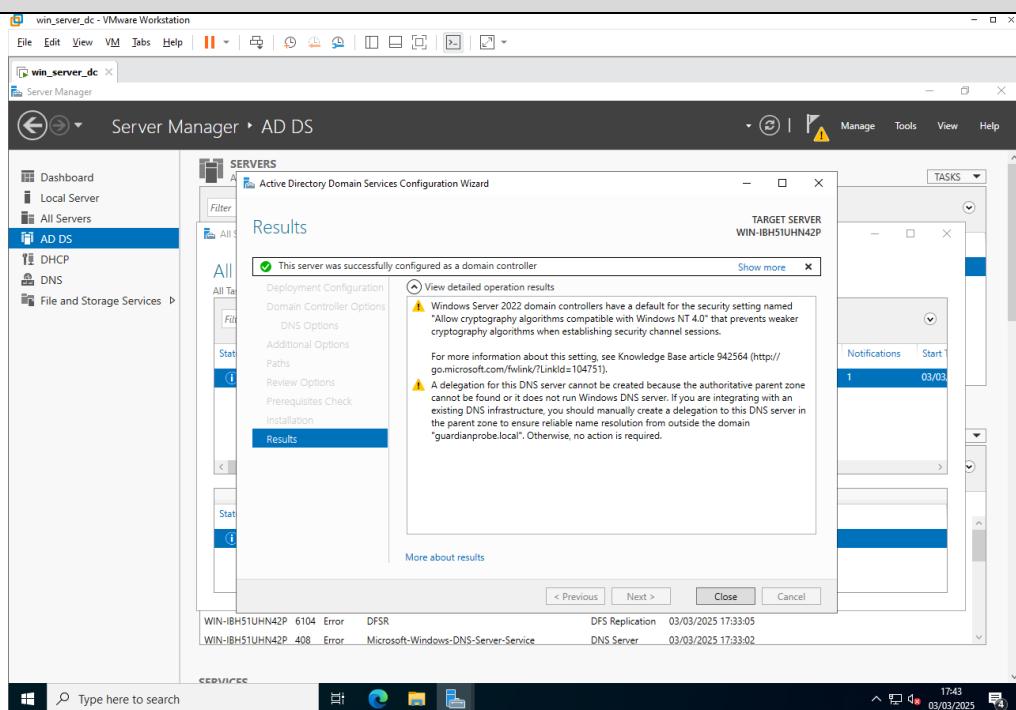


Imagen 23

Técnico Especialista Cibersegurança - CET93

- Server será reiniciado automaticamente após a config completa do ADDS.
- Por padrão na interface de rede no Preferred DNS Server pega o ip loopback, se esse for o caso deverá reconfigurar de acordo com o ambiente do projeto.

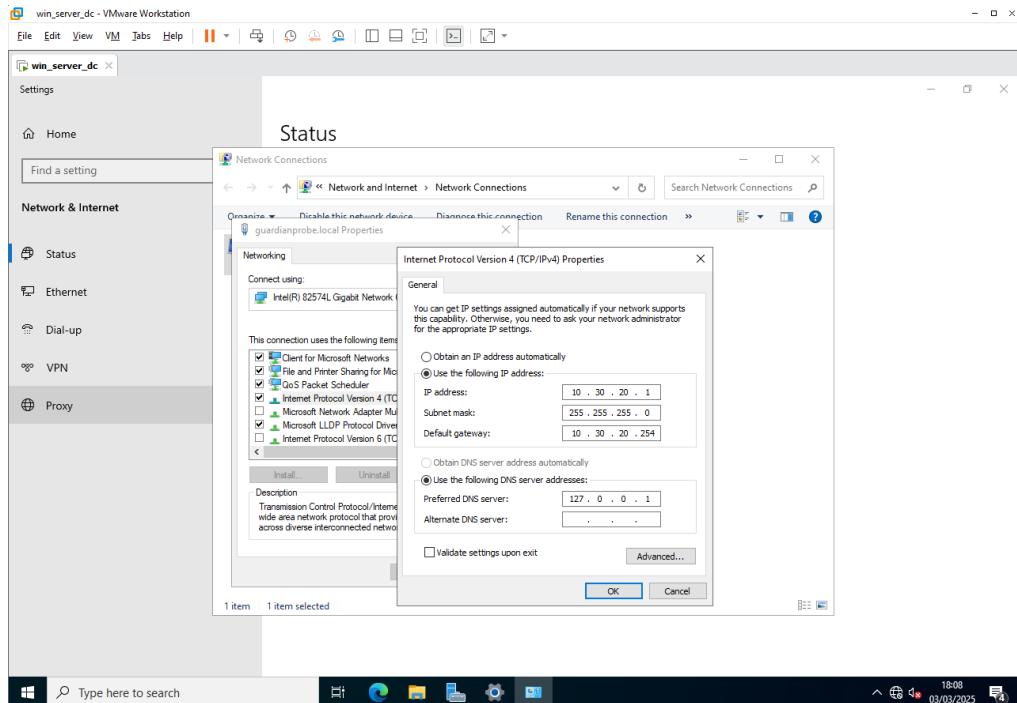


Imagen 24

- Deverá alterar o Computer Name de acordo com o ambiente do projeto, e reiniciar.

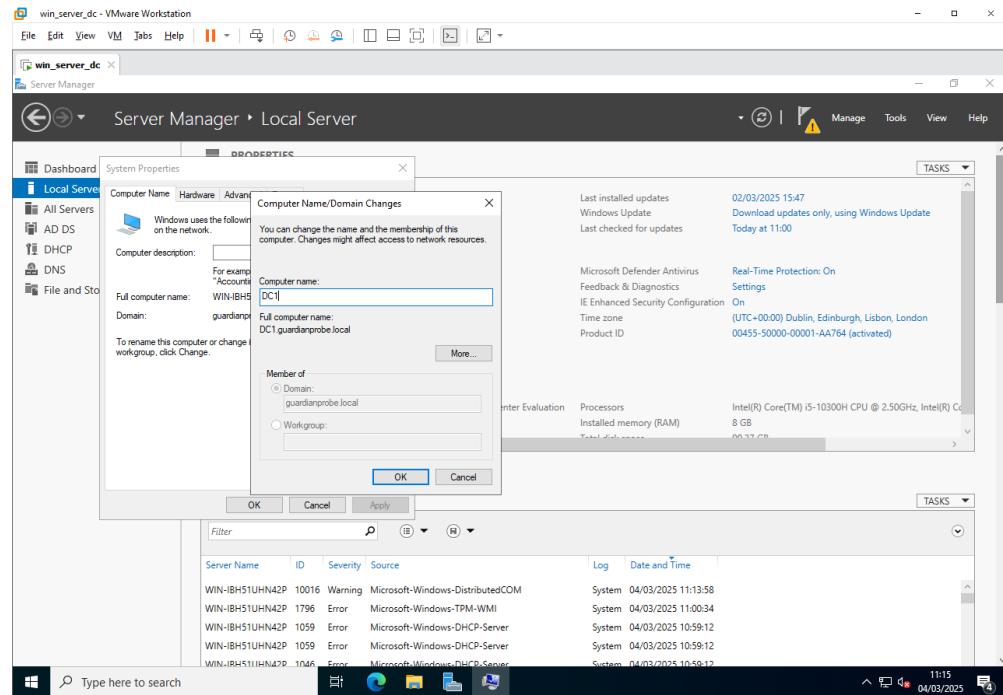
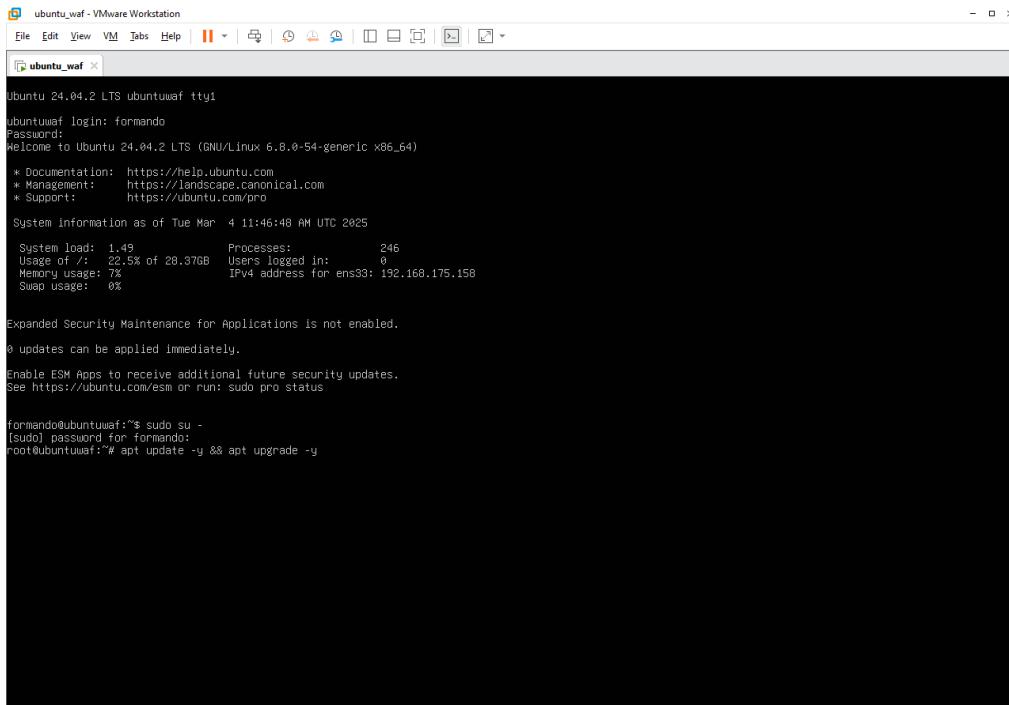


Imagen 25

Ubuntu Linux (WAF)

Configs e settings:

- Após install do S.O, realizar update e upgrade do sistema.
- sudo apt update -y && apt upgrade -y
-



```
ubuntu_waf - VMware Workstation
File Edit View VM Tabs Help ||| X
ubuntu_waf x
Ubuntu 24.04.2 LTS ubuntuwaf tty1
ubuntuwaf login: formando
Password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-54-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Tue Mar  4 11:46:48 AM UTC 2025

System load: 1.49 Processes: 246
Usage of /: 22.5% of 28.37GB Users logged in: 0
Memory usage: 7% IPv4 address for ens3: 192.168.175.158
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

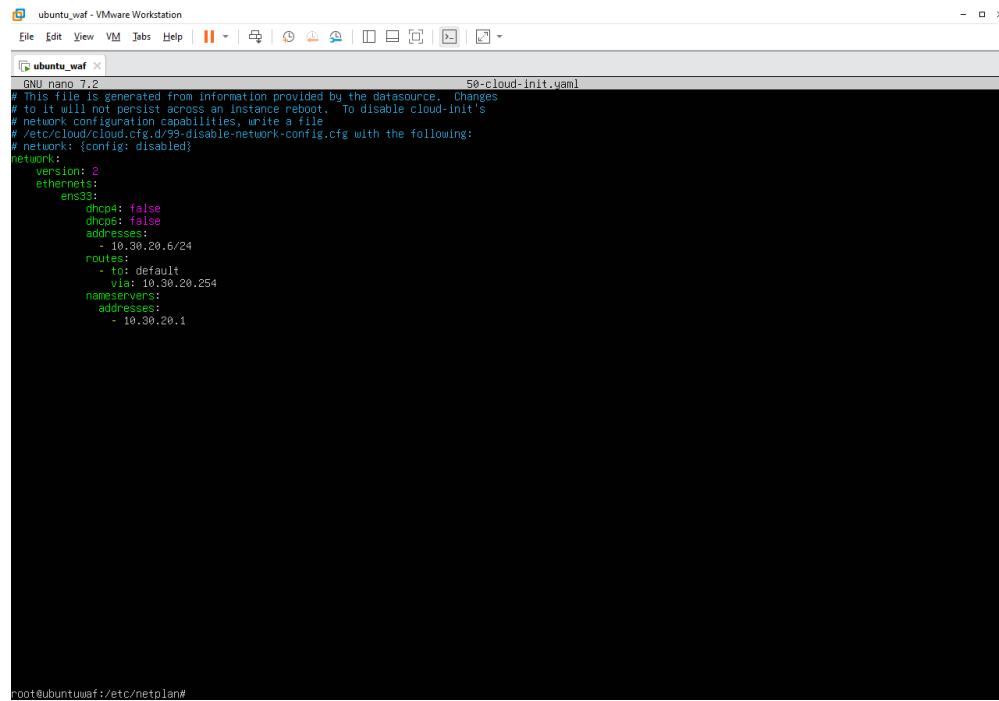
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

formando@ubuntuwaf:~$ sudo su -
[sudo] password for formando:
root@ubuntuwaf:~# apt update -y && apt upgrade -y
```

Imagen 26

- Config interface de rede, netplan.
- /etc/netplan

Técnico Especialista Cibersegurança - CET93

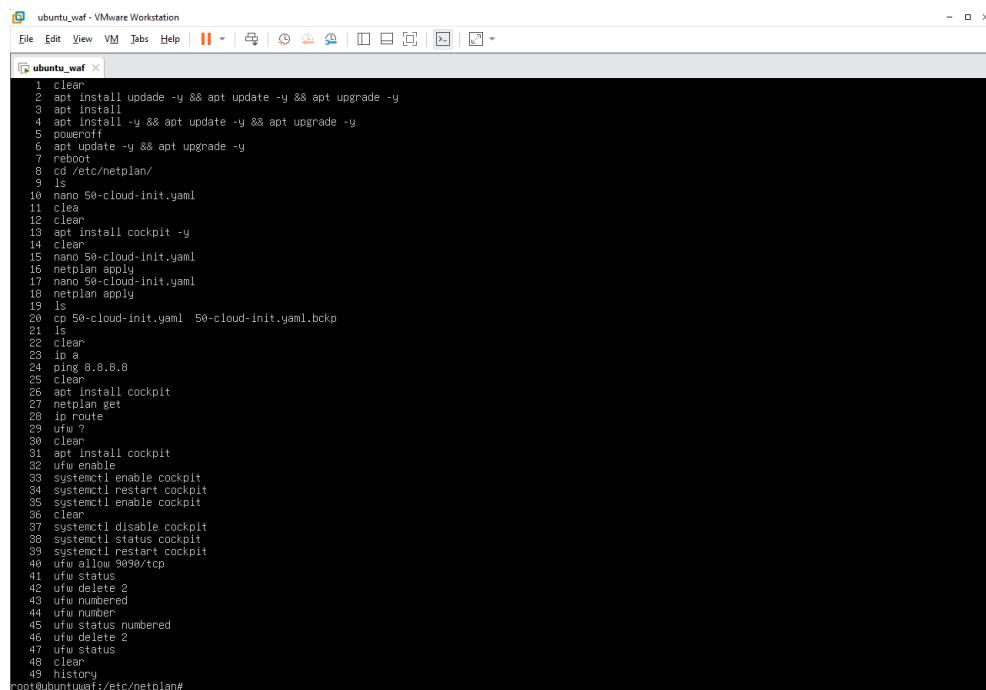


```
ubuntu_waf ~
GNU nano 7.2                               50-cloud-init.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: false
      dhcp6: false
      addresses:
        - 10.30.20.6/24
      routes:
        - to: default
          via: 10.30.20.254
      nameservers:
        addresses:
          - 10.30.20.1

root@ubuntuwaf:/etc/netplan#
```

Imagen 27

- Inserir comando, netplan apply.
- netplan apply para definir e atualizar com as configurações realizadas no arquivo.
- Installar cockpit, sudo apt install cockpit
- Habilitar UFW (Uncomplicated Firewall) com config por padrão, ufw enable
- Habilitar abertura do port 9090/tcp para acesso ao cockpit através de outro dispositivo, ufw allow 9090/tcp



```
ubuntu_waf ~
1 clear
2 apt install update -y && apt update -y && apt upgrade -y
3 apt install -y
4 apt install -y && apt update -y && apt upgrade -y
5 poweroff
6 apt update -y && apt upgrade -y
7 reboot
8 cd /etc/netplan/
9 ls
10 nano 50-cloud-init.yaml
11 clear
12 apt install cockpit -y
13 clear
14 nano 50-cloud-init.yaml
15 netplan apply
16 nano 50-cloud-init.yaml
17 netplan apply
18 ls
19 cp 50-cloud-init.yaml 50-cloud-init.yaml.bckp
20 ls
21 clear
22 clear
23 ip a
24 ping 0.0.0.0
25 clear
26 apt install cockpit
27 netplan get
28 ip route
29 ufw ?
30 clear
31 apt install cockpit
32 ufw enable
33 systemctl enable cockpit
34 systemctl restart cockpit
35 systemctl enable cockpit
36 clear
37 systemctl disable cockpit
38 systemctl status cockpit
39 systemctl restart cockpit
40 ufw allow 9090/tcp
41 ufw status
42 ufw delete 2
43 ufw numbered
44 ufw number
45 ufw status numbered
46 ufw delete 2
47 ufw status
48 clear
49 history
root@ubuntuwaf:/etc/netplan# _
```

Imagen 28

Técnico Especialista Cibersegurança - CET93

Acessar Ubuntu Server pelo cockpit através de outro PC no browser,
<https://10.30.20.6:9090/>

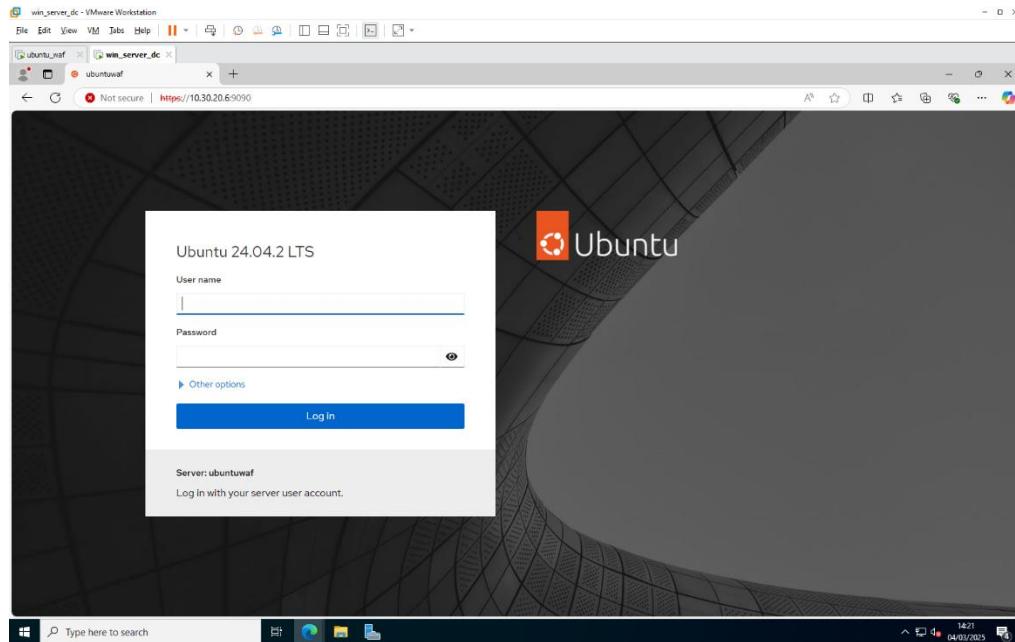


Imagen 29

mod-security

```
sudo apt install apache2 libapache2-mod-security2 -y
```

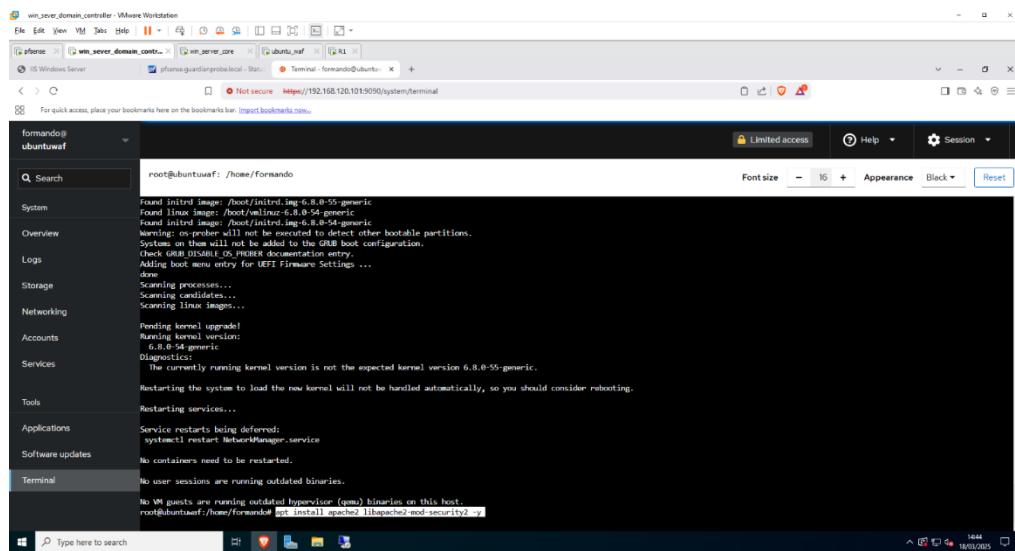


Imagen 30

Técnico Especialista Cibersegurança - CET93

Restart services

```
sudo a2enmod proxy
sudo a2enmod proxy_http
sudo a2enmod security2
sudo systemctl restart apache2
```

Repo modsecurity core rule set

```
Clonar repositório corerules:
cd /usr/share/modsecurity-crs
git clone https://github.com/coreruleset/coreruleset.git
```

- Copiar e alterar arquivo de configuração modsecurity.conf

```
cd /etc/modsecurity/
ls
cp /etc/modsecurity/modsecurity.conf-recommended
/etc/modsecurity/modsecurity.conf
nano /etc/modsecurity/modsecurity.conf
```

- Alterar essas config no arquivo:

```
# Enable ModSecurity
SecRuleEngine On
# Enable request body inspection
SecRequestBodyAccess On
# Disable response body inspection (optional)
SecResponseBodyAccess Off
# Log debug data
SecDebugLog /var/log/apache2/modsec_debug.log
# Set debug log level (adjust as needed)
SecDebugLogLevel 3
# Log audit data
SecAuditLog /var/log/apache2/modsec_audit.log
```

- Criar links das regras modsecurity:

```
ln -s /usr/share/modsecurity-crs/crs-setup.conf.example /etc/modsecurity/crs-
setup.conf
ln -s /usr/share/modsecurity-crs/rules/REQUEST-900-EXCLUSION-RULES-BEFORE-
CRS.conf /etc/modsecurity/
ln -s /usr/share/modsecurity-crs/rules/RESPONSE-999-EXCLUSION-RULES-AFTER-
CRS.conf /etc/modsecurity/
```

Técnico Especialista Cibersegurança - CET93

```
sudo systemctl restart apache2
sudo nano /etc/apache2/sites-available/reverse-proxy.conf

<VirtualHost *:80> ServerName your-domain.com
# Enable ModSecurity
SecRuleEngine On

# Proxy settings
ProxyPreserveHost On
ProxyPass / http://<IIS SERVER IP>:80/
ProxyPassReverse / http://<IIS SERVER IP>:80/

# Optional: Secure SSL connections
# ProxyPass / https://<IIS SERVER IP>:443/
# ProxyPassReverse / https://<IIS SERVER IP>:443/

# Error handling
ErrorLog ${APACHE_LOG_DIR}/reverse-proxy-error.log
CustomLog ${APACHE_LOG_DIR}/reverse-proxy-access.log combined
```

- Reload service apache2, activate virtual host e ver test de config

```
systemctl reload apache2
a2ensite reverse-proxy.conf
apachectl configtest
```

- Copiar chave e certificado para o Ubuntu WAF, pelo pfSense:

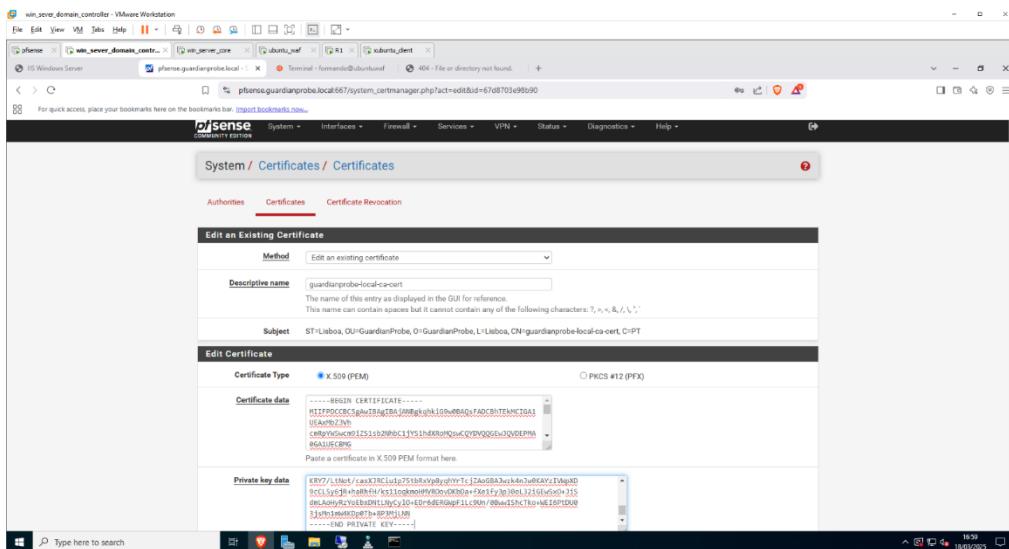


Imagen 31

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
Start-Service sshd
Set-Service -Name sshd -StartupType 'Automatic'
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled
True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
```

Técnico Especialista Cibersegurança - CET93

- Criar certificado para o web page IIS WAF

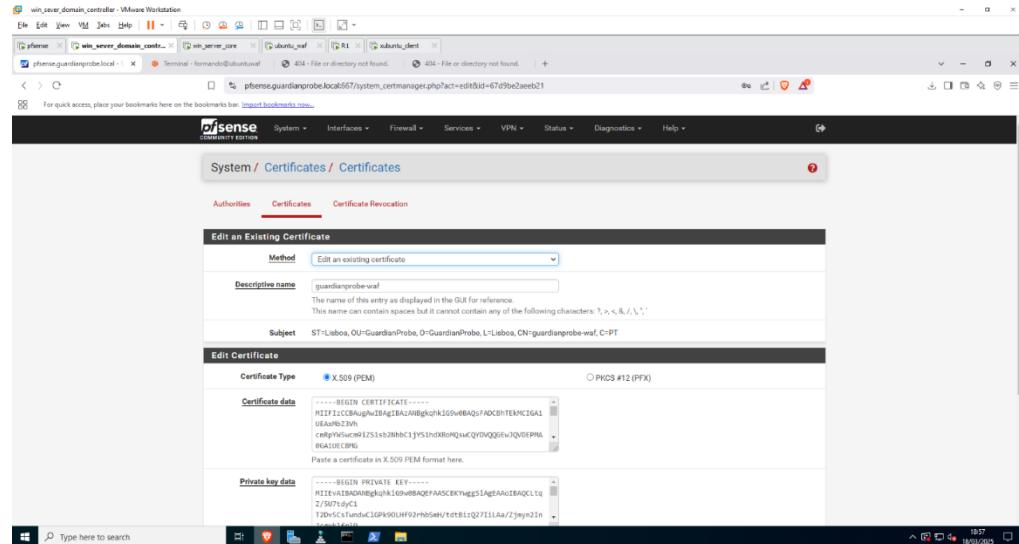


Imagen 32

Nos campos adicionar:

- FQDN or HOSTNAME: www.guardianprobe.local
- IP: 192.168.120.101
 - Copiar .cert e .key para o Ubuntu WAF, do windows DC1

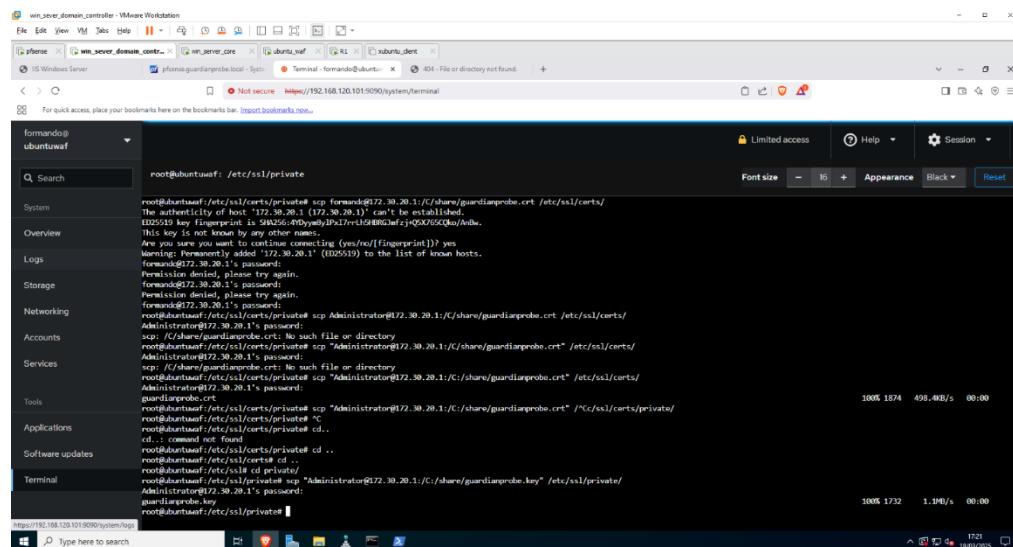


Imagen 33

```
scp "Administrator@172.30.20.1:/C:/share/guardianprobe.crt" /etc/ssl/certs/
scp "Administrator@172.30.20.1:/C:/share/guardianprobe.key" /etc/ssl/private/
```

Técnico Especialista Cibersegurança - CET93

Criar VirtualHost para SSL:

```
nano /etc/apache2/sites-available/reverse-proxy-ssl.conf
```

```
<VirtualHost *:443>
ServerName guardianprobe.local

# Enable SSL
SSLEngine On
SSLCertificateFile /etc/ssl/certs/guardianprobe.crt
SSLCertificateKeyFile /etc/ssl/private/guardianprobe.key
# SSLCertificateChainFile /etc/ssl/certs/intermediate-cert.crt

# Enable ModSecurity
SecRuleEngine On

# Proxy settings (forward to IIS over HTTP)
ProxyPreserveHost On
ProxyPass / http://192.168.120.102:80/
ProxyPassReverse / http://192.168.120.102:80/

# Error handling
ErrorLog ${APACHE_LOG_DIR}/reverse-proxy-ssl-error.log
CustomLog ${APACHE_LOG_DIR}/reverse-proxy-ssl-access.log combined
```

Reiniciar apache2, ativar ssl, ativar ssl proxy conf e reload apache2:

```
systemctl restart apache2
2enmod ssl
a2ensite reverse-proxy-ssl.conf
systemctl reload apache2
a2ensite reverse-proxy-ssl.conf
```

Adicionar o WWW ao dns do DC1:

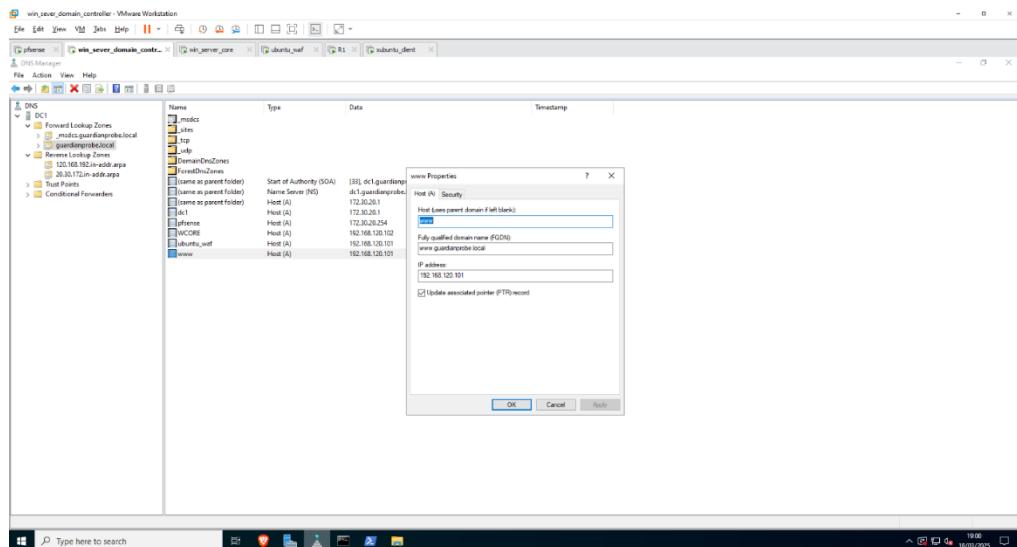


Imagen 34

Técnico Especialista Cibersegurança - CET93

- Adicionar ao arquivo /etc/hosts do PC remoto:

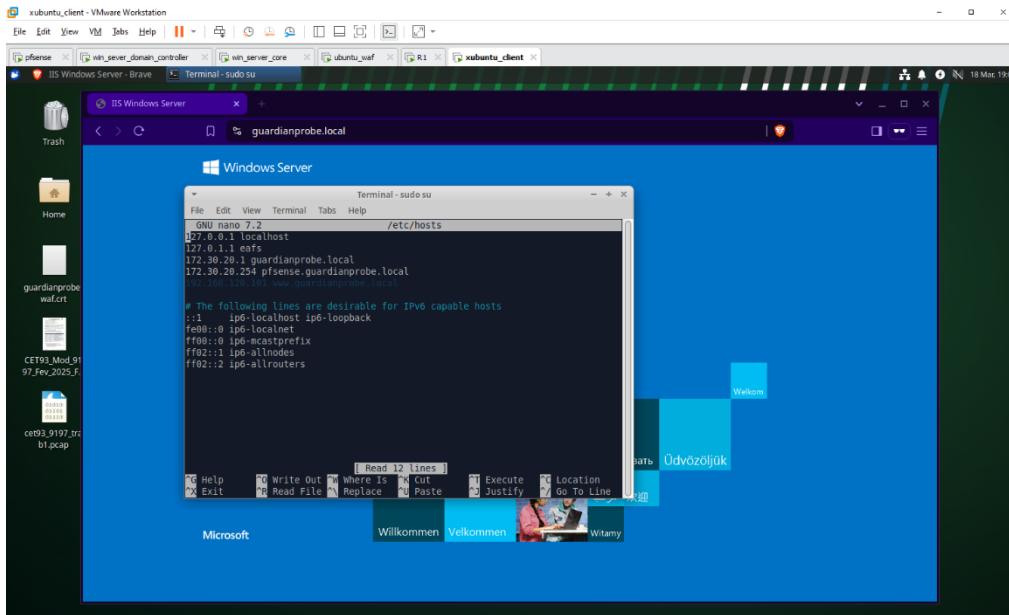


Imagen 35

Windows Server DC1 RADIUS VPN

Criar OU e criar user ao OU.

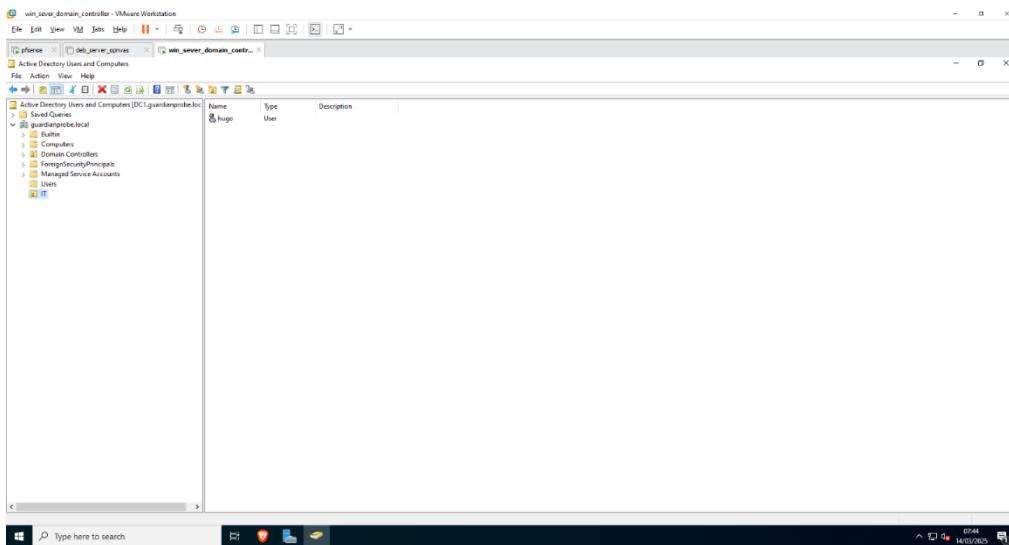


Imagen 36

«

Técnico Especialista Cibersegurança - CET93

Criar openvpn para radius.

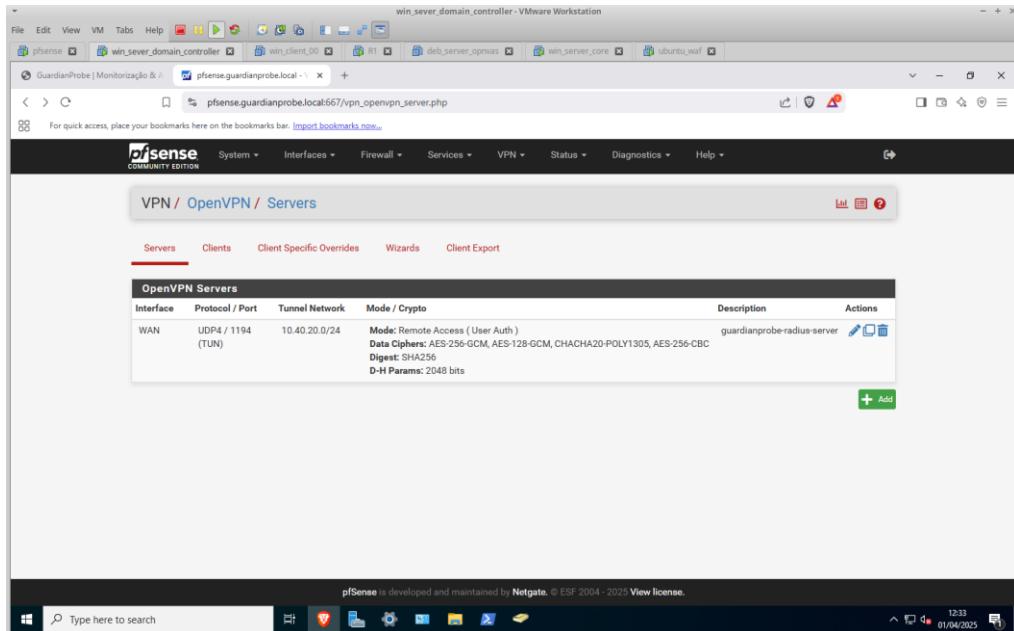


Imagen 37

- Backend for authentication – GuardianProbeServerAuth

IPv4 Tunnel Network – 10.40.20.0/24
IPv4 Local network(s) – 172.30.20.0/24

- DNS Default Domain – guardianprobe.local

DNS Server – 172.30.20.1

- SystemUser Manager - Authentication Servers - Shared Secret - Passw0rd
- Network Policy Server

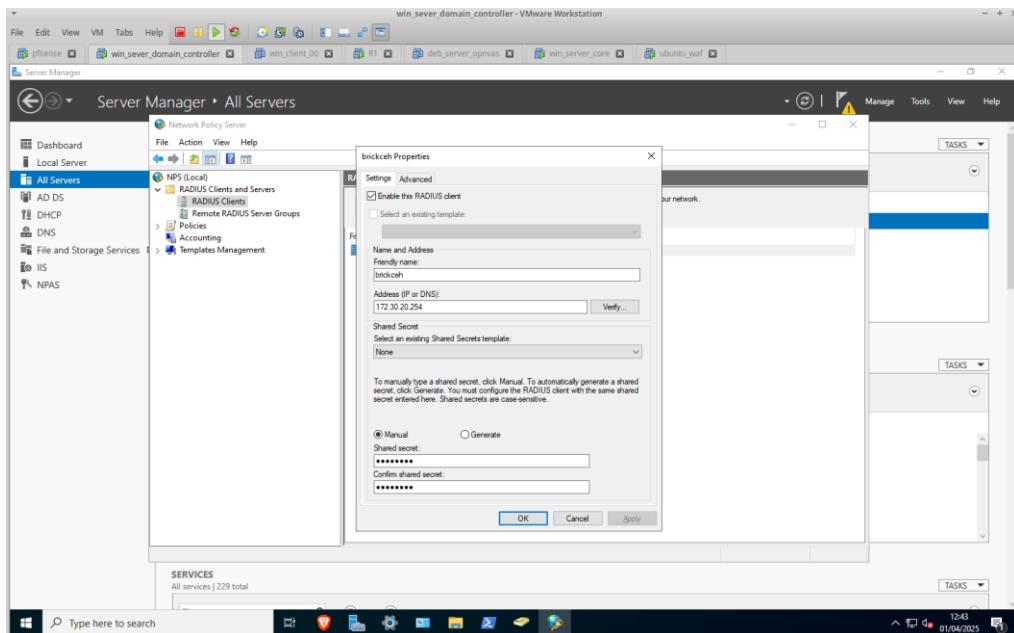


Imagen 38

Técnico Especialista Cibersegurança - CET93

- Address - 172.30.20.254
- Shared Secret - Passw0rd
- Network Policies

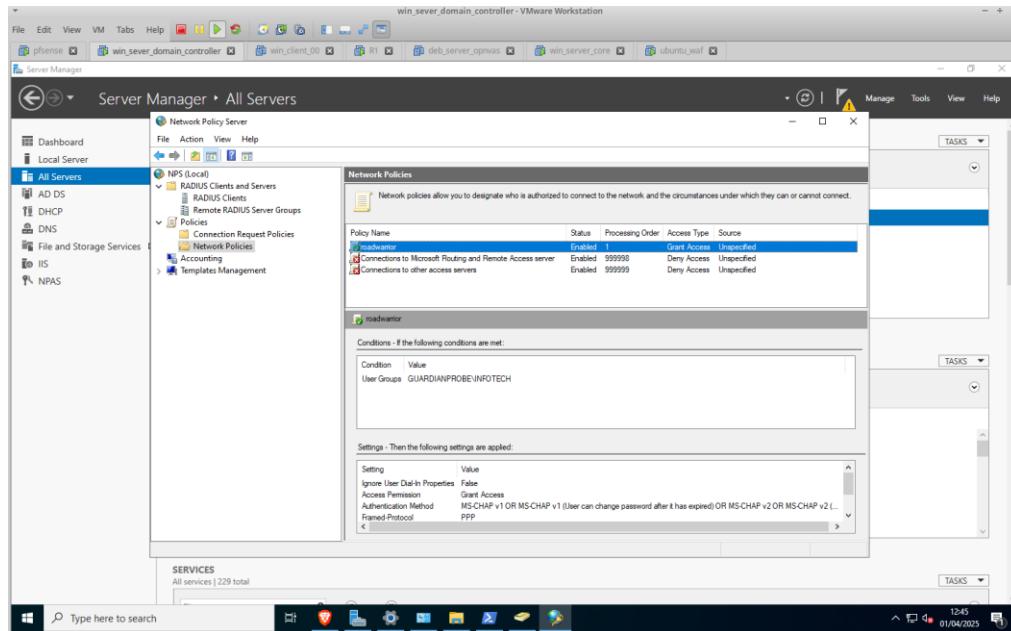


Imagen 39

- Habilitar roadwarrior policy

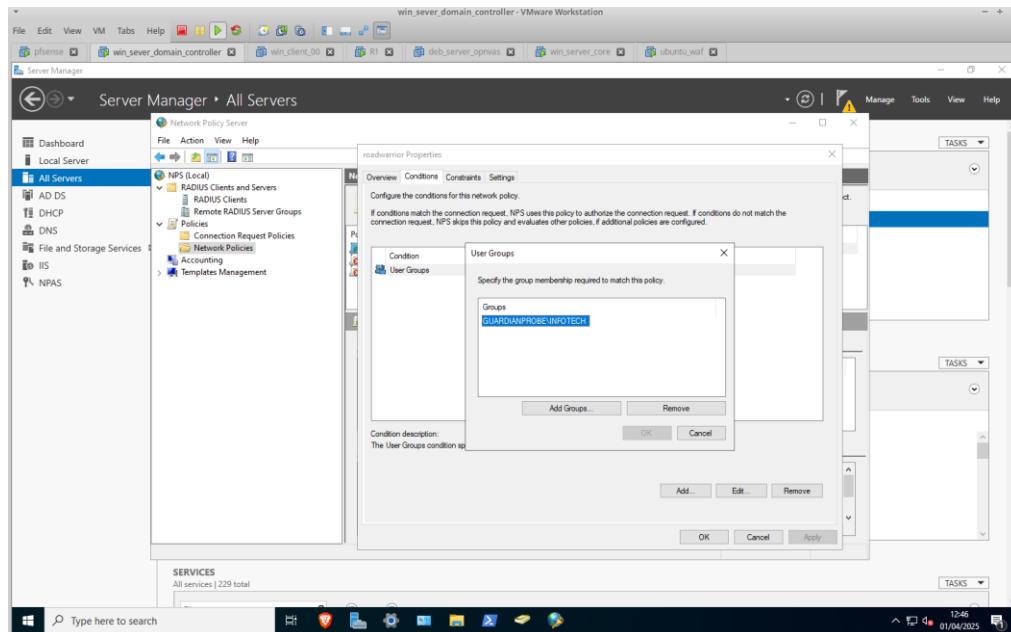


Imagen 40

Técnico Especialista Cibersegurança - CET93

- Adicionar o grupo OU que foi criado no ADDS ao policy roadwarrior.

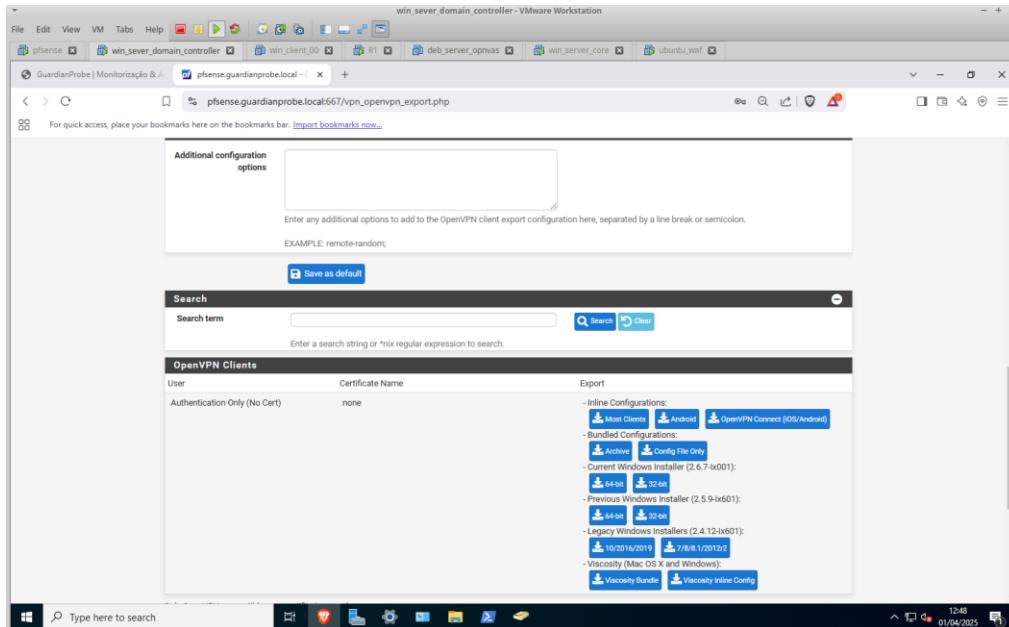


Imagen 41

- Baixar o instalador do client export open vpn para instalar no windows client.

Configuração VPN RoadWarrior RADIUS

Depois de Extraido a pasta colocar na seguinte localização:

C:\Program Files\OpenVPN\config

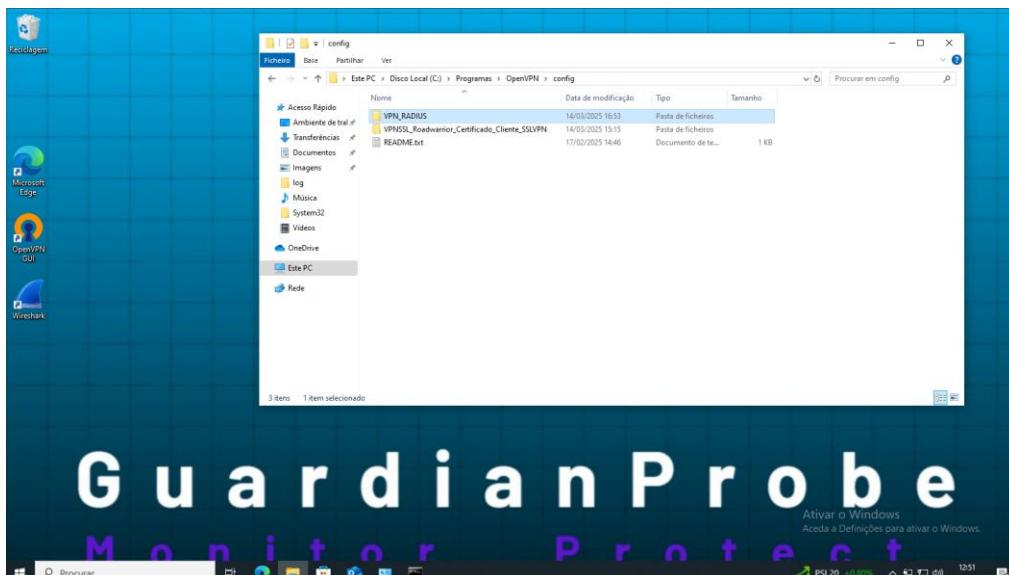


Imagen 12

Técnico Especialista Cibersegurança - CET93

Com o lado direito do rato, clicar no ícon do OpenVPN e selecionar a VPN importada anteriormente (RADIUS)

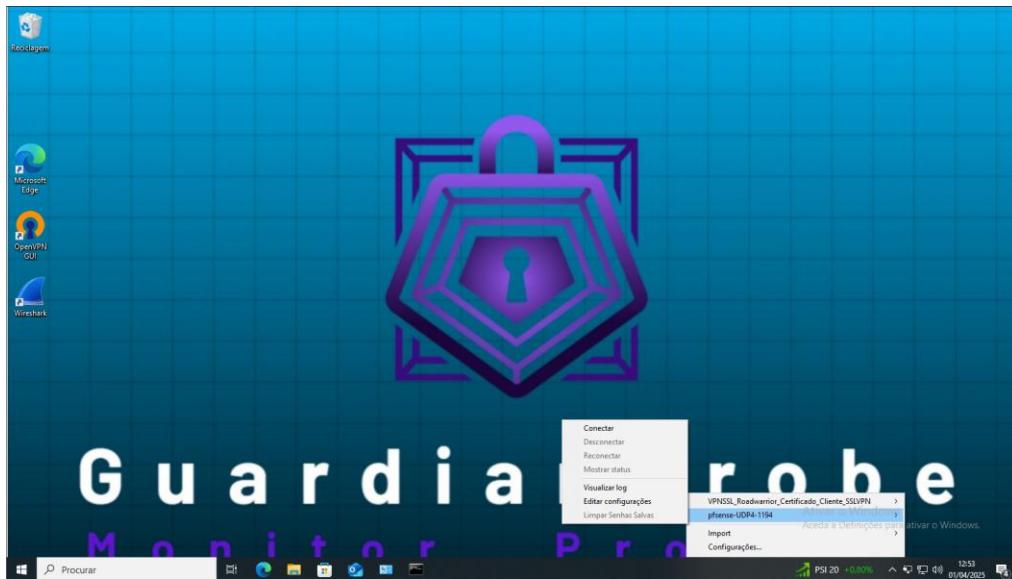


Imagen 13

Usar as credenciais que foram criadas no Windows Server (Utilizador IT)



Imagen 14

Verificamos que a conexão foi concluída com sucesso.

Técnico Especialista Cibersegurança - CET93

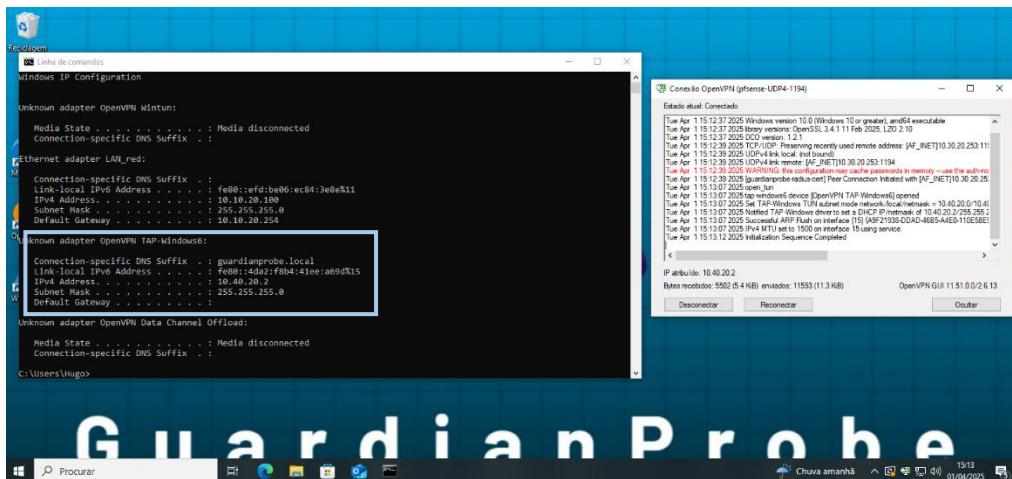


Imagen 15

Windows Server CORE

Definir os settings de rede:

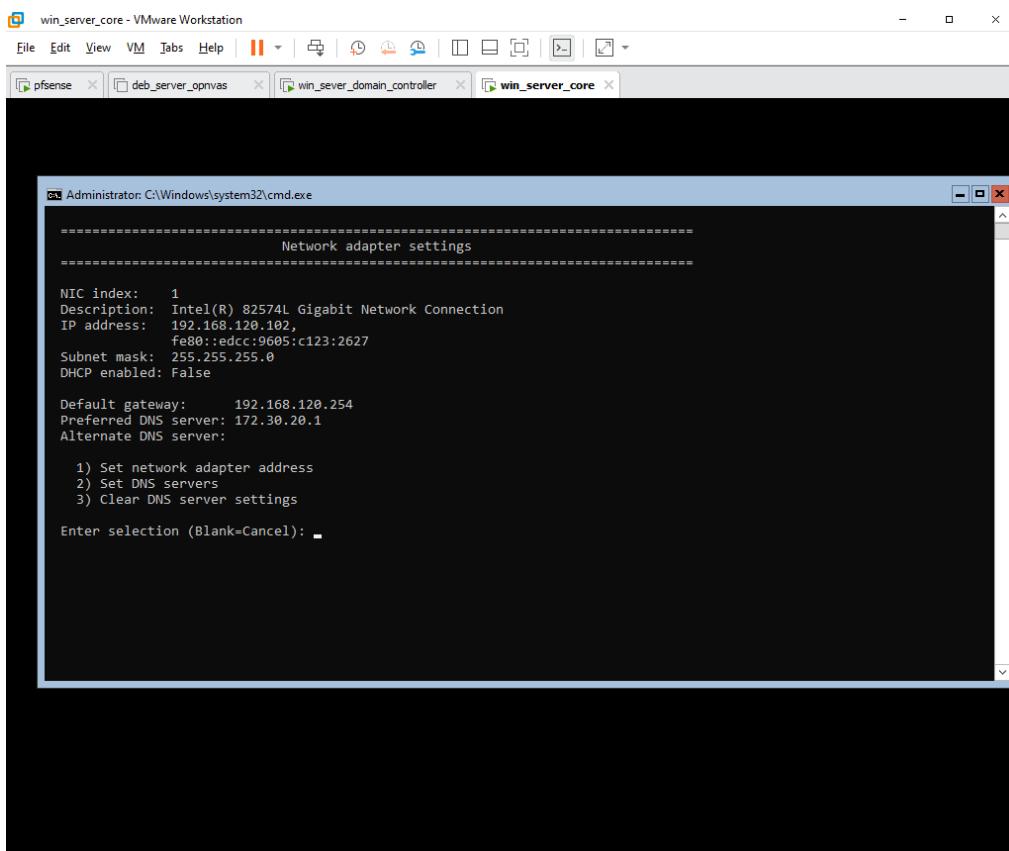


Imagen 42

Adicionar Windows Core no AD

Técnico Especialista Cibersegurança - CET93

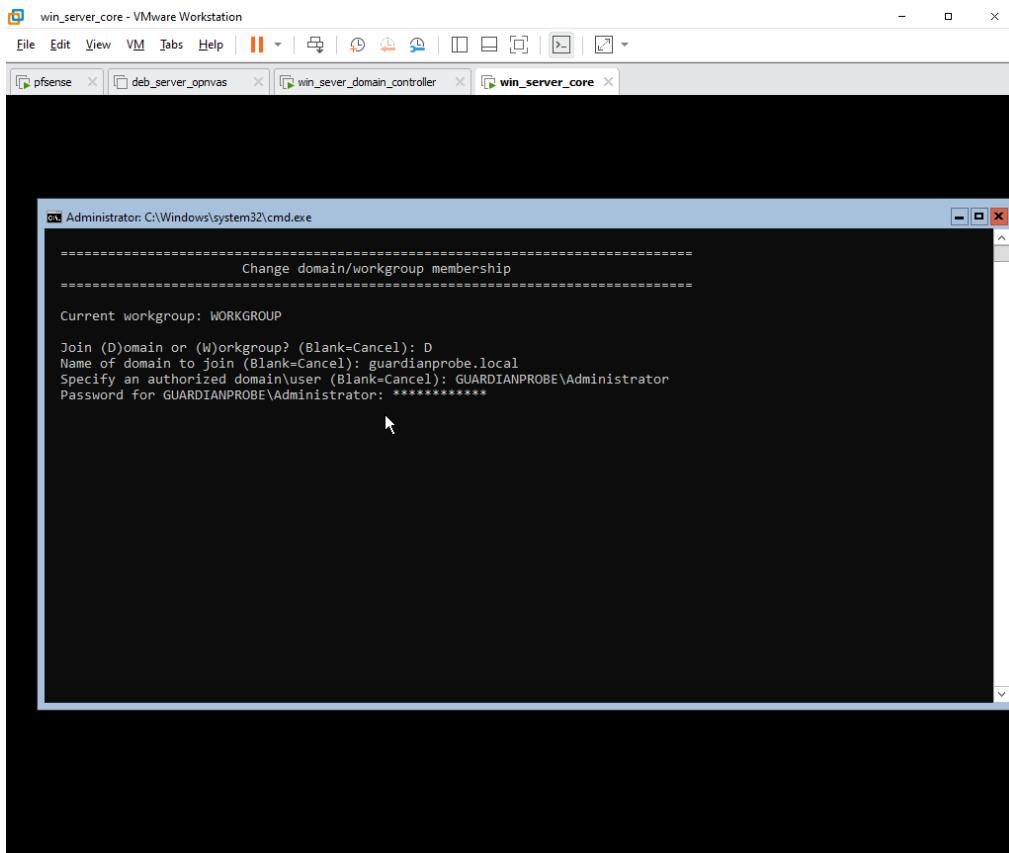


Imagen 43

Adicionar Server CORE para gerenciamento:

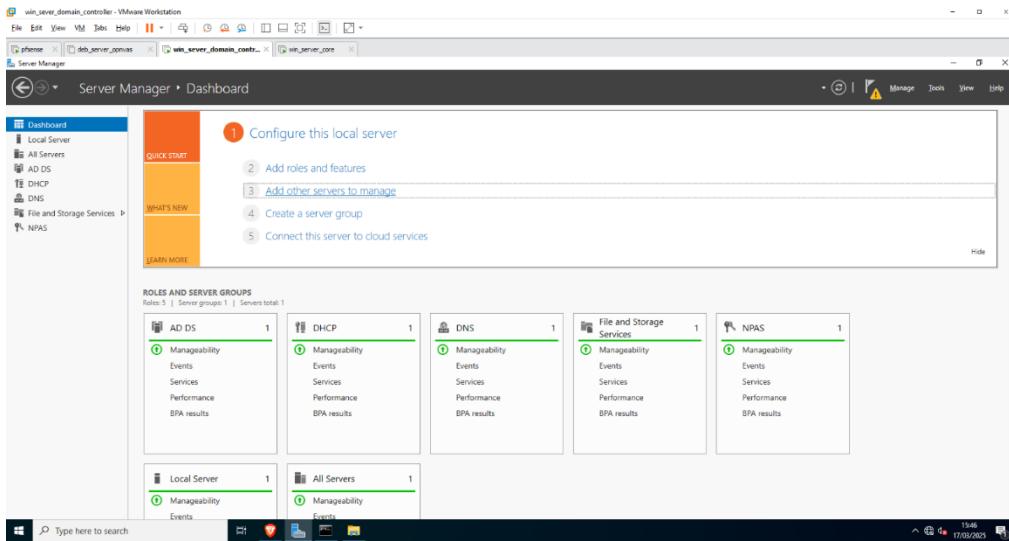


Imagen 44

Técnico Especialista Cibersegurança - CET93

- Buscar o Windows CORE para ser adicionado

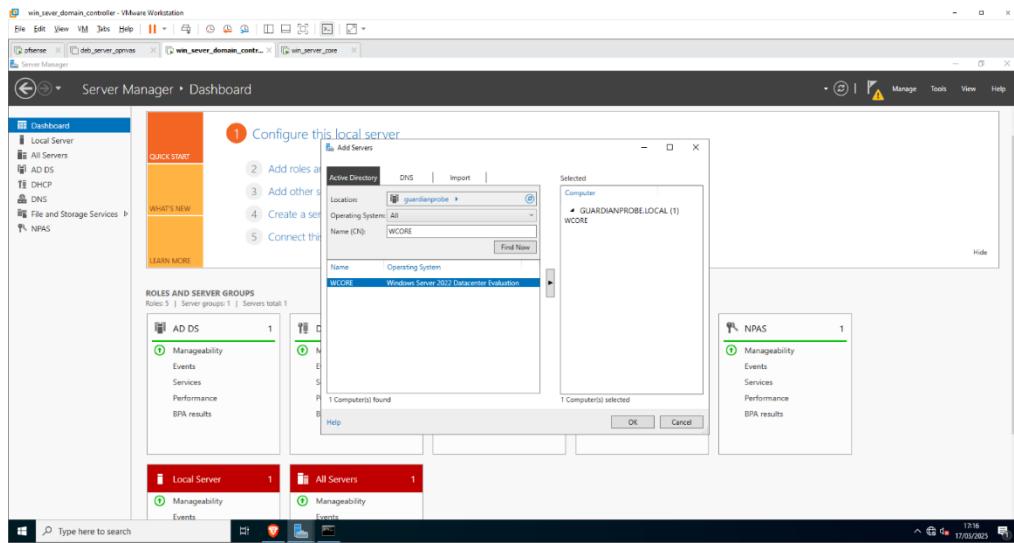


Imagen 45

- Verificar se foi adicionado.

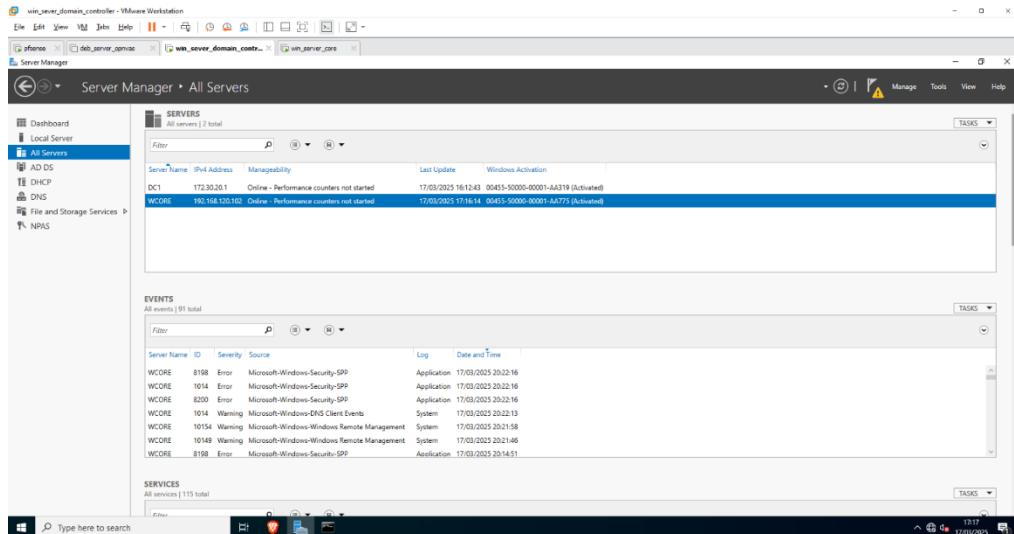


Imagen 46

Técnico Especialista Cibersegurança - CET93

Instalar IIS no Windows CORE pelo DC1 Server Manager:

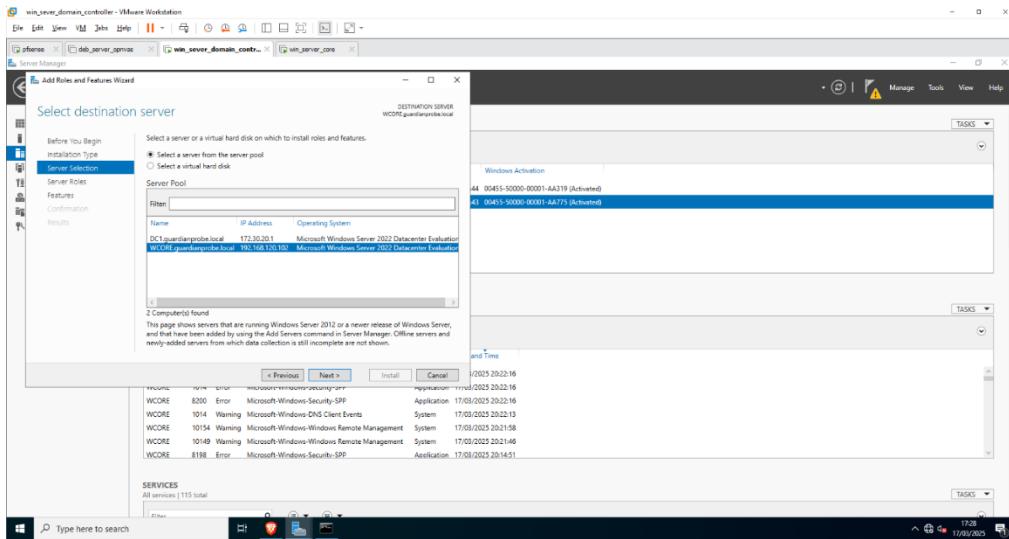


Imagen 47

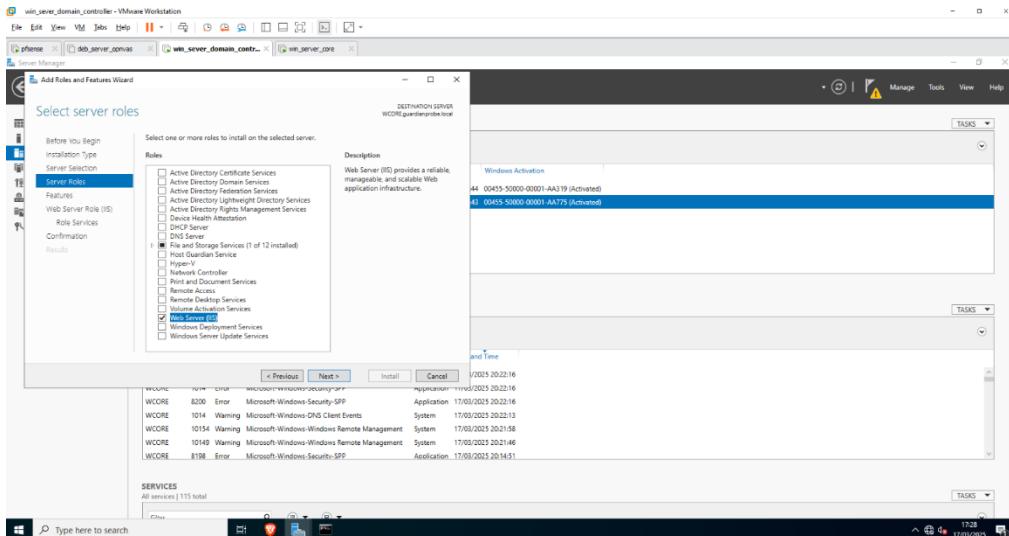


Imagen 48

Técnico Especialista Cibersegurança - CET93

- Instalado.

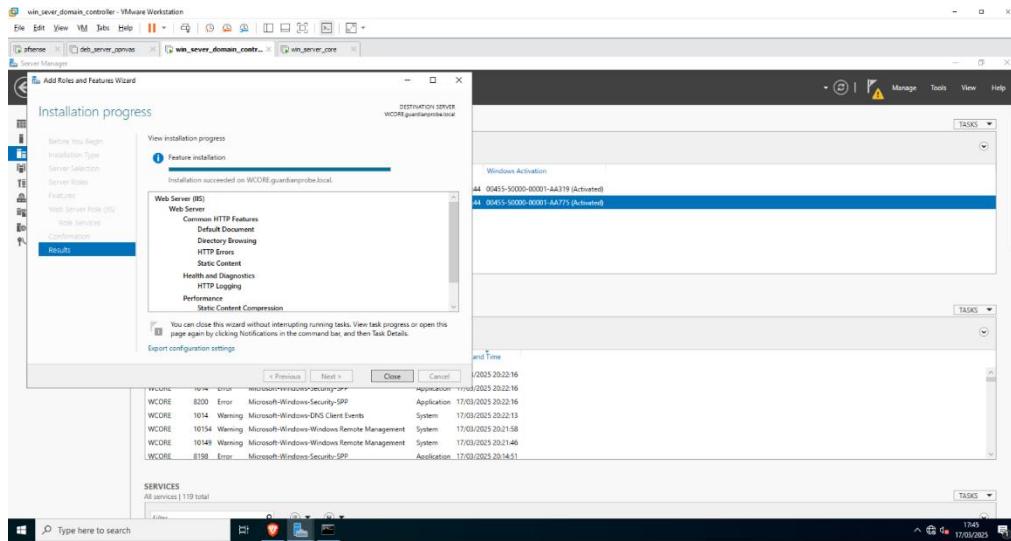


Imagen 4

- Conferir o status e o Service instalado.

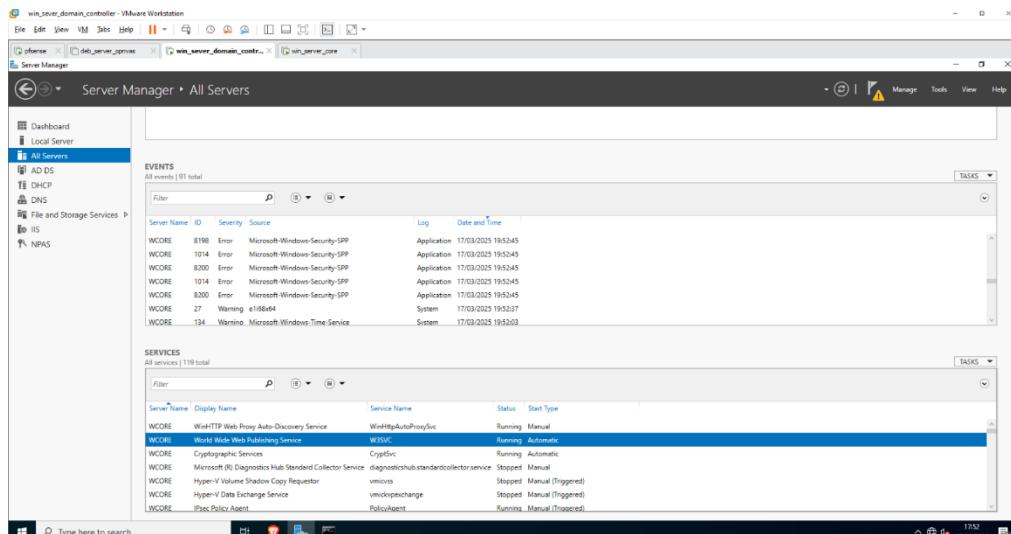


Imagen 50

Técnico Especialista Cibersegurança - CET93

- Acessar IIS via browser.

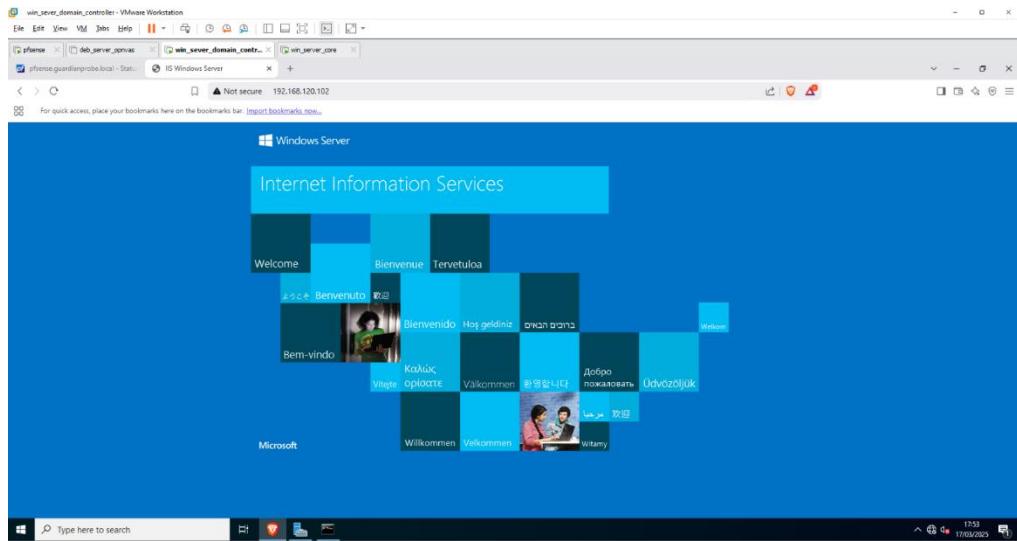


Imagen 51

Para alterar o conteúdo padrão do web page e da imagem do IIS, deve alterar o ficheiro *iisstart.htm* e *iisstart.png*.

```
Através do Windows Server DC1 para o Windows Server Core, utilizando o powershell:  
Copy-Item .\iisstart.htm -Destination "\\\192.168.120.102\C$\inetpub\wwwroot" -  
Recurse -Force  
Copy-Item .\iisstart.png -Destination "\\\192.168.120.102\C$\inetpub\wwwroot" -  
Recurse -Force
```

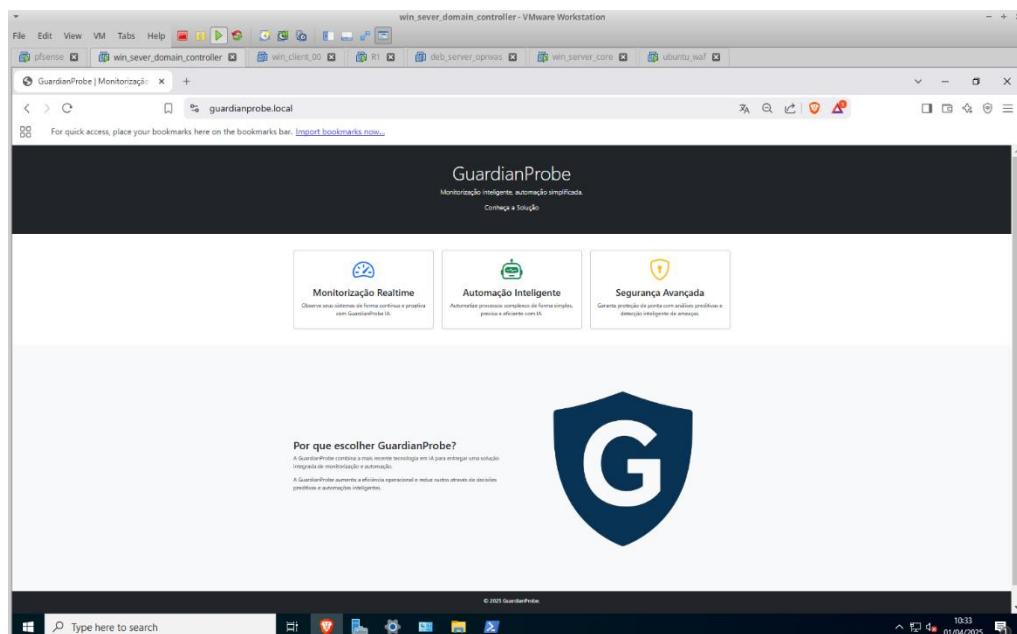


Imagen 52

Técnico Especialista Cibersegurança - CET93

Instalar nxlog ao Windows Server Core

```
Invoke-WebRequest -Uri "https://dl.nxlog.co/dl/67e140c364813" -OutFile "C:\nxlog-installer.msi"  
msiexec /i C:\nxlog-installer.msi /quiet /norestart
```

Teste para enviar log

```
logger -n 172.20.20.1 -P 514 -T "Remote syslog test event"
```

Arquivo de config para o nxsylog

```
<Input eventlog> Module im_msvisalog </Input>  
<Output syslog_out> Module om_udp Host 172.20.20.1 Port 514 Exec \ # Map  
Windows Event Log fields to syslog format \ $Message = "EventID=" + $EventID +  
" " + $Message; \ $Hostname = hostname(); \ $Severity = "INFO"; # Adjust based  
on $Level if needed \ to_syslog_bsd(); </Output>  
<Route eventlog_to_syslog> Path eventlog => syslog_out </Route>
```

Reiniciar service nxlog

```
net stop nxlog  
net start nxlog
```

Windows Server Core SQLSERVER

```
Invoke-WebRequest -Uri  
"https://go.microsoft.com/fwlink/?linkid=2216019&clcid=0x4009&culture=en-in&country=in" -OutFile "C:\SQLServer2022-ENU.exe"
```

```
.\setup.exe /Q /ACTION=Install  
/FEATURES=SQLENGINE,FullText,Replication,AS,IS,Conn /INSTANCENAME=MSSQLSERVER  
/INSTANCEID=MSSQLSERVER /SQLSVACCOUNT="NT Service\MSSQLSERVER"  
/SQLSYSADMINACCOUNTS="guardianprobe.local\Administrator" /ASSVCACCOUNT="NT  
Service\MSSQLServerOLAPService"  
/ASSYSADMINACCOUNTS="guardianprobe.local\Administrator"  
/ASSERVERMODE=MULTIDIMENSIONAL /TCPENABLED=1 /IAcceptSQLServerLicenseTerms=True
```

Técnico Especialista Cibersegurança - CET93

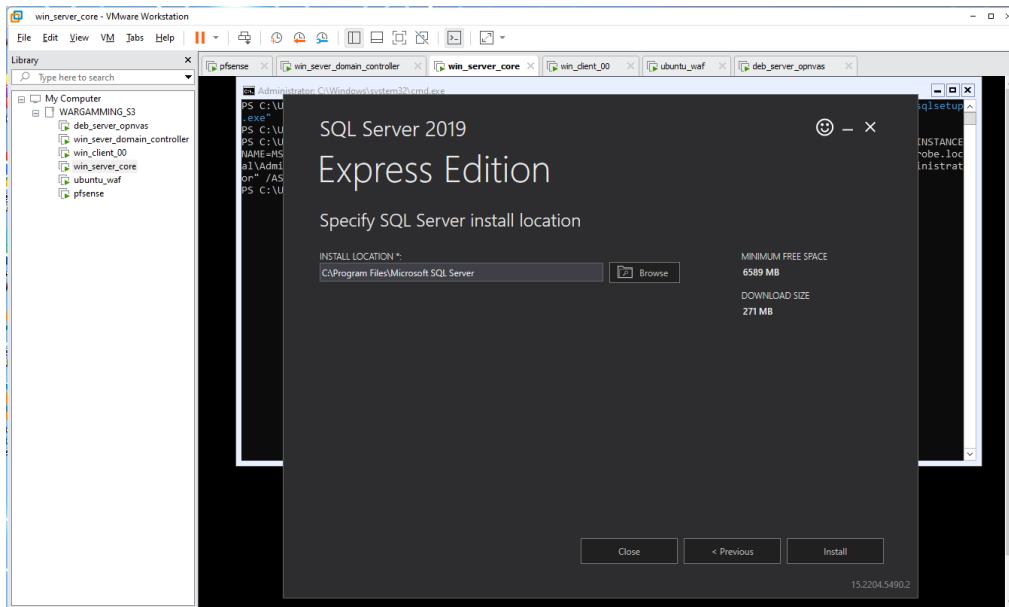


Imagen 53

Explicação dos parâmetros:

```
/Q
Instalação silenciosa (não-interativa).
/ACTION=Install
Realiza a instalação.
/FEATURES=SQLENGINE,FullText,Replication,AS,IS,Conn
Recursos a serem instalados.
/INSTANCENAME=MSSQLSERVER e /INSTANCEID=MSSQLSERVER
Instalação padrão (Default Instance).
/SQLSVCACCOUNT e /ASSVCACCOUNT
Contas padrão para execução dos serviços do SQL Server e Analysis Services.
/SQLSYSADMINACCOUNTS e /ASSYSADMINACCOUNTS
Administradores configurados para acesso aos serviços SQL e Analysis Services.
/ASERVERMODE=MULTIDIMENSIONAL
Define o modo operacional do Analysis Services.
/TCPENABLED=1
Habilita protocolo TCP/IP para conexões remotas.
/IAcceptSQLServerLicenseTerms=True
Aceitação obrigatória da licença.
```

Técnico Especialista Cibersegurança - CET93

Verificar services SQL:

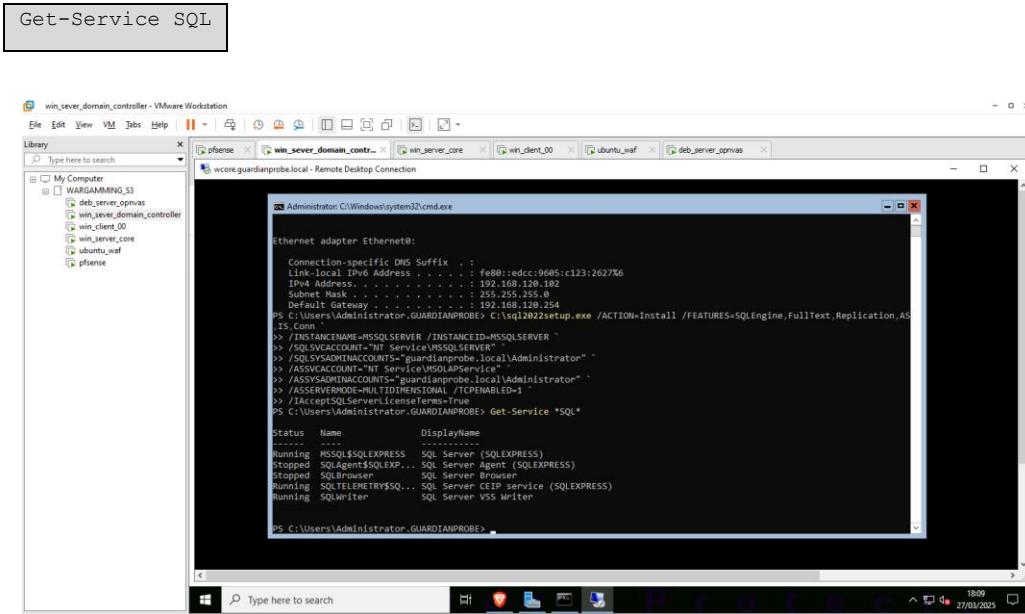


Imagen 54

Debian Server

OpenVAS

Instalar o OpenVas:

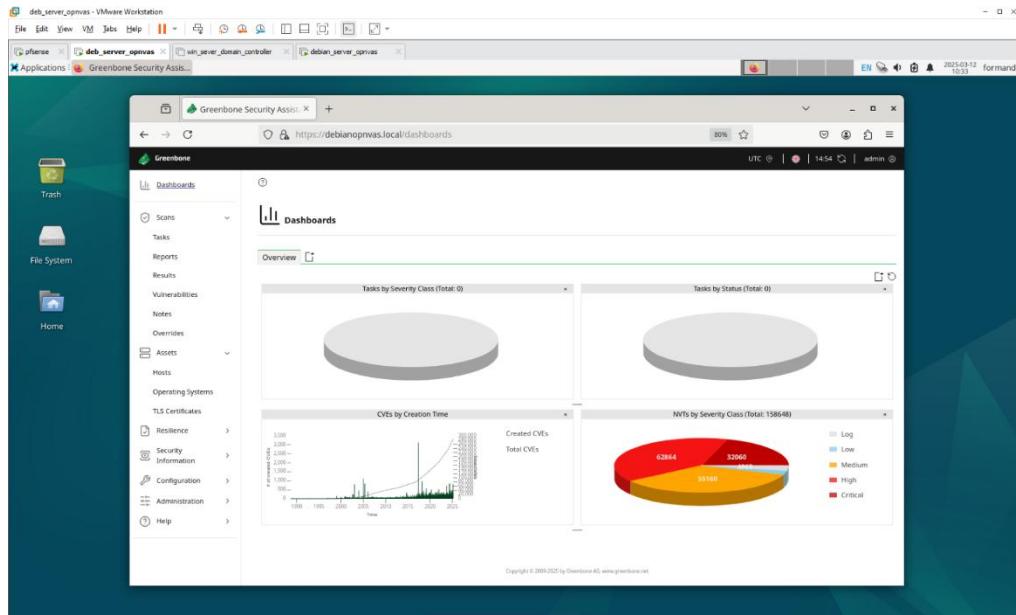


Imagen 55

Técnico Especialista Cibersegurança - CET93

- Usar o comando:

```
wget https://raw.githubusercontent.com/itiligious/Easy-OpenVAS-Installer/main/openvas-install.sh && chmod +x openvas-install.sh && ./openvas-install.sh
```

- Seguir os passos que são pedido, como definir user, definir password
- Após Instalação, acessar o GreenBone via Browser, e esperar atualizar o feed status.

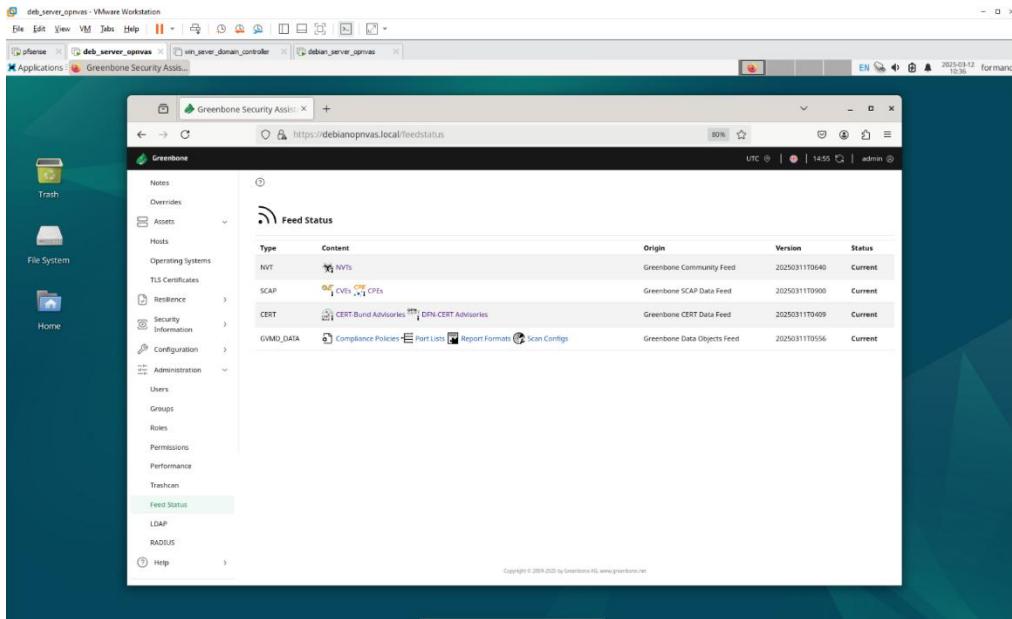


Imagen 56

Criar tarefas para varredura de rede:

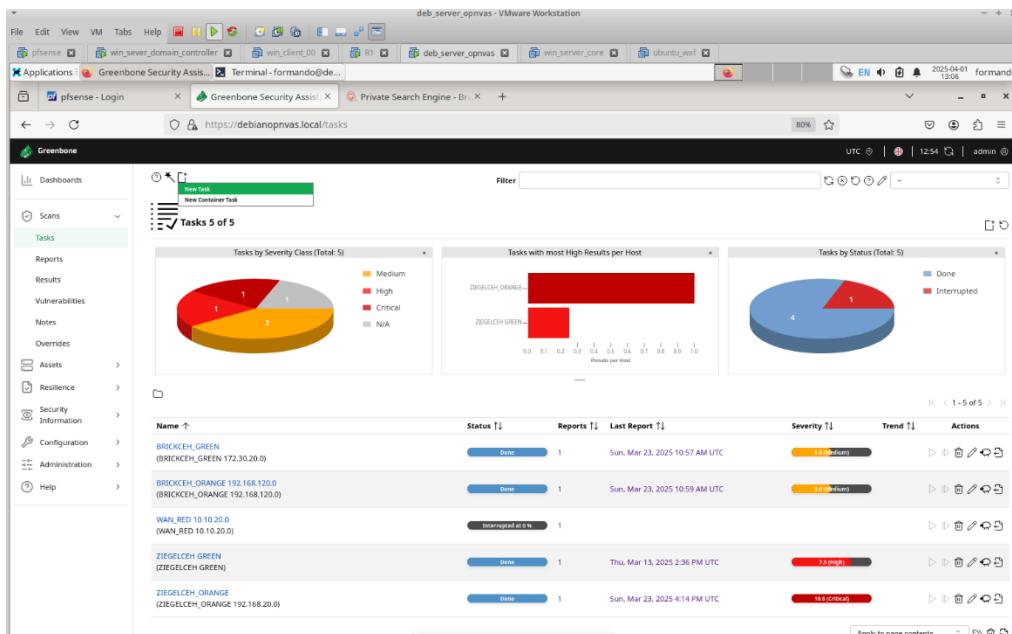


Imagen 57

Técnico Especialista Cibersegurança - CET93

Criar novo target/alvo de rede para varredura:

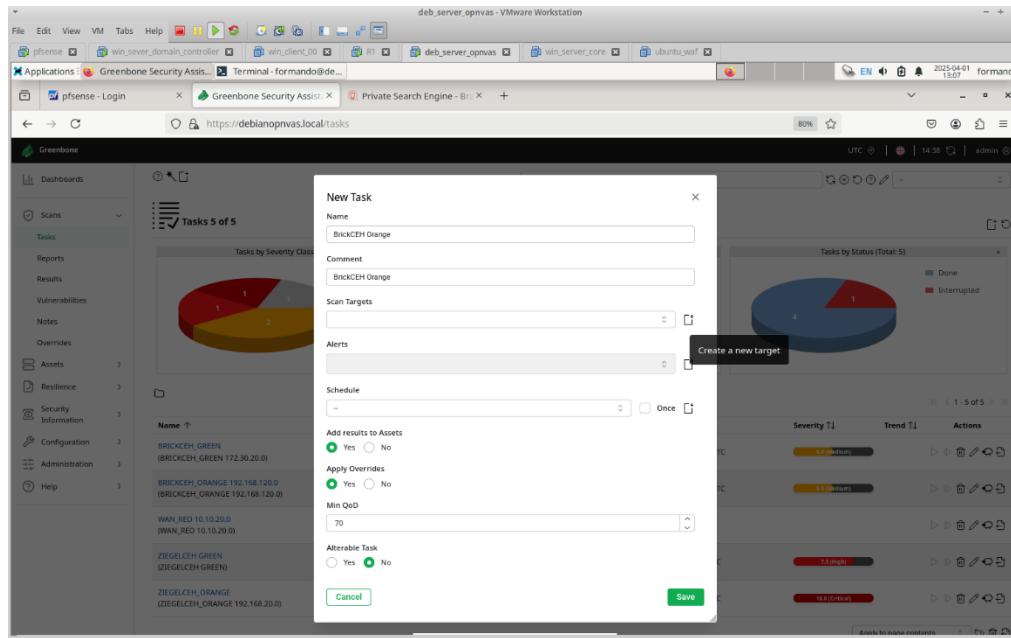


Imagen 58

- Adicionar o host para varredura e port lists All IANA assigned TCP and UDP

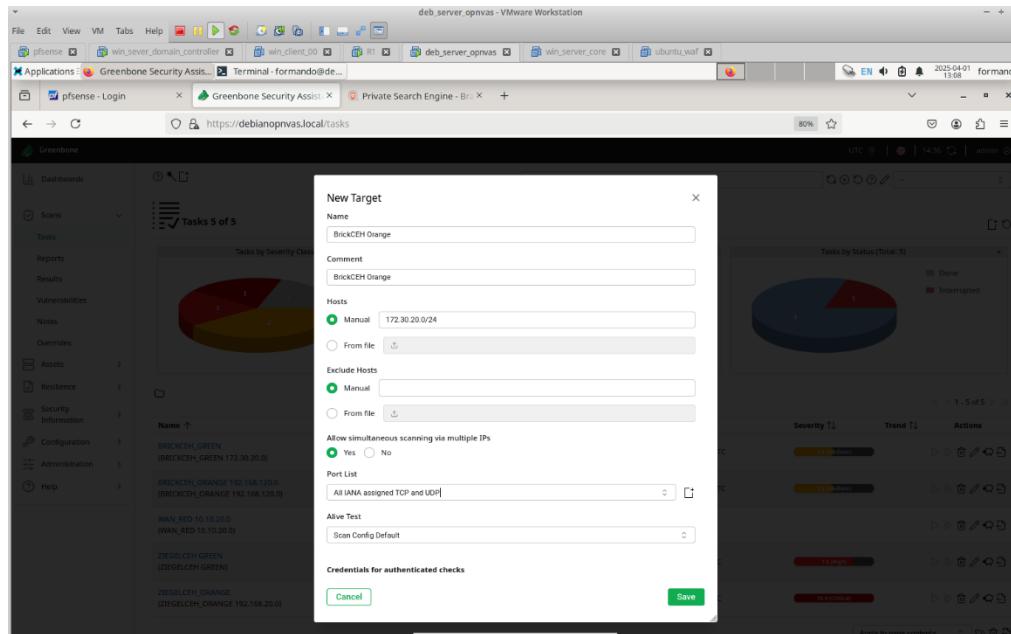


Imagen 59

Técnico Especialista Cibersegurança - CET93

- Após salvar o target, selecione o mesmo às tarefas

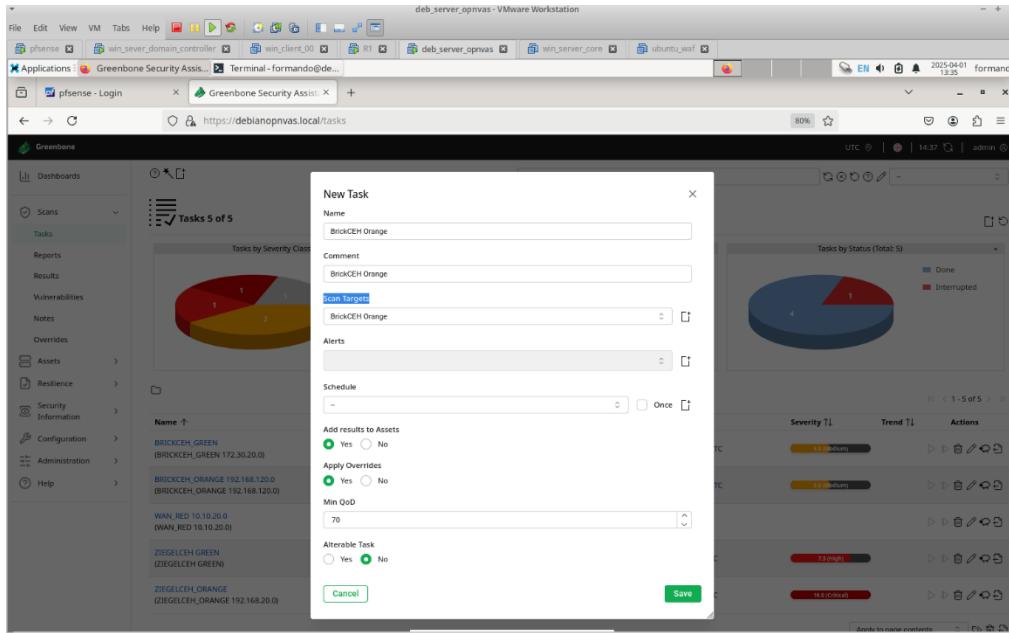


Imagen 60

Iniciar action para varredura da rede:

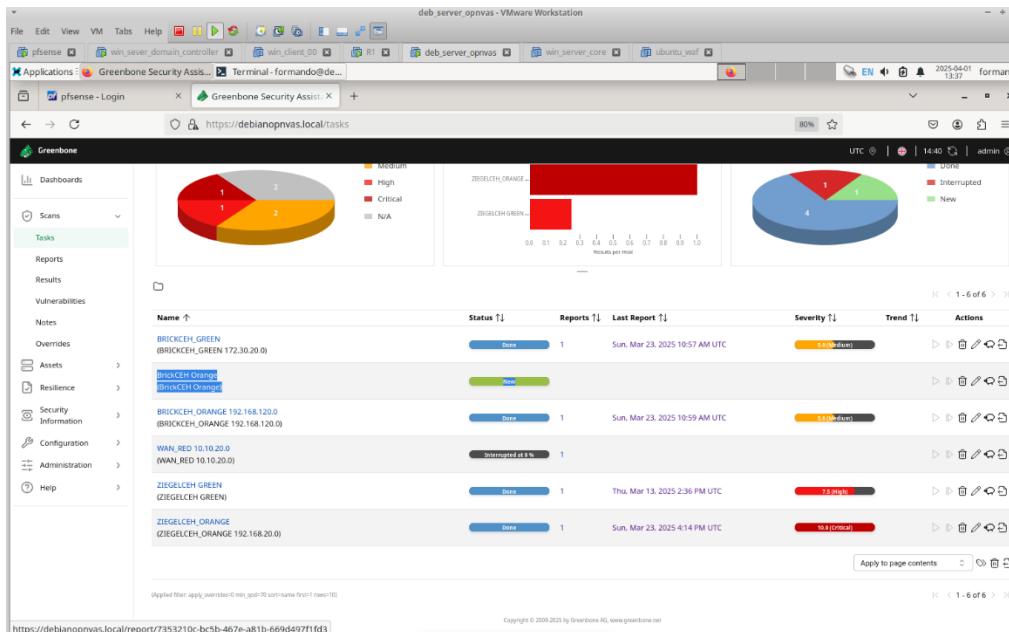
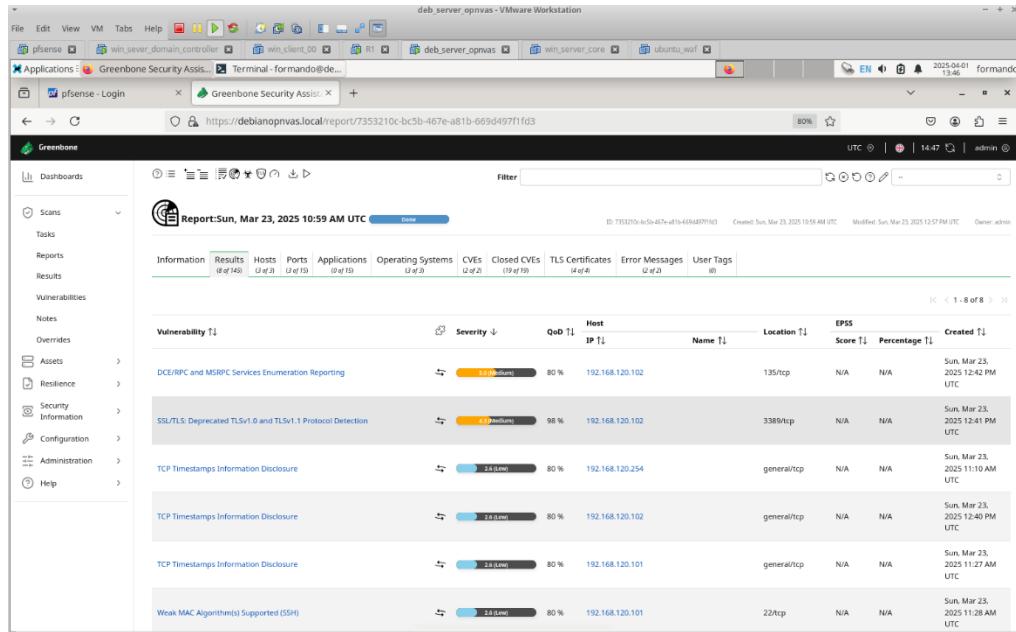


Imagen 61

Técnico Especialista Cibersegurança - CET93

- Após finalizar, informações sobre a rede



Vulnerability	Severity	Host IP	Name	Location	EPSS Score	Percentage	Created
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	192.168.120.102		135/tcp	N/A	N/A	Sun, Mar 23, 2025 12:42 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.9 (Medium)	192.168.120.102		3389/tcp	N/A	N/A	Sun, Mar 23, 2025 12:41 PM UTC
TCP Timestamps Information Disclosure	2.8 (Low)	192.168.120.254		general/tcp	N/A	N/A	Sun, Mar 23, 2025 11:10 AM UTC
TCP Timestamps Information Disclosure	2.8 (Low)	192.168.120.102		general/tcp	N/A	N/A	Sun, Mar 23, 2025 12:40 PM UTC
TCP Timestamps Information Disclosure	2.8 (Low)	192.168.120.101		general/tcp	N/A	N/A	Sun, Mar 23, 2025 11:27 AM UTC
Weak MAC Algorithm(s) Supported (SSH)	2.8 (Low)	192.168.120.101		22/tcp	N/A	N/A	Sun, Mar 23, 2025 11:28 AM UTC

Imagen 62

Técnico Especialista Cibersegurança - CET93

PfSense briceh

Snort

Instalar package snort:

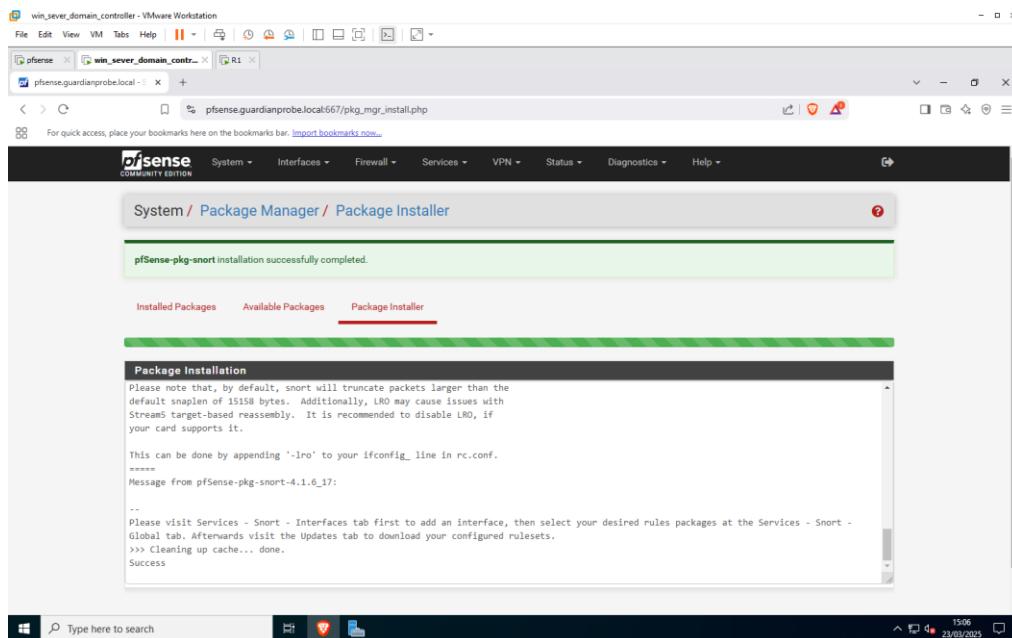


Imagen 63

Criar snort interface para wan:

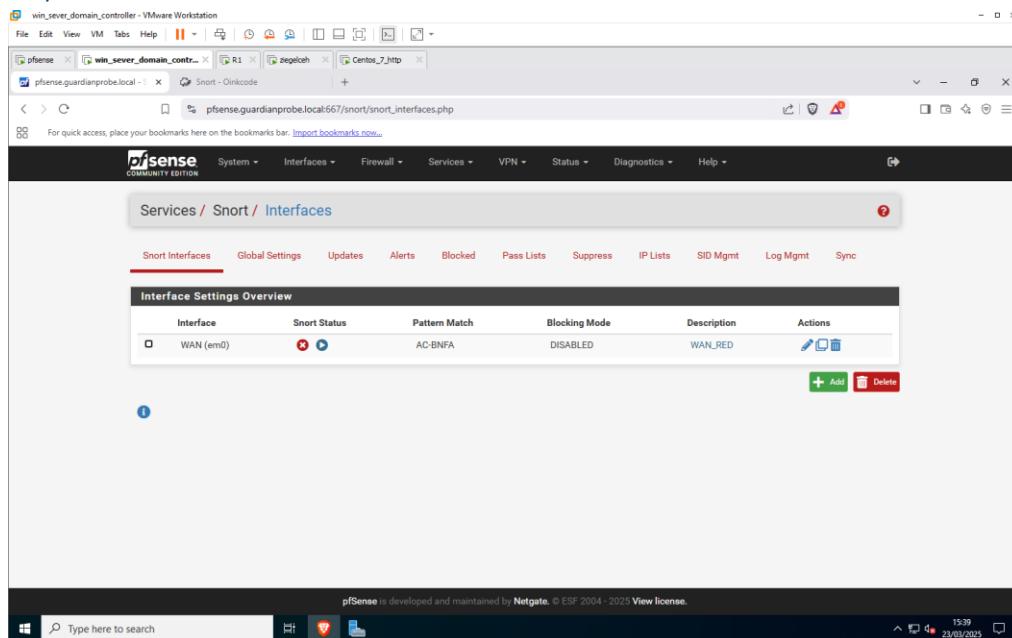


Imagen 64

Técnico Especialista Cibersegurança - CET93

Criar snort interface para LAN:

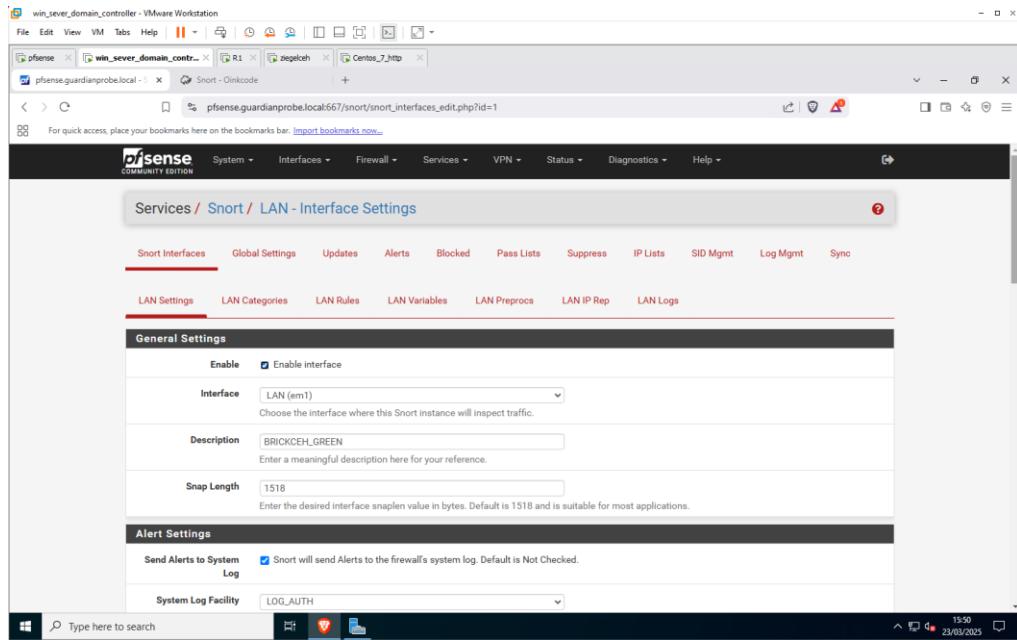


Imagen 65

Global setting ativar, registrar para ter snort code:

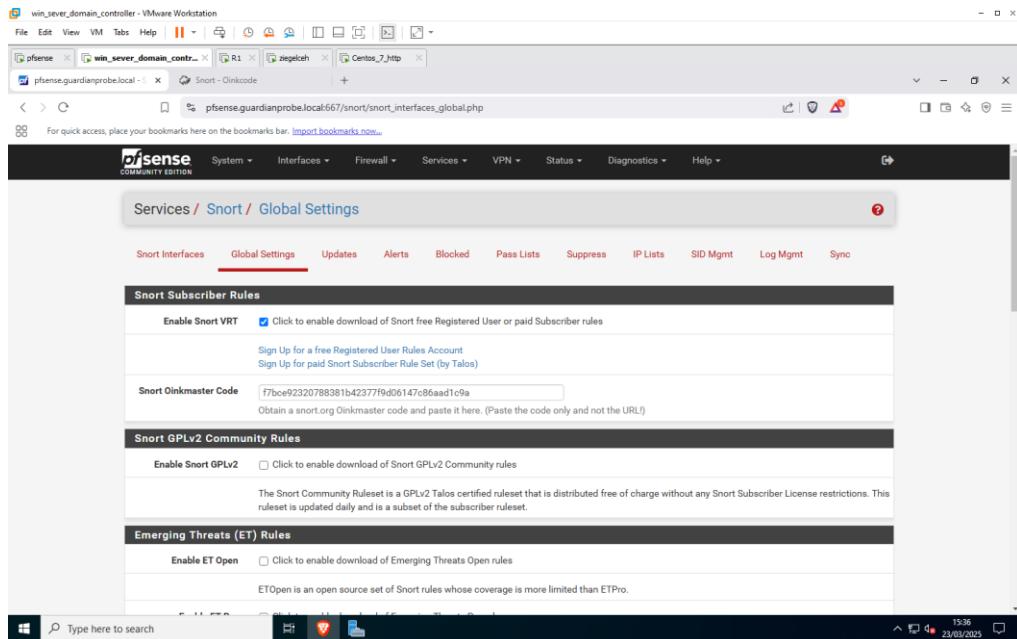


Imagen 66

Técnico Especialista Cibersegurança - CET93

Habilitar IPS Policy tanto para WAN como para a LAN:

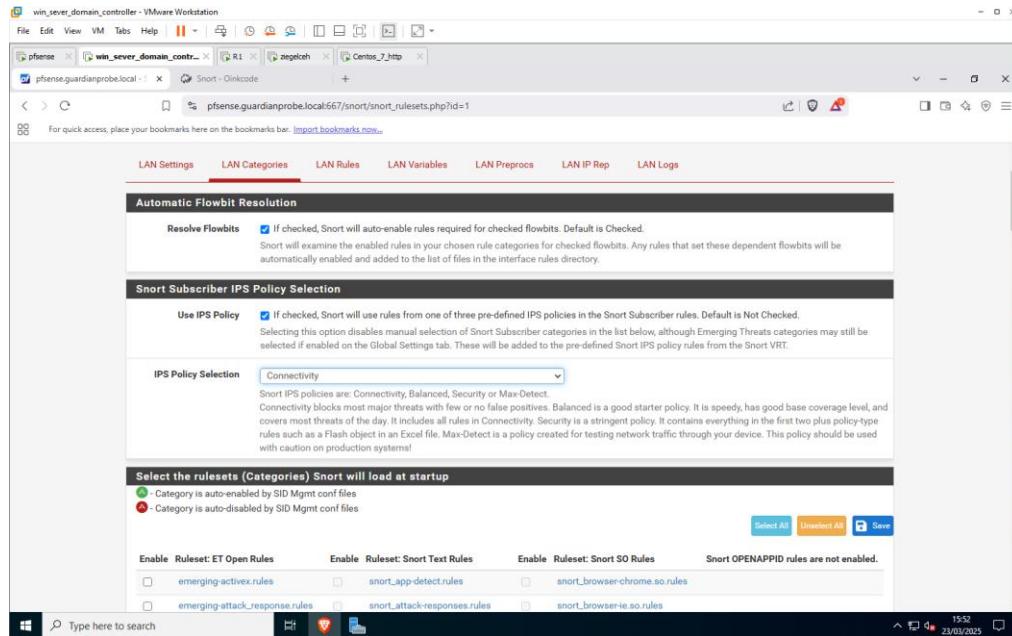


Imagen 67

Updates rules do Snort:

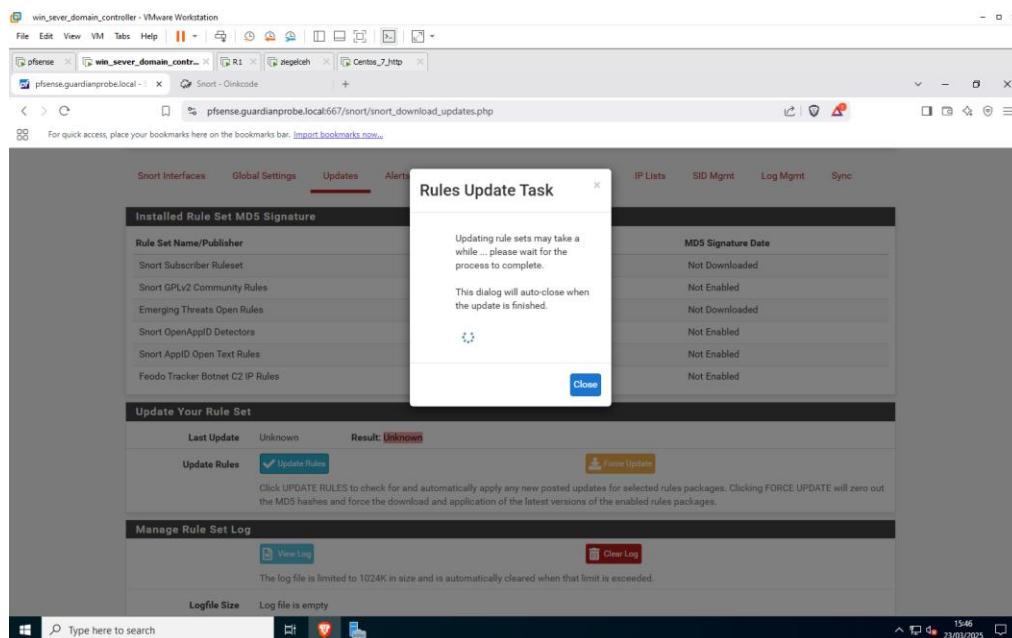
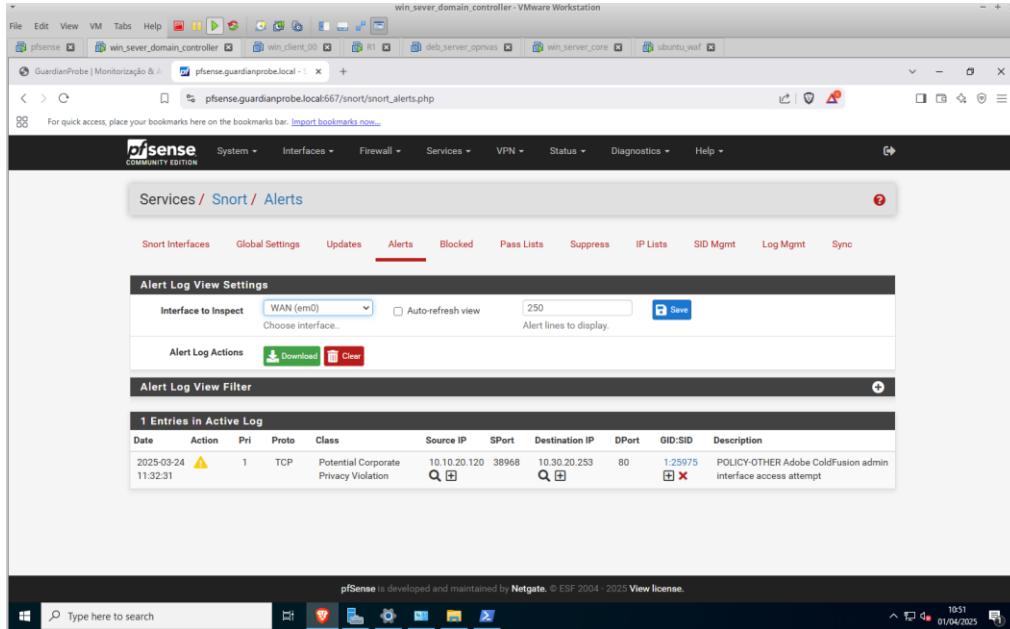


Imagen 68

Técnico Especialista Cibersegurança - CET93

Alertas:



The screenshot shows the pfSense Snort Alerts interface. The top navigation bar includes tabs for Snort Interfaces, Global Settings, Updates, **Alerts**, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. The main content area displays "Alert Log View Settings" with an interface dropdown set to "WAN (em0)" and an "Alert lines to display" input field set to 250. Below this is the "Alert Log Actions" section with "Download" and "Clear" buttons. The "Alert Log View Filter" section has a single entry: "1 Entries in Active Log". The log table has columns: Date, Action, Pri, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. The single entry is: "2025-03-24 11:32:31" (yellow warning icon), Action 1, TCP, Potential Corporate Privacy Violation, Source IP 10.10.20.120, SPort 38968, Destination IP 10.30.20.253, DPort 80, GID:SID 1:25975, Description POLICY-OTHER Adobe ColdFusion admin interface access attempt.

Imagen 69

Técnico Especialista Cibersegurança - CET93

ZenMap brickceh

Scan NMAP redes brickceh green e orange:

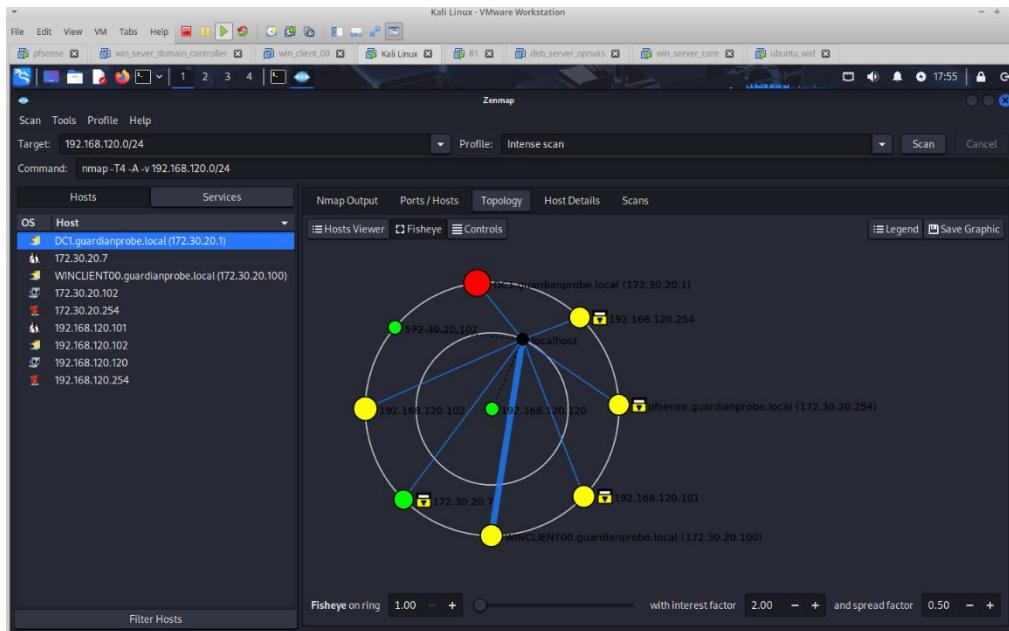


Imagen 70

Ports scan NMAP redes brickceh green e orange:

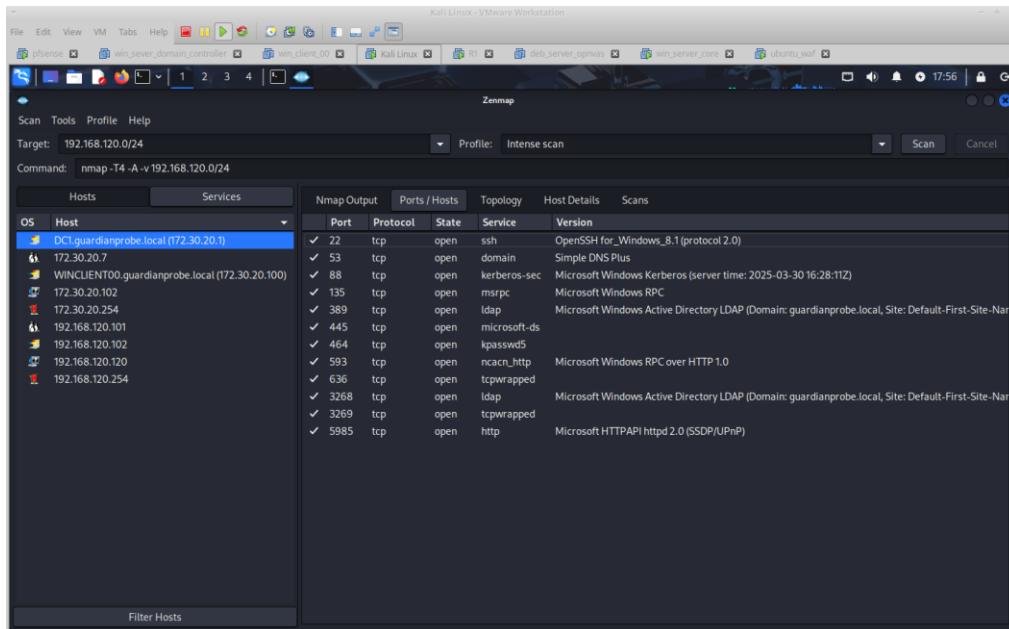


Imagen 71

ziegelceh

cockpit

Grafana, Wazuh

Foi instalado o cockpit:

```
apt -y install cockpit
systemctl enable cockpit.socket
ufw allow 9090
ufw reload
```

```
# Create the 'inet filter' table (if missing)
nft add table inet filter
# Create the 'input' chain (if missing)
nft add chain inet filter input { type filter hook input
priority 0\; policy accept\; }
```

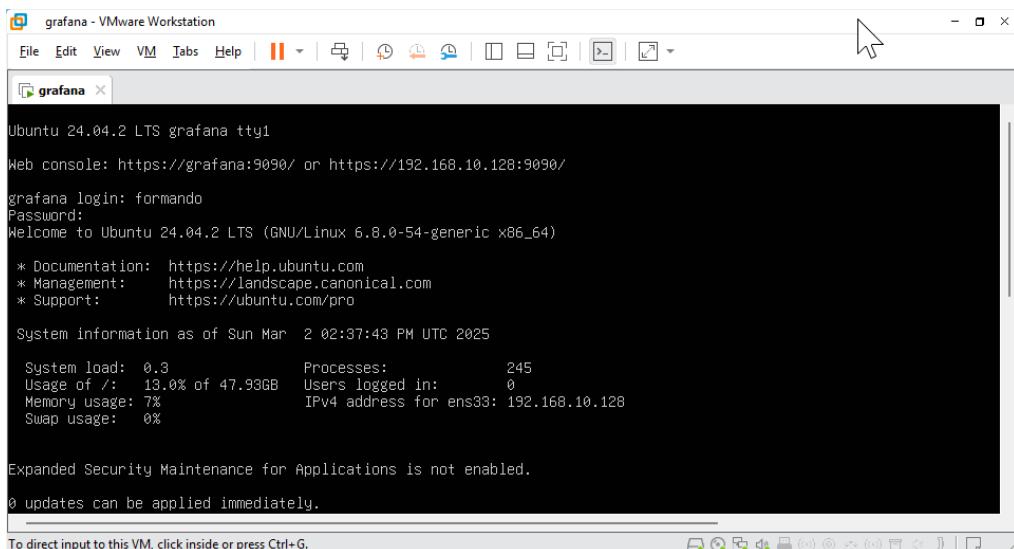


Imagen 72

Técnico Especialista Cibersegurança - CET93

VPN IPSec

Para estabelecer uma VPN IPSec, efetuamos as seguintes configurações:

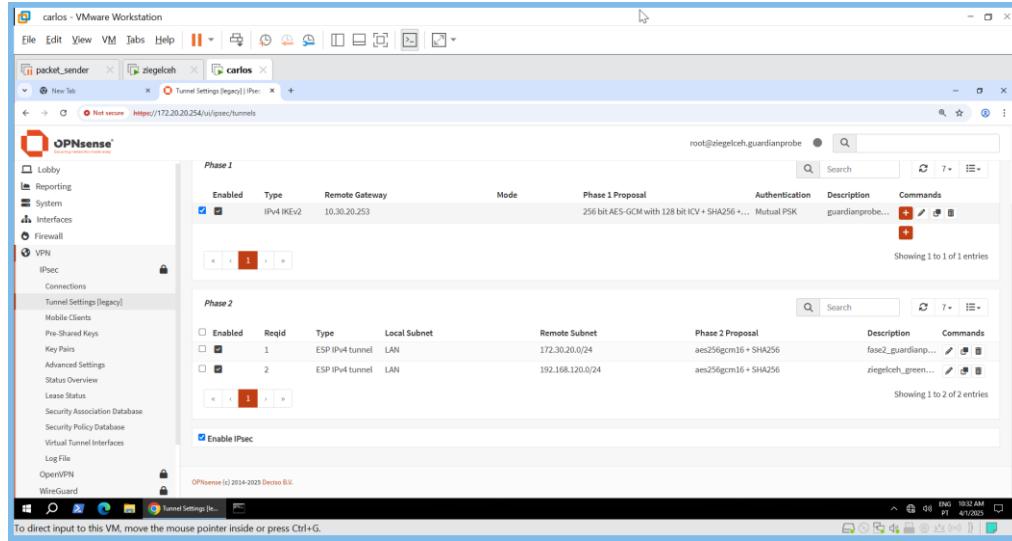


Imagen 73

Em VPN \ IPSec \ Tunnel Settings, criamos a fase 1:

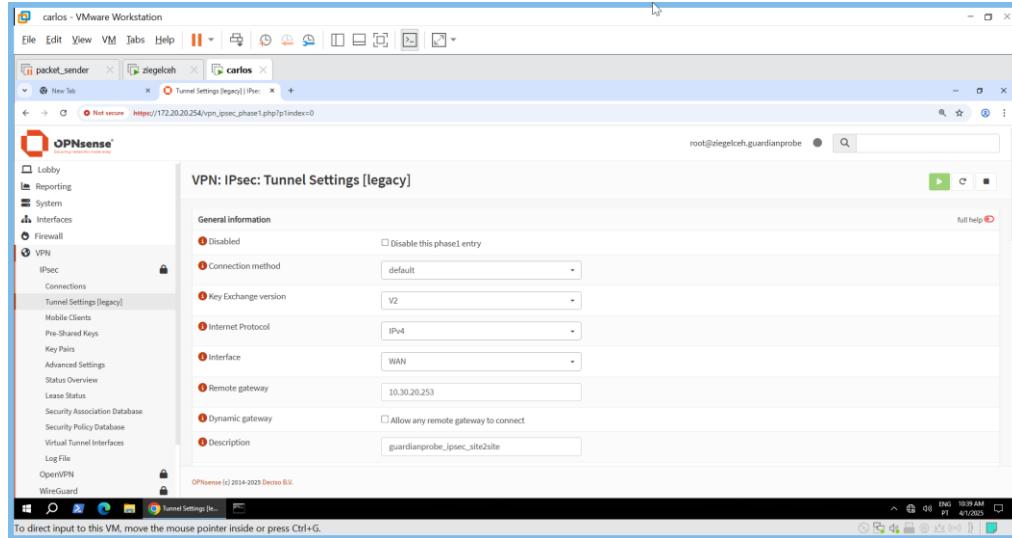


Imagen 74

Técnico Especialista Cibersegurança - CET93

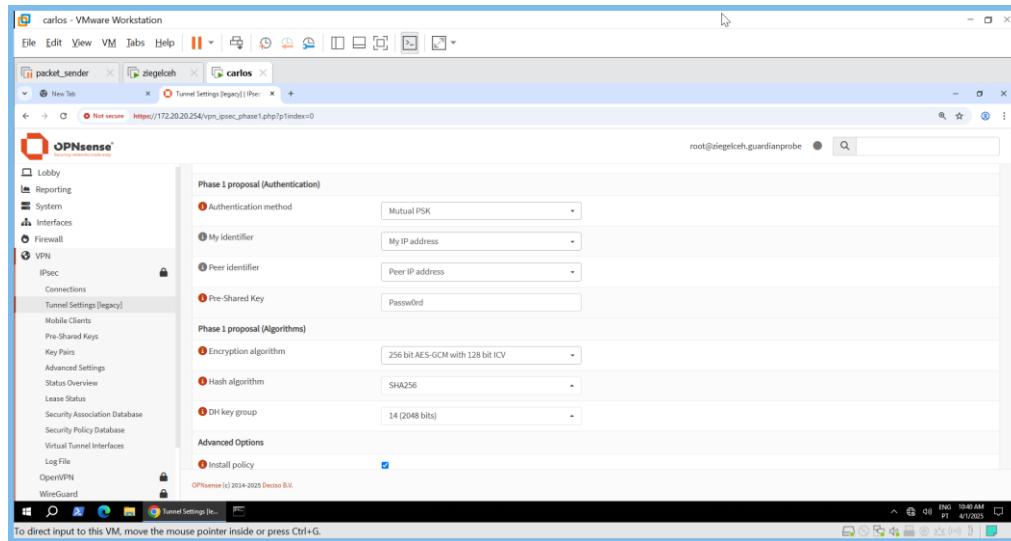


Imagen 75

Depois criamos 2 fases 2, uma para a zona Green e outra para a zona Orange:

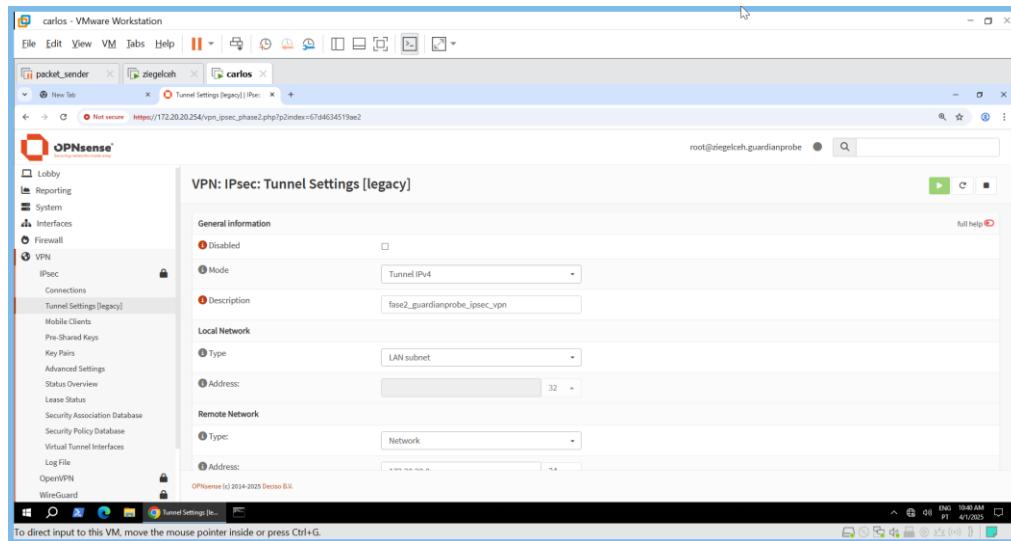


Imagen 76

Técnico Especialista Cibersegurança - CET93

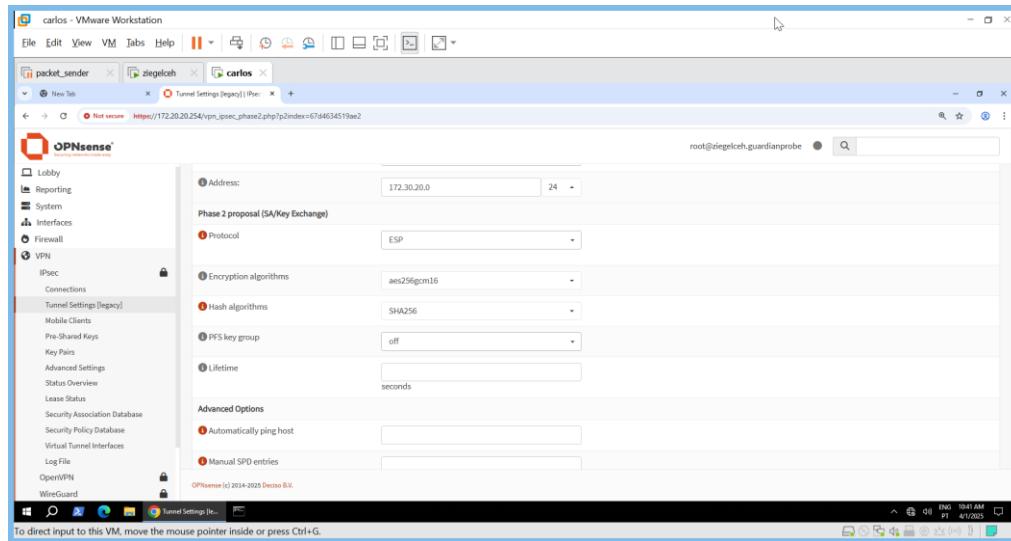


Imagen 77

Técnico Especialista Cibersegurança - CET93

OpenVPN RoadWarrior

Para um PC aceder remotamente, criamos um servidor OpenVPN:

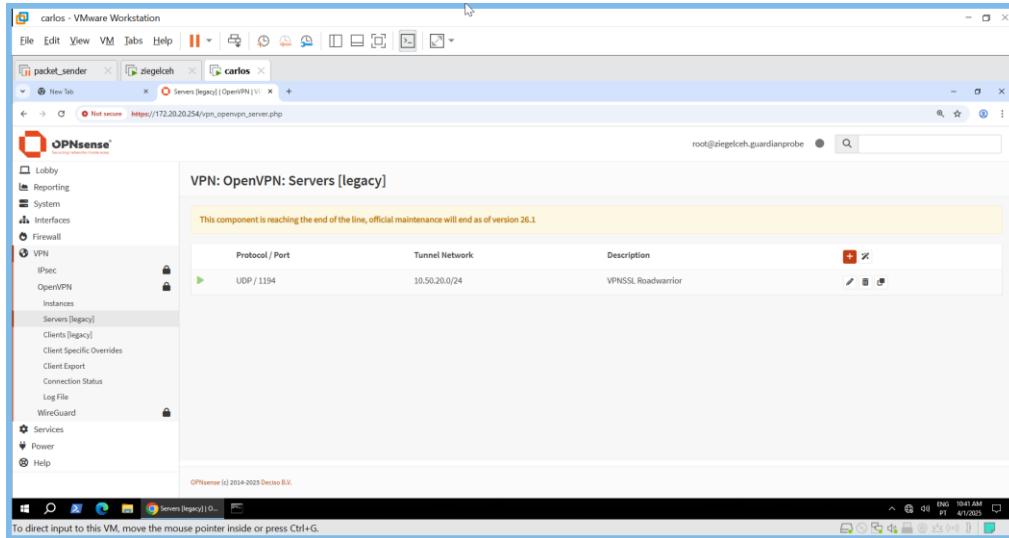


Imagen 78

Com as seguintes configurações:

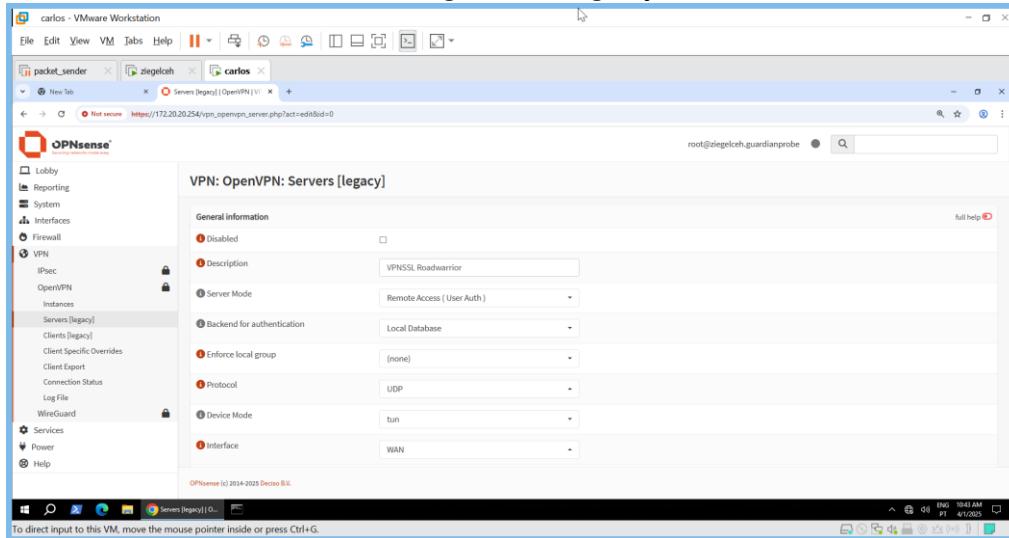


Imagen 79

Técnico Especialista Cibersegurança - CET93

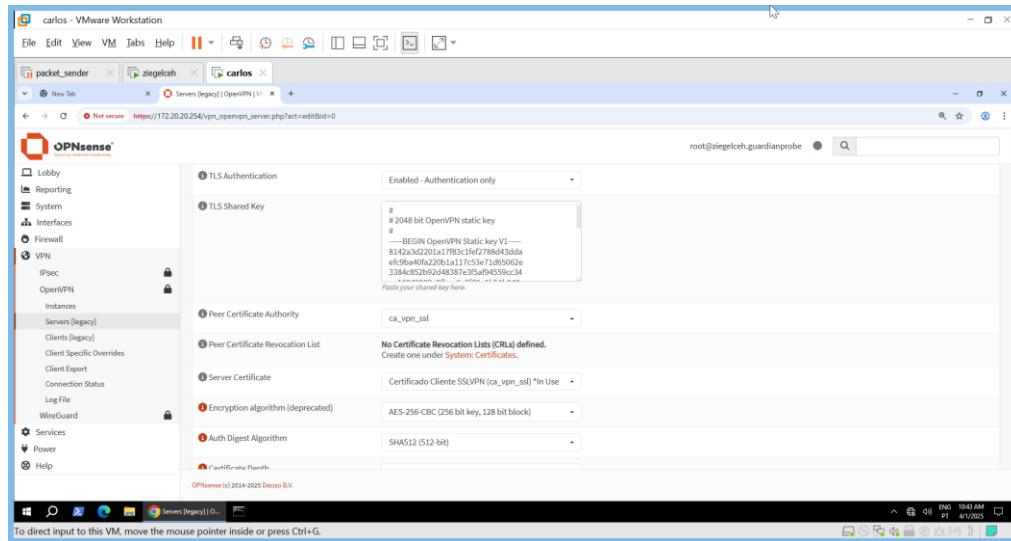


Imagen 80

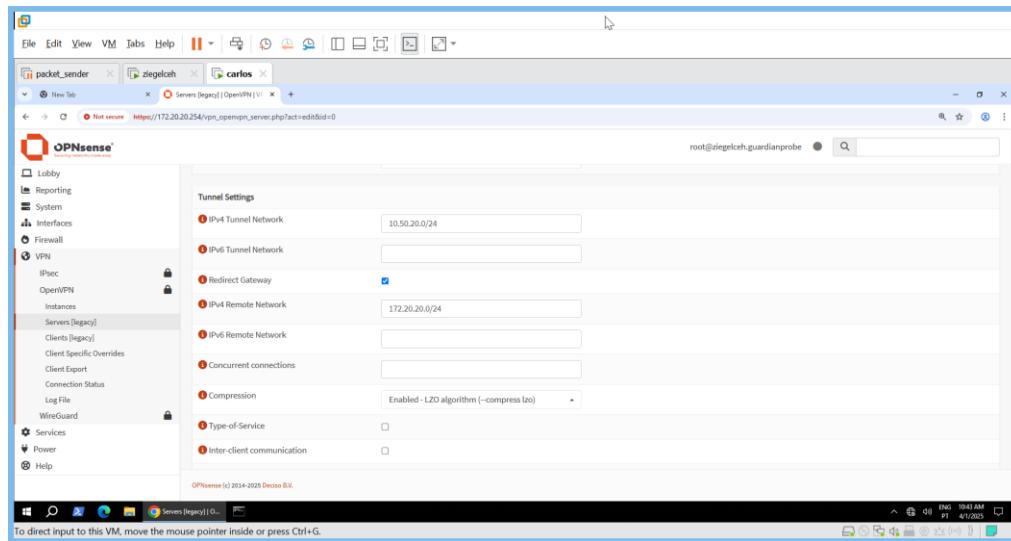


Imagen 81

Técnico Especialista Cibersegurança - CET93

Confirmar que foi criada uma regra que permite o tráfego da VPN na porta UDP\1194:

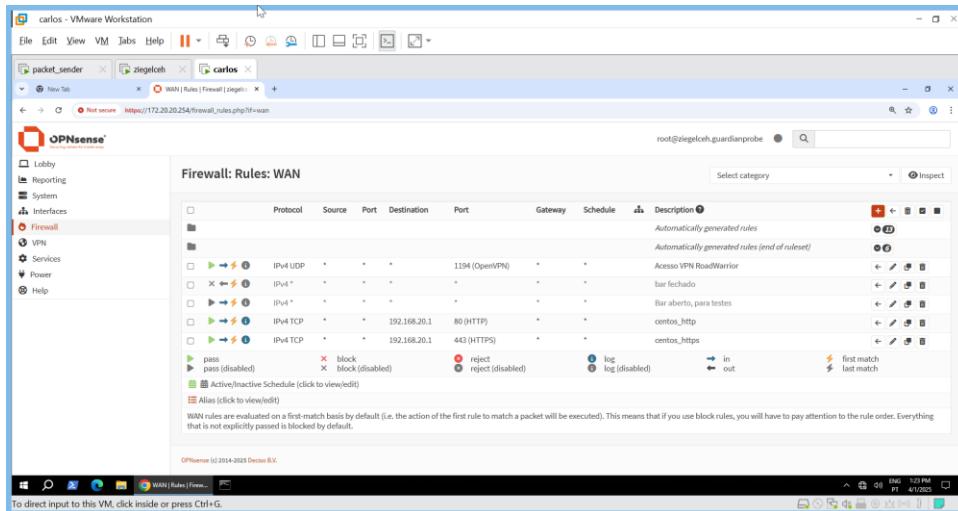


Imagen 82

Configuração VPN SSL RoadWarrior cliente

Ir s VPN > Client Export, e alterar as seguintes definições:

```

Remote Access Server: VPNSSL RoadWarrior
Export Type: Archive
Hostname: <IP da interface WAN da Firewall> 10.20.20.253
Port: Deixar a default
Use random port: Check
Validate server object: Check
Windows Certificate System Store: Check

```

Fazer export da configuração, em que será feito a transferência de um arquivo, que depois irá ser entregue ao computador cliente.

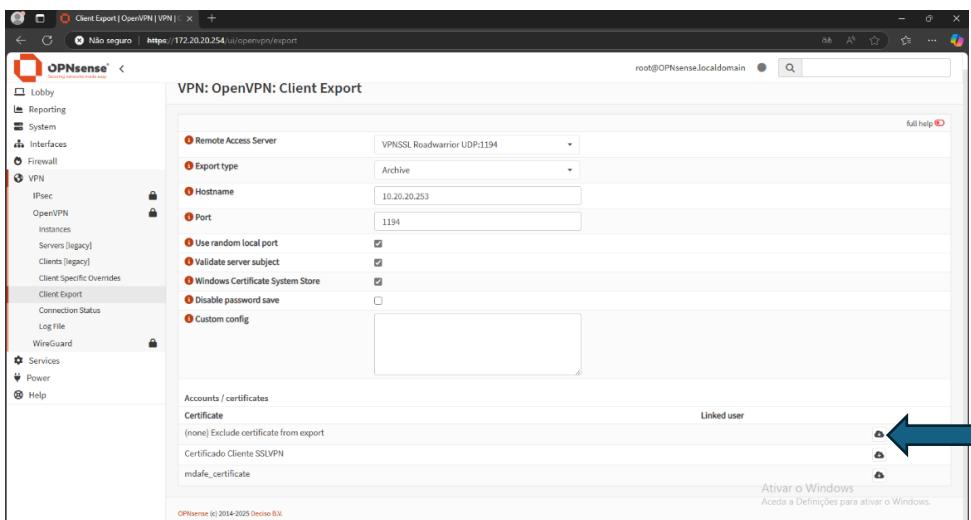


Imagen 7

Técnico Especialista Cibersegurança - CET93

Depois de transferido o ficheiro para o computador cliente, extrair e colocar a pasta com os conteúdos na seguinte localização:

C:\Program Files\OpenVPN\config

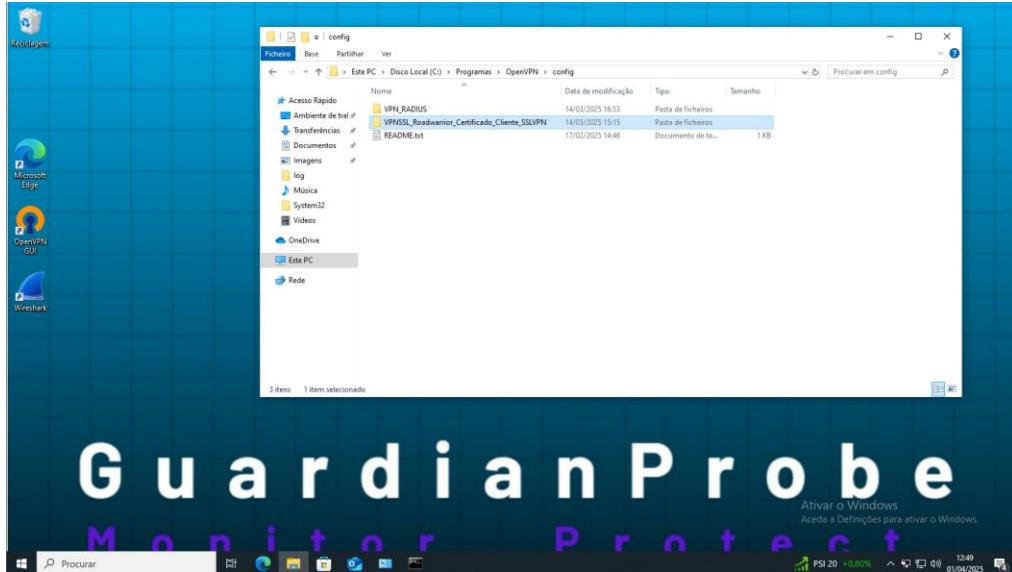


Imagen 8

De seguida clicar com o lado direito no ícone do OpenVPN, selecionar a VPN adicionada e em Conectar.

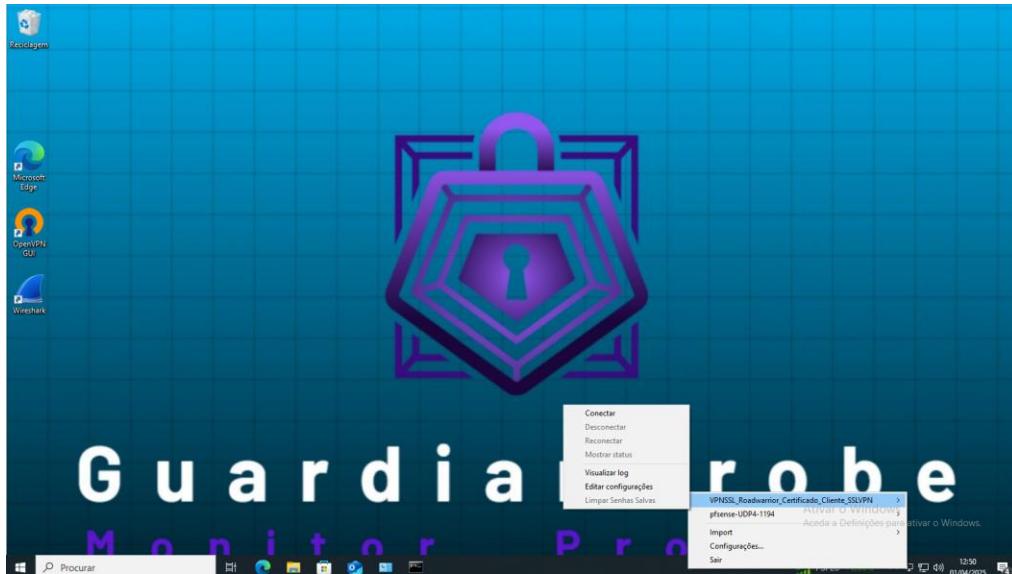


Imagen 9

Irá ser apresentado uma janela para adicionar as credenciais criadas na OPNsense.

Técnico Especialista Cibersegurança - CET93



Imagen 10

Verificamos que a conexão foi realizada com sucesso

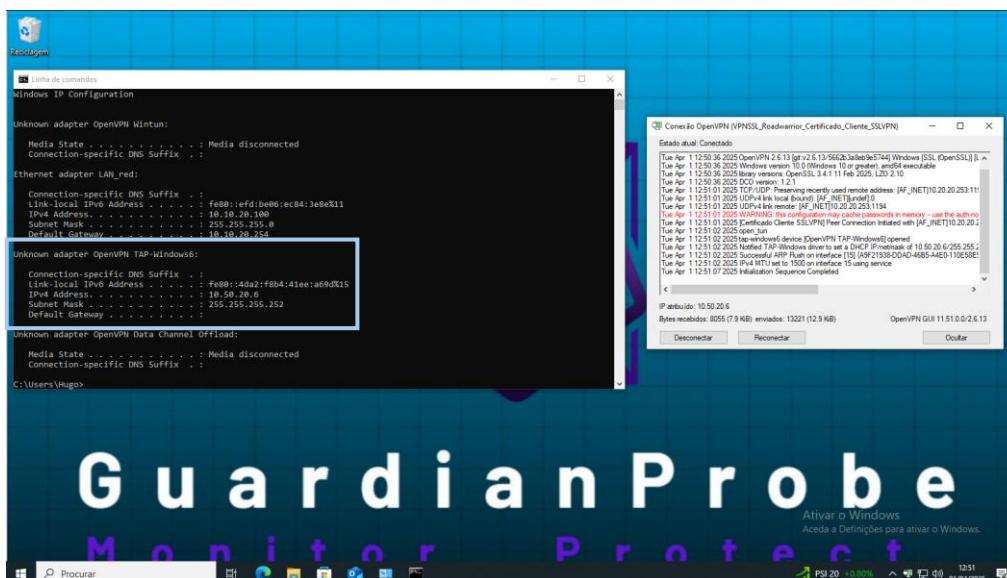


Imagen 11

Técnico Especialista Cibersegurança - CET93

Wazuh Server

Comando para instalação do wazuh. Este processo irá demorar pois irá ser instalado todas as dependências e componentes para o funcionamento e também utilização da dashboard:

```
curl -s0 https://packages.wazuh.com/4.11/wazuh-install.sh &&
sudo bash ./wazuh-install.sh -a
```

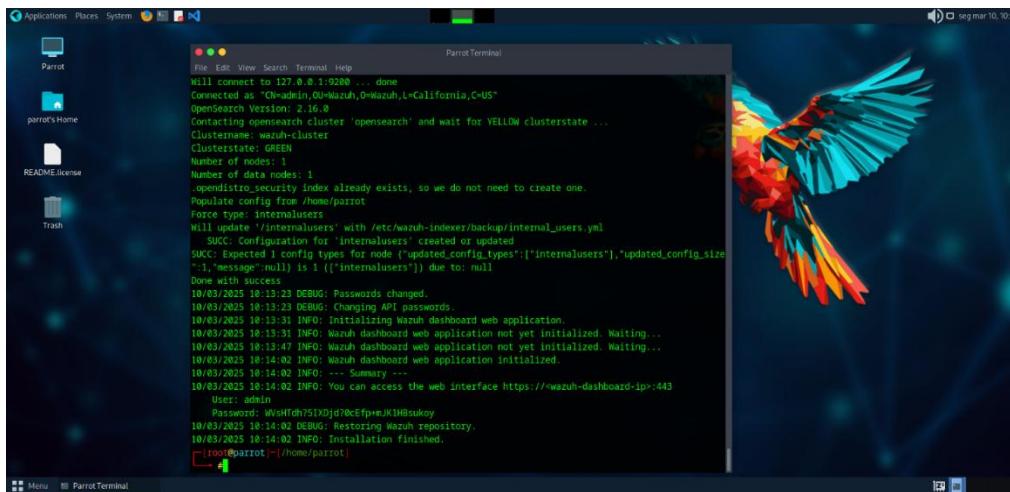


Imagen 83

Depois de instalado, guardar as credenciais apresentadas, abrir um browser e aceder a Dashboard pelo URL <IP da máquina>:443. Irá ser apresentado um aviso de falha de certificado. Clicar em ‘Advanced’ e em ‘Accept the Risk and Continue’.

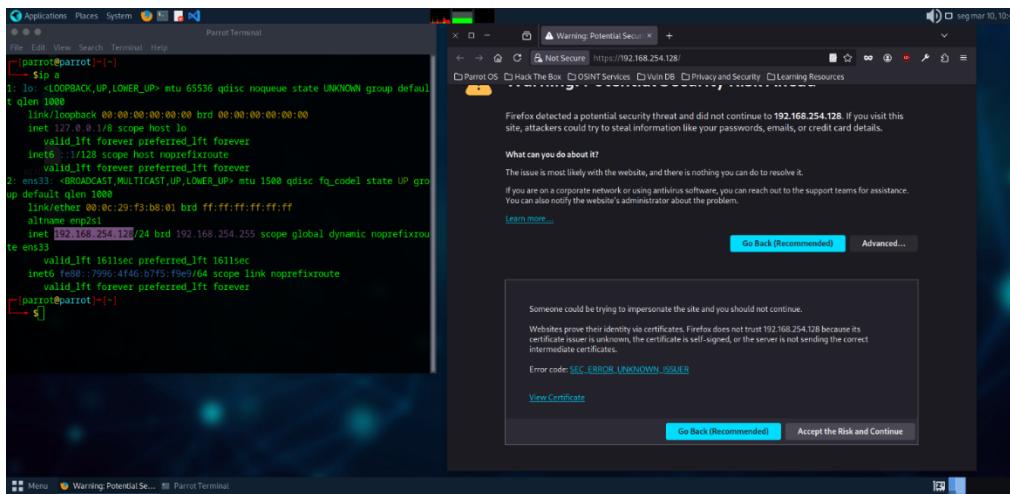


Imagen 84

De seguida irá ser apresentado a página de login. Inserir as credenciais guardadas.

Técnico Especialista Cibersegurança - CET93

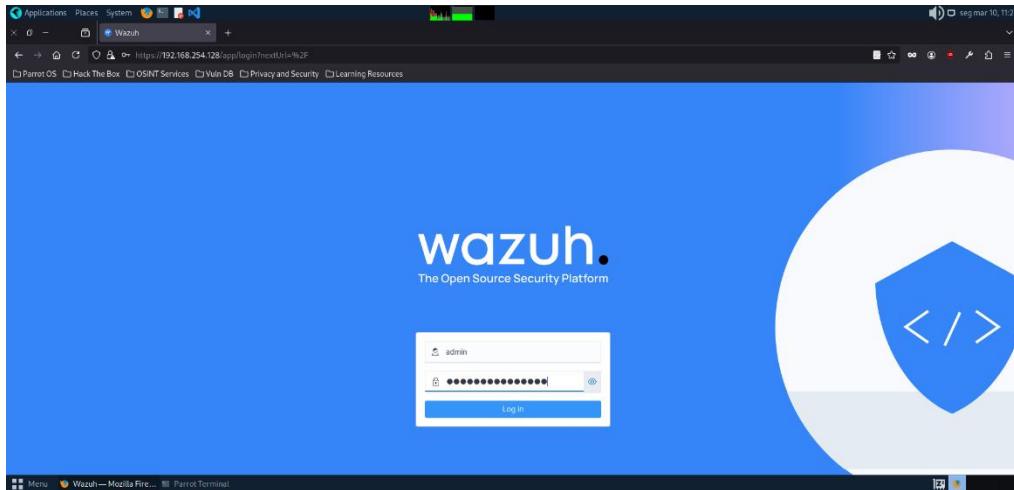


Imagen 85

Depois de acedido com sucesso, irá ser apresentado a dashboard principal do wazuh.

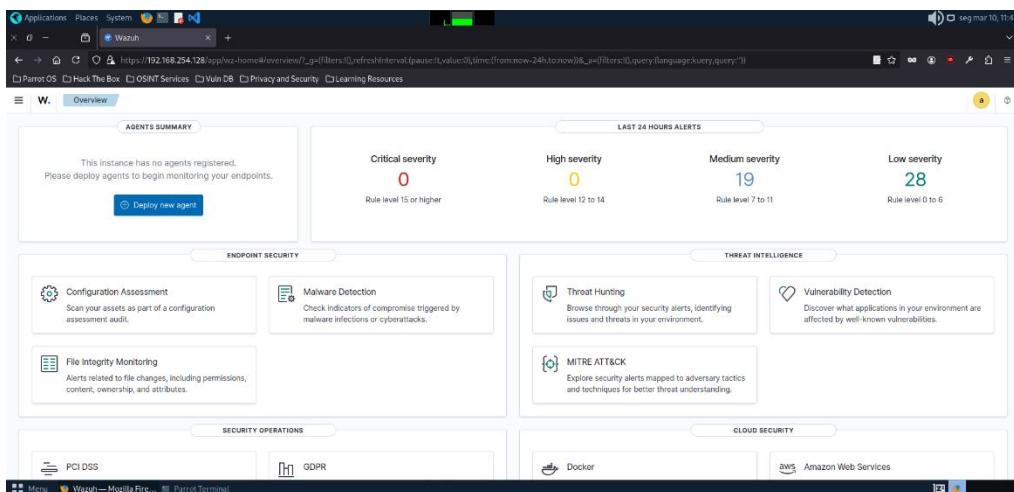
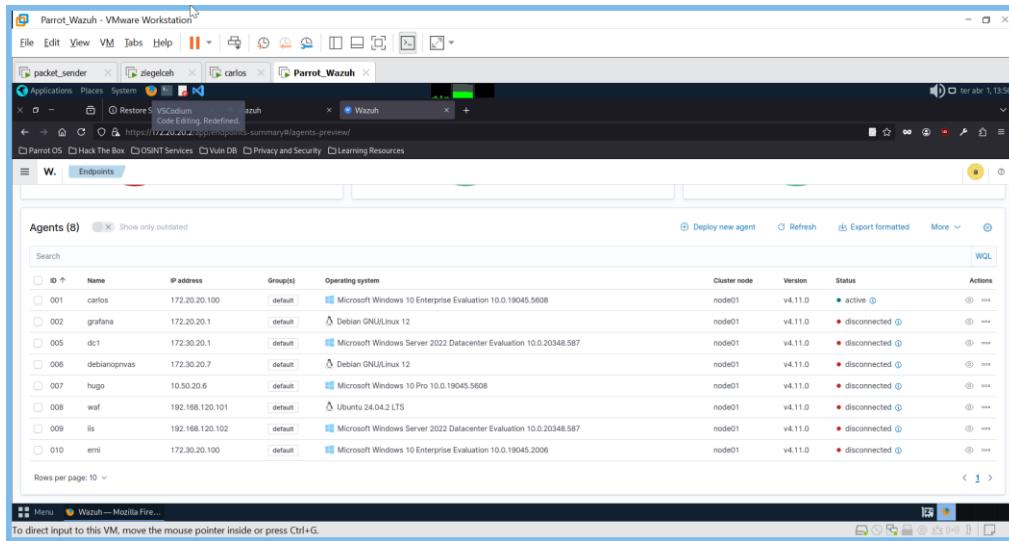


Imagen 86

Técnico Especialista Cibersegurança - CET93

Resumo dos EndPoints



ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	carlos	172.20.20.100	default	Microsoft Windows 10 Enterprise Evaluation 10.0.19045.5608	node01	v4.11.0	● active	
002	grafana	172.20.20.1	default	Debian GNU/Linux 12	node01	v4.11.0	● disconnected	
005	dc1	172.30.20.1	default	Microsoft Windows Server 2022 Datacenter Evaluation 10.0.20348.587	node01	v4.11.0	● disconnected	
006	debianopnvas	172.30.20.7	default	Debian GNU/Linux 12	node01	v4.11.0	● disconnected	
007	hugo	10.50.20.6	default	Microsoft Windows 10 Pro 10.0.19045.5608	node01	v4.11.0	● disconnected	
008	waf	192.168.120.101	default	Ubuntu 24.04.2 LTS	node01	v4.11.0	● disconnected	
009	lls	192.168.120.102	default	Microsoft Windows Server 2022 Datacenter Evaluation 10.0.20348.587	node01	v4.11.0	● disconnected	
010	erni	172.30.20.100	default	Microsoft Windows 10 Enterprise Evaluation 10.0.19045.2096	node01	v4.11.0	● disconnected	

Imagen 87

Técnico Especialista Cibersegurança - CET93

Wazuh Agent

Acedemos ao site do Wazuh: <https://172.20.20.2/>

E em

Agents Management \ Summary

Selecionamos o respetivo sistema operativo, definimos o nome do agente, que poderá ser o nome do host que vai receber o agente:

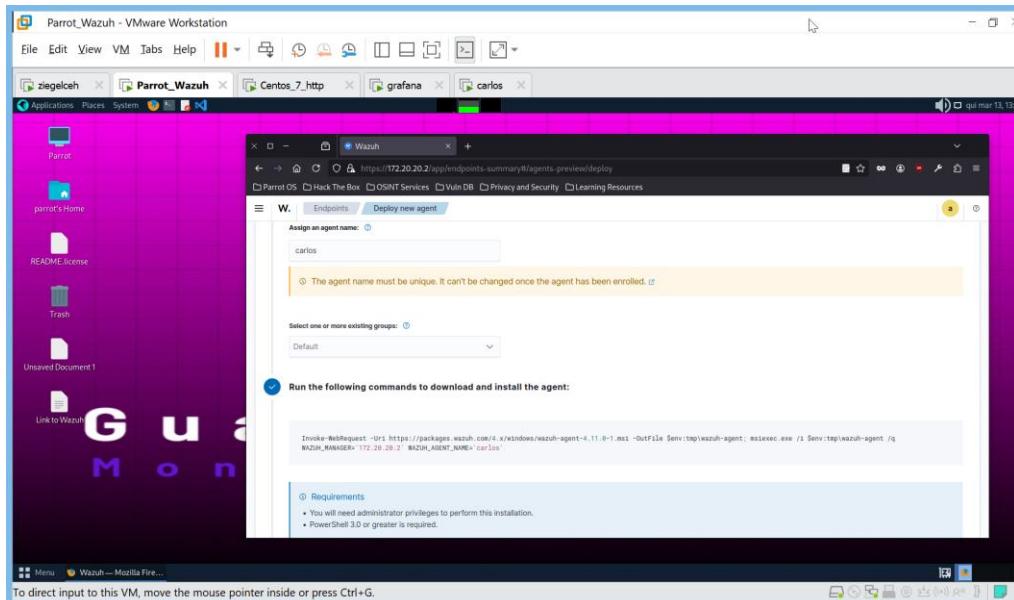


Imagen 88

Copiamos o comando e executamos no host:

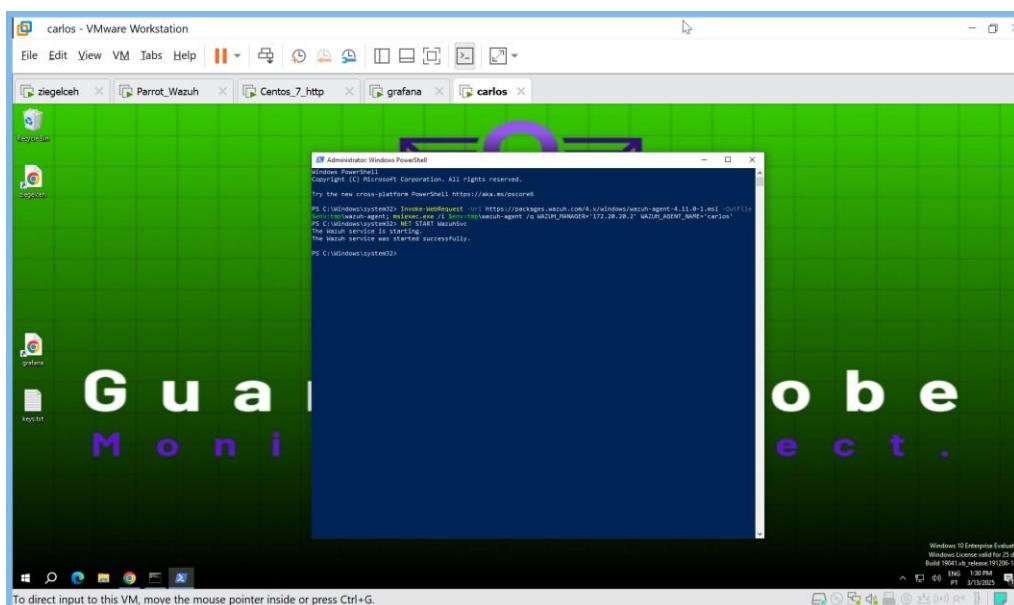


Imagen 89

Syslog-ng Server

Instalar o servidor do SysLog-NG:

```
apt install syslog-ng
nano /etc/syslog-ng/syslog-ng.conf
```

```
# Define a source for network logs (UDP)
source s_network {
    udp(ip(0.0.0.0) port(514));  # Listen on UDP port 514
    tcp(ip(0.0.0.0) port(514));  # Optional: Also listen on TCP
};

# Destination: Logs split by source IP
destination d_per_ip {
    file(
        "/var/log/syslog-ng/${SOURCEIP}.log"  # Use ${SOURCEIP} macro directly
        create_dirs(yes)  # Auto-create directories
    );
};
# Log path (connect source to destination)
log {
    source(s_network);
    destination(d_syslog);
};
```

```
nano /etc/syslog-ng/conf.d/*.conf
mkdir -p /var/log/syslog-ng
useradd -r -s /usr/sbin/nologin -g adm syslog
chown -R syslog:adm /var/log/syslog-ng
chmod 755 /var/log/syslog-ng
getcap $(which syslog-ng)
setcap 'cap_net_bind_service,cap_net_admin,cap_syslog+ep' \
$(which syslog-ng)
chown -R syslog:adm /var/log
chmod -R 755 /var/log
syslog-ng --syntax-only

sudo chown -R syslog:adm /var/log/syslog-ng
sudo chmod 755 /var/log/syslog-ng
```

Técnico Especialista Cibersegurança - CET93

Configurar o serviço do syslog-ng para usar o utilizador syslog:

```
systemctl edit syslog-ng
```

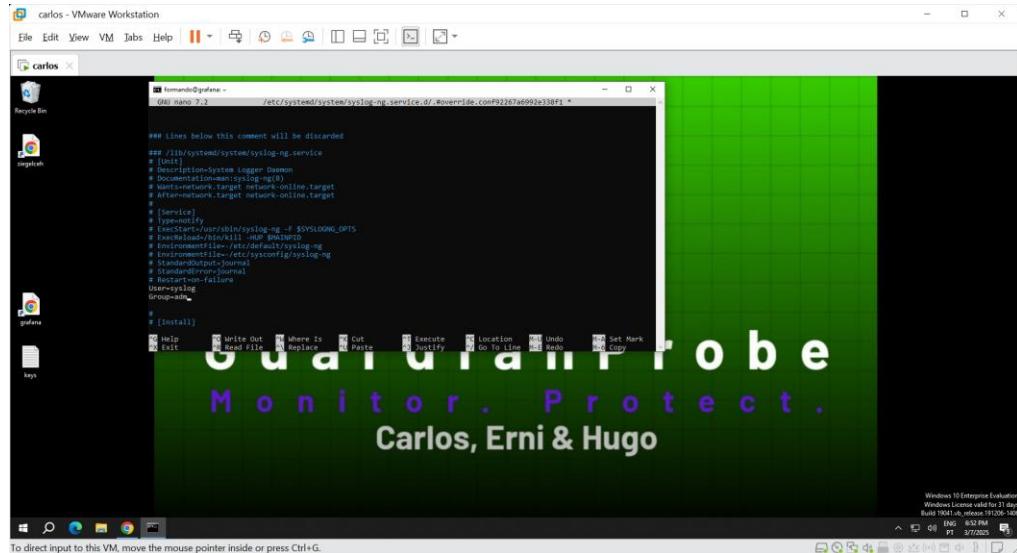


Imagen 90

```
systemctl daemon-reload
sudo systemctl restart syslog-ng
sudo systemctl status syslog-ng
journalctl -u syslog-ng --since "1 hour ago"
sudo iptables -A INPUT -p udp --dport 514 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 514 -j ACCEPT
sudo iptables-save | sudo tee /etc/iptables/rules.v4
sudo iptables -L -n
```

Syslog-ng Local Log

No caso do próprio grafana, temos que reencaminhar localmente os próprios logs para o respetivos ficheiros:

```
nano /etc/syslog-ng/syslog-ng.conf
```

```
# Define the log directory
destination d_remote_logs {
    file("/var/log/remote/${HOST}.log");
};

# Filter for local logs
filter f_local { host("$HOST"); };

# Destination for local logs
destination d_local_log {
    file("/var/log/remote/$HOST.log");
};

# Source for local logs (system logs)
source s_local {
    system();
};

# Apply logging rules
log { source(s_local); filter(f_local); destination(d_local_log); };
```

```
systemctl restart syslog-ng
```

Syslog-ng Client

Editar o ficheiro de configuração:

```
sudo apt update
sudo apt install syslog-ng
sudo nano /etc/syslog-ng/syslog-ng.conf
```

```
destination d_remote {
    tcp("172.20.20.1" port(514));
};

log { source(s_src); destination(d_remote); };
```

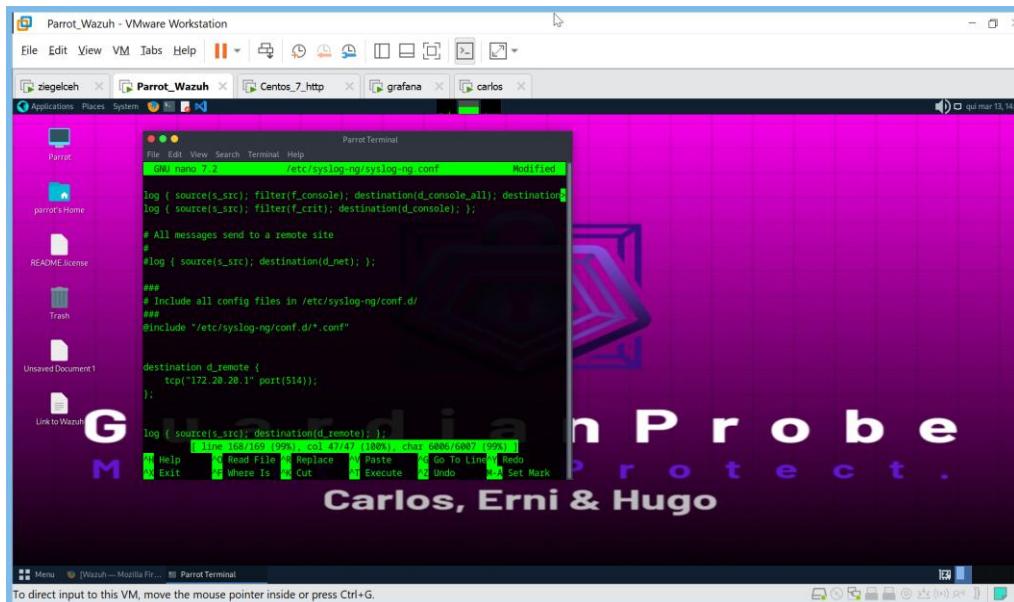


Imagen 91

```
systemctl enable syslog-ng
systemctl restart syslog-ng
```

Syslog-*ng* a partir da OpenSense

Em

System \ Settings \ Logging

Definimos o servidor remoto que vai receber os logs.

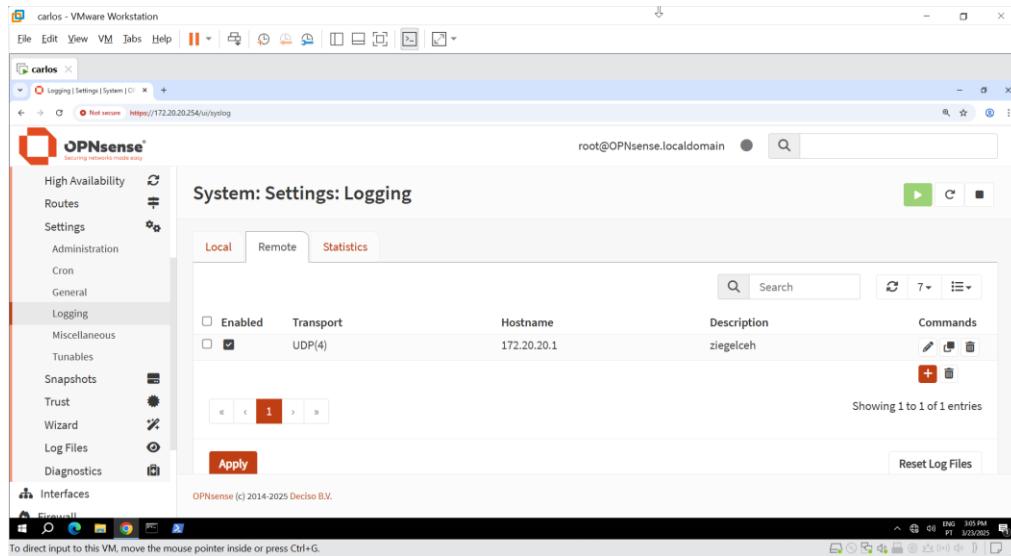


Imagen 92

Syslog-ng do Apache2

Para que o Apache Server reencaminhe os logs, necessitamos de efetuar as seguintes alterações:

```
nano /etc/apache2/sites-enabled/000-default.conf
```

```
CustomLog "|/usr/bin/logger -t apache_access -p local1.info" combined
ErrorLog "|/usr/bin/logger -t apache_error -p local1.err"
```

```
CustomLog "/tmp/apache_access.log" "%h %l %u %t \"%r\" %>s %b"
```

```
systemctl restart apache2
```

Alterar também o ficheiro syslog-ng.conf:

```
nano /etc/syslog-ng/syslog-ng.conf
```

```
source s_local1 {
    unix-stream("/dev/log");
};

filter f_apache { facility(local1); };

log {
    source(s_local1);
    filter(f_apache);
    destination(d_remote);
};
```

```
systemctl restart syslog-ng
```

Syslog-ng do wazuh

Para reencaminharmos os logs do Wazuh:

```
sudo nano /var/ossec/etc/ossec.conf
```

```
<ossec_config>
  <integration>
    <name>custom-syslog</name>
    <hook_url>tcp://172.20.20.1:514</hook_url>
    <rule_id>all</rule_id>
  </integration>
</ossec_config>
```

```
systemctl restart wazuh-manager
```

Syslog-ng, testes

Para testar manualmente se os logs estão a ser recebidos pelo servidor podemos gerar uma entrada no log:

```
logger -n 172.20.20.1 -p 514 -T "Remote syslog test event"
```

Syslog-*ng* no Cisco

Para ativar o encaminhamento de logs a partir dos switches Cisco:

```
logging trap debugging
logging source-interface Vlan93
logging host 172.20.20.1 transport tcp port 514
```

para o router, usamos a seguinte configuração:

```
conf t
logging host 172.20.20.1 transport tcp port 514
logging trap informational
logging host 172.20.20.1 transport udp port 514
logging trap debugging
logging on
exit
```

Técnico Especialista Cibersegurança - CET93

Syslog-ng, no Windows (NXLog)

Depois de instalar: <https://nxlog.co/products/nxlog-community-edition>, adicionar as seguintes linhas ao ficheiro:

C:\Program Files\NXLog\conf

```
# Input: Collect Windows Event Log
<Input eventlog>
    Module im_msvistalog
</Input>

# Output: Forward to syslog-ng server (UDP)
<Output syslog_out>
    Module om_udp
    Host 172.20.20.1
    Port 514
    Exec \
        # Map Windows Event Log fields to syslog format \
        $Message = "EventID=" + $EventID + " " + $Message; \
        $Hostname = hostname(); \
        $Severity = "INFO"; # Adjust based on $Level if needed \
        to_syslog_bsd();
</Output>

# Define the log routing
<Route eventlog_to_syslog>
    Path eventlog => syslog_out
</Route>
```

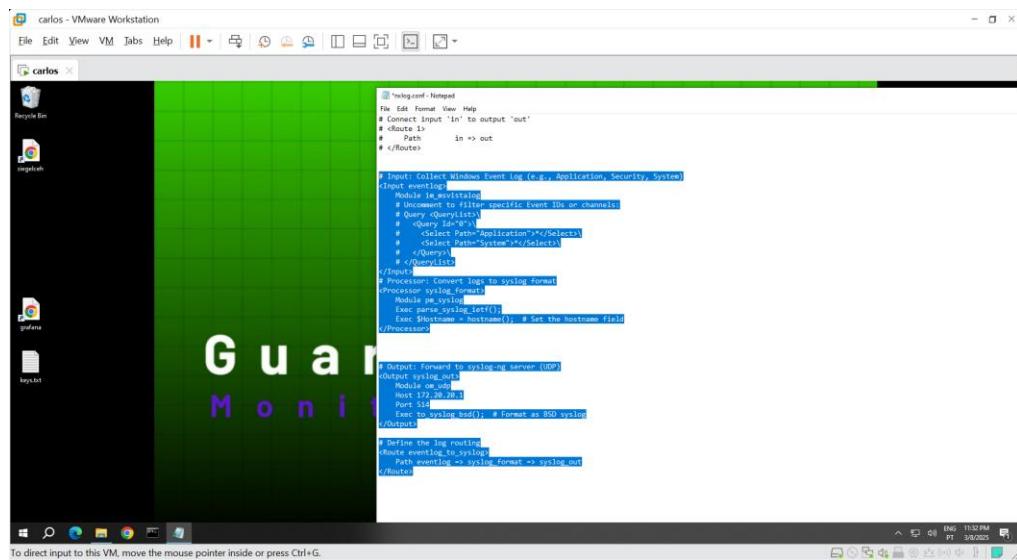


Imagen 93

Técnico Especialista Cibersegurança - CET93

Reiniciar os serviços:

```
net stop nxlog
net start nxlog
```

Podemos verificar se localmente os logs estão a ser produzidos:

```
dir C:\Program Files\nxlog\data\nxlog.log
```

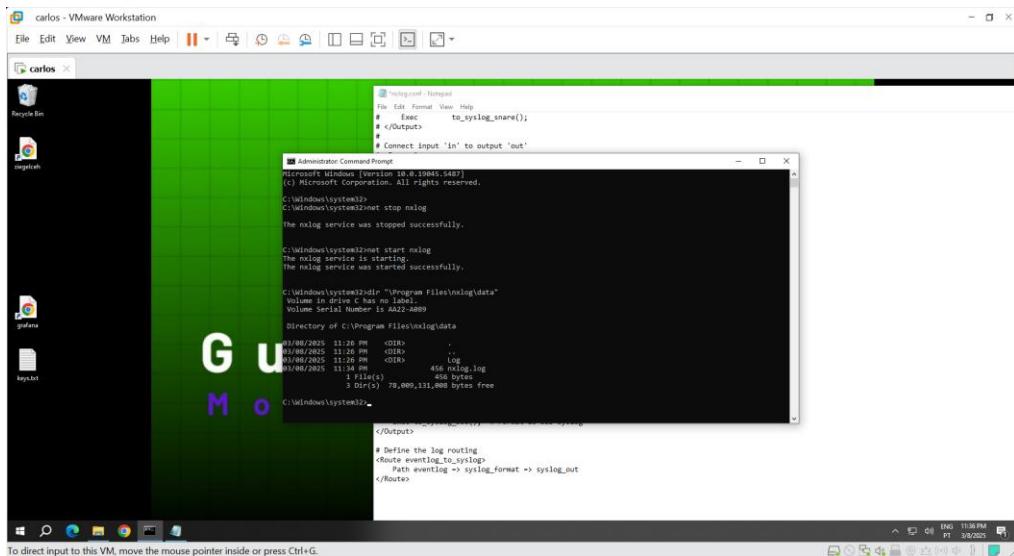


Imagen 94

Técnico Especialista Cibersegurança - CET93

Syslog-*ng* da firewall

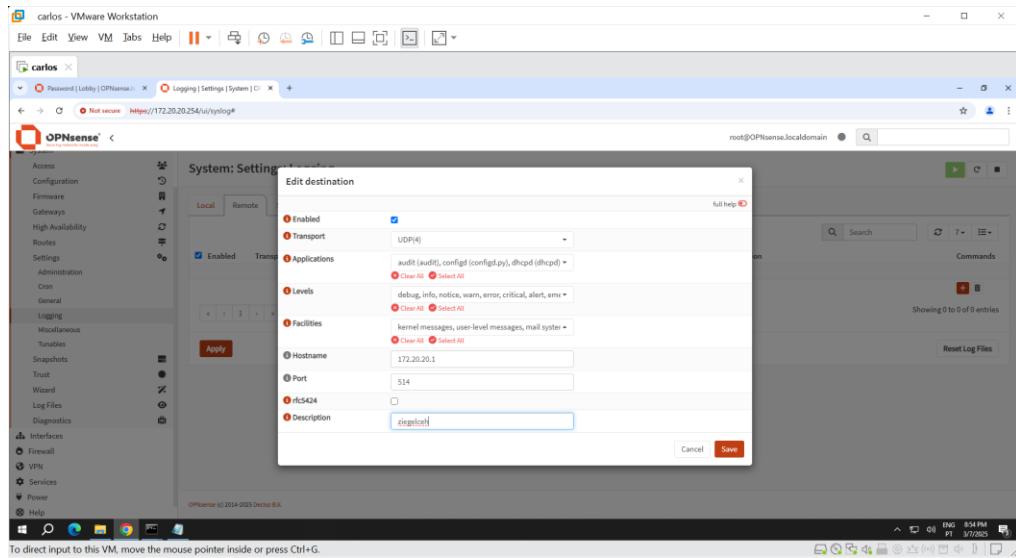


Imagen 95

Promtail, Configuração

Vamos agora configurar o Promtail para ler os logs que estão a ser reencaminhados para o servidor.

```
nano /etc/promtail/config.yml
```

```
server:
  http_listen_port: 9080  # Promtail HTTP server port (for metrics and health
  checks)
  grpc_listen_port: 0      # Disable gRPC (can be omitted if you don't need it)

positions:
  filename: /tmp/positions.yaml # Tracks where Promtail is in the log file

clients:
  - url: http://localhost:3100/loki/api/v1/push # URL of your Loki server

scrape_configs:
  - job_name: system
    static_configs:
      - targets:
          - localhost
        labels:
          job: syslog # Label for logs coming from syslog
          __path__: /var/log/syslog-ng/*.log # Path to your syslog file
```

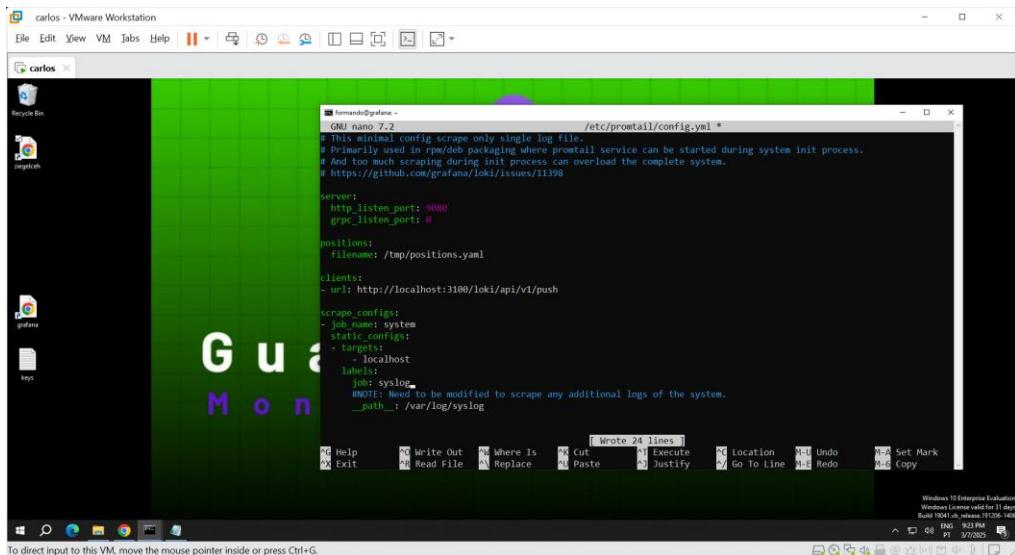


Imagen 96

```
sudo usermod -aG adm promtail
sudo systemctl restart promtail
```

Técnico Especialista Cibersegurança - CET93

Grafana

Utilizando o Grafana conseguimos ter uma visão instantânea do estado da rede.

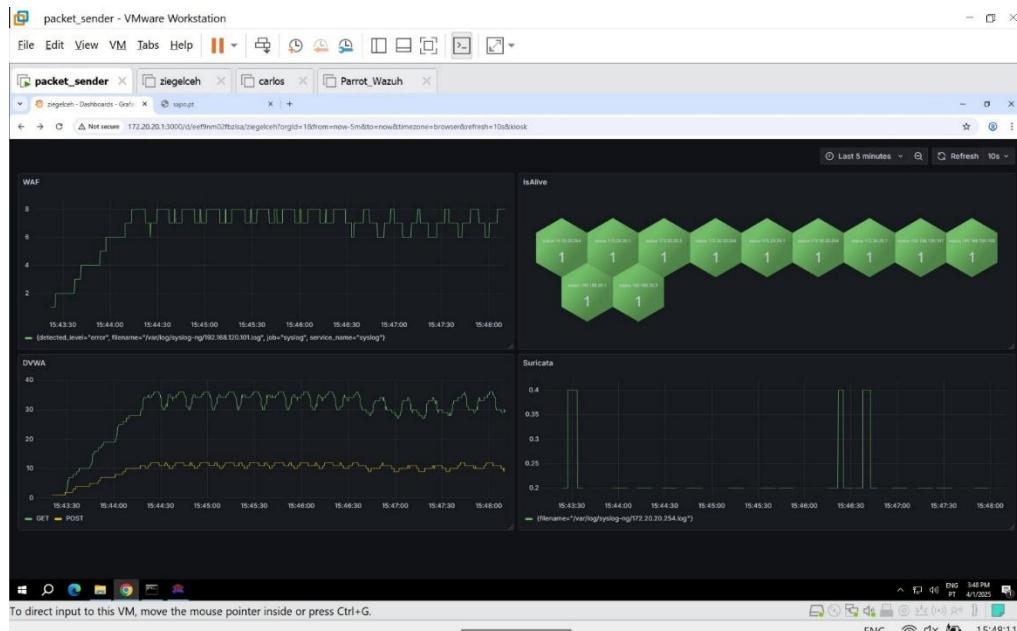


Imagen 97

Técnico Especialista Cibersegurança - CET93

Configuração da LAN, com IP estático, no servidor Debian:

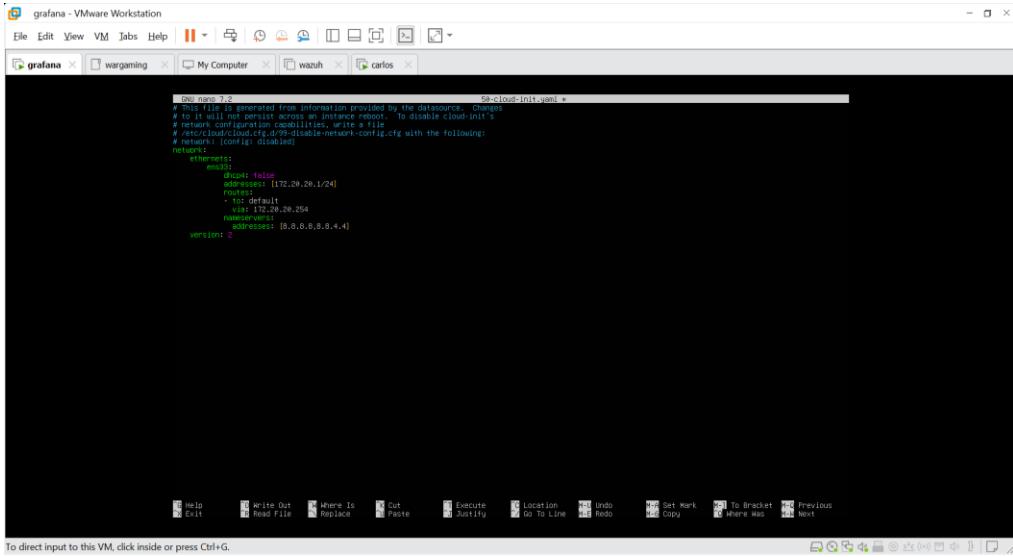


Imagen 98

```
netplan apply
netplan --debug apply
```

Instalação do Grafana:

```
apt-get update
sudo mkdir -p /etc/apt/keyrings/
wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor >
/etc/apt/keyrings/grafana.gpg
echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg]
https://apt.grafana.com stable main" | sudo tee
/etc/apt/sources.list.d/grafana.list
sudo apt update
apt-get install loki promtail
apt install -y Grafana
sudo systemctl start grafana-server
sudo systemctl enable grafana-server
sudo systemctl status grafana-server
sudo ufw allow 3000
```

Técnico Especialista Cibersegurança - CET93

Configuração do da fonte de dados, (ficheiros log, através do Loki)

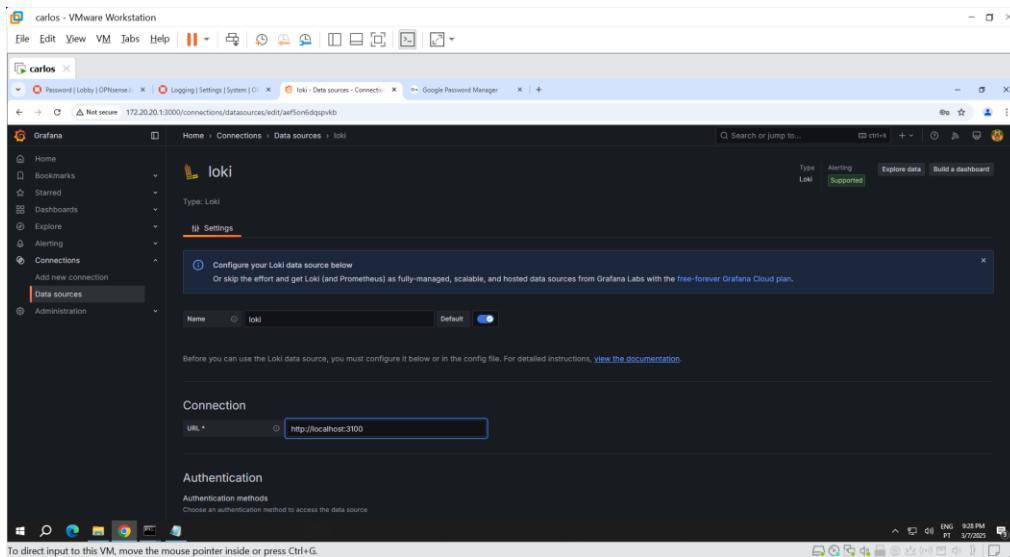


Imagen 99

Técnico Especialista Cibersegurança - CET93

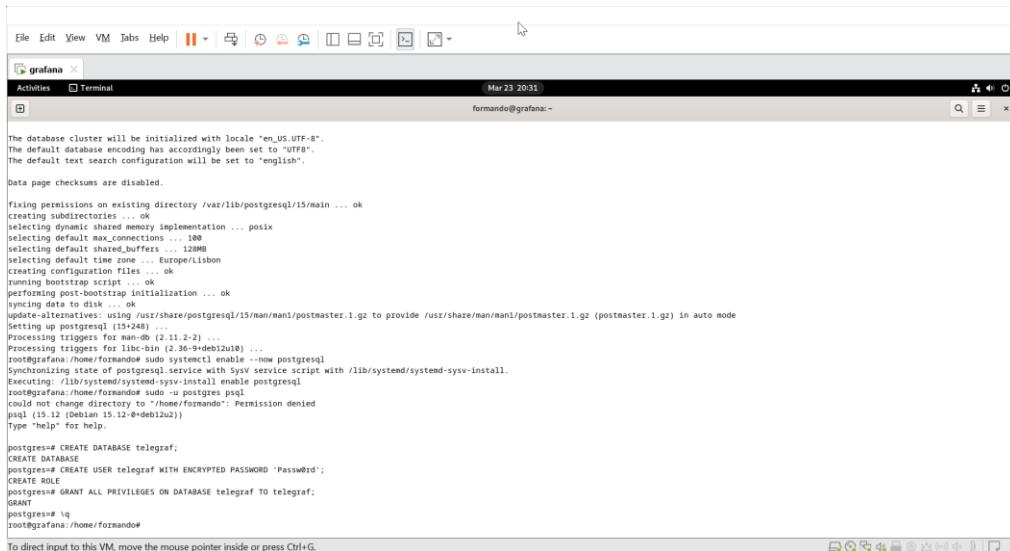
Polystat to monitor ping

Vamos criar uma visualização que nos permita monitorizar os equipamentos que estão ligados.

Instalar PostGres

```
sudo apt install postgresql -y
sudo systemctl enable --now postgresql
```

```
sudo -u postgres psql
CREATE DATABASE telegraf;
CREATE USER telegraf WITH ENCRYPTED PASSWORD 'Passw0rd';
GRANT ALL PRIVILEGES ON DATABASE telegraf TO telegraf;
\q
```



The screenshot shows a terminal window titled "grafana" running on a Linux desktop environment. The terminal output details the installation of PostgreSQL 15, including setting locale, creating the "telegraf" database, creating a user "telegraf" with password "Passw0rd", granting all privileges on the database to the user, and exiting the psql prompt. It also shows the configuration of the PostgreSQL service via Systemctl.

```
The database cluster will be initialized with locale "en_US.UTF-8".
The default database encoding has accordingly been set to "UTF8".
The default text search configuration will be set to "english".

Data page checksums are disabled.

fixing permissions on existing directory /var/lib/postgresql/15/main ... ok
creating subdirectories ... ok
selecting dynamic shared memory implementation ... posix
selecting default max_connections ... 100
selecting default shared_buffers ... 128MB
selecting default time zone ... Europe/Lisbon
creating configuration files ... /etc/postgresql/15/main
creating log directory ... /var/log/postgresql/15
running bootstrap script ... ok
performing post-bootstrap initialization ... ok
syncing data to disk ... ok
updated configuration written to /usr/share/postgresql/15/man/man1/postmaster.1.gz to provide /usr/share/man/man1/postmaster.1.gz (postmaster.1.gz) in auto mode
Setting up postgresql (15+248)
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libpq5 (2.36-9+deb12u1) ...
Syncronizing state of postgresql service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable postgresql
root@grafana:/home/formando# sudo -u postgres psql
could not change directory to '/home/formando': Permission denied
psql: could not connect to server: FATAL:  authentication failed for user "postgres"
        (Debian 15.12-0+deb12u2)
        "type 'help' for help.

postgres=# CREATE DATABASE telegraf;
CREATE DATABASE
postgres=# CREATE USER telegraf WITH ENCRYPTED PASSWORD 'Passw0rd';
CREATE ROLE
postgres=# GRANT ALL PRIVILEGES ON DATABASE telegraf TO telegraf;
GRANT
postgres=# \q
root@grafana:/home/formando#
```

Imagen 100

Técnico Especialista Cibersegurança - CET93

Criar a tabela “ping” no PostgreSQL

```
sudo -u postgres psql
\c telegraf

CREATE TABLE ping (
    time TIMESTAMPTZ NOT NULL,
    measurement TEXT NOT NULL,
    tags JSONB,
    fields JSONB
);

ALTER TABLE public.ping ALTER COLUMN measurement SET DEFAULT
'ping';

GRANT CONNECT ON DATABASE your_database TO telegraf;
GRANT USAGE ON SCHEMA public TO telegraf;
GRANT INSERT, SELECT, UPDATE, DELETE ON ping TO telegraf;

GRANT USAGE ON SCHEMA public TO telegraf;
GRANT CREATE ON SCHEMA public TO telegraf;
GRANT INSERT, SELECT, UPDATE, DELETE ON ALL TABLES IN SCHEMA
public TO telegraf;
ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT INSERT, SELECT,
UPDATE, DELETE ON TABLES TO telegraf;
ALTER USER telegraf WITH SUPERUSER;
```

sudo systemctl restart telegraf



```
File Edit View VM Tabs Help || Activities Terminal Mar 23 20:54 formando@grafana:~ Mar 23 20:34:21 grafana systemd[1]: Stopped telegraf.service - Telegraf. Mar 23 20:34:21 grafana systemd[1]: Starting telegraf.service - Telegraf... Mar 23 20:34:21 grafana telegraf[8970]: 2023-03-23T20:34:21 E! [telegraf] Error running agent: no outputs found, probably invalid config file provided Mar 23 20:34:21 grafana systemd[1]: telegraf.service: Main process exited, code=exited, status=1/FAILURE Mar 23 20:34:21 grafana systemd[1]: telegraf.service Failed with result 'exit-code'. Mar 23 20:34:21 grafana systemd[1]: Failed to start telegraf.service - Telegraf. Mar 23 20:34:21 grafana systemd[1]: telegraf.service timed out waiting for job. Restart counter is at 5. Mar 23 20:34:21 grafana systemd[1]: Stopped telegraf.service - Telegraf. Mar 23 20:34:21 grafana systemd[1]: telegraf.service: Start request repeated too quickly. Mar 23 20:34:21 grafana systemd[1]: telegraf.service: Failed with result 'exit-code'. Mar 23 20:34:21 grafana systemd[1]: Failed to start telegraf.service - Telegraf. root@grafana:~/home/formando$ sudo systemctl enable --now telegraf root@grafana:~/home/formando$ sudo nano /etc/telegraf/telegraf.conf root@grafana:~/home/formando$ nano /etc/telegraf/telegraf.conf root@grafana:~/home/formando$ psql postgres postgres: could not connect to database "postgres" postgres: could not change directory to "/home/formando": Permission denied psql (15.12 (Debian 15.12-0+deb12u2)) Type "help" for help. postgres=# CREATE DATABASE telegraf; ERROR: database "telegraf" already exists postgres=# \c telegraf You are now connected to database "telegraf" as user "postgres". telegraf=# CREATE TABLE ping ( time TIMESTAMPTZ NOT NULL DEFAULT now(), host TEXT NOT NULL, ip TEXT NOT NULL, ttl INT NOT NULL, itt FLOAT NOT NULL ); CREATE TABLE _table_ telegraf# \q root@grafana:~/home/formando$
```

Imagen 101

```
sudo telegraf --test --config /etc/telegraf/telegraf.conf  
sudo systemctl restart telegraf
```

Install Telegraf

```
# Add InfluxData GPG key
wget -qO- https://repos.influxdata.com/influxdata-
archive_compat.key | sudo tee
/etc/apt/trusted.gpg.d/influxdata.asc

# Add the Telegraf repository
echo "deb https://repos.influxdata.com/ubuntu $(lsb_release -
cs) stable" | sudo tee /etc/apt/sources.list.d/influxdata.list

# Update package list
sudo apt update

# Install Telegraf
sudo apt install telegraf -y

sudo systemctl enable --now telegraf
sudo nano /etc/telegraf/telegraf.conf
```

```
[[outputs.postgresql]]
  connection = "host=localhost user=telegraf password=Passw0rd dbname=telegraf
sslmode=disable"
  schema = "public"
  tags_as_jsonb = true  # Opcional: armazenar tags como JSONB
  fields_as_jsonb = true # Opcional: armazenar campos como JSONB
  data_format = "influx"
  name_override = "ping"
  namepass = ["ping"]
```

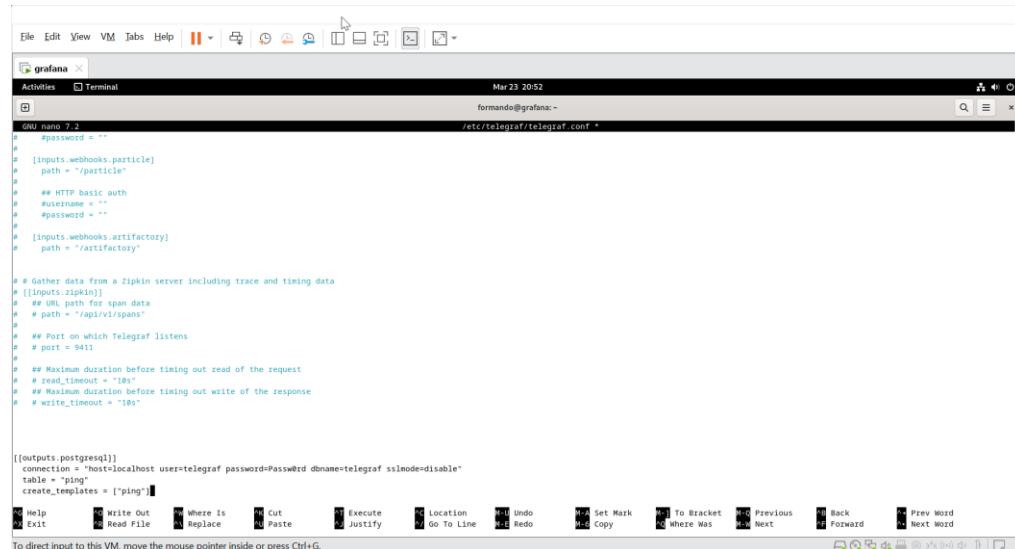


Imagen 102

```
sudo systemctl enable --now telegraf  
sudo systemctl restart telegraf
```

Técnico Especialista Cibersegurança - CET93

Vamos indicar os IPs das máquinas que queremos monitorizar, quanto seu estado On/Off:

```
nano /etc/telegraf/telegraf.conf
```

```
[inputs.ping]
## Hosts to send ping packets to.
urls = ["10.20.10.254", "172.20.20.1", "172.20.20.2",
        "192.168.20.1", "192.168.20.2",
        "172.30.20.1", "172.30.20.7", "192.168.120.101", "192.168.120.102"]
count = 3
timeout = 2.0
```

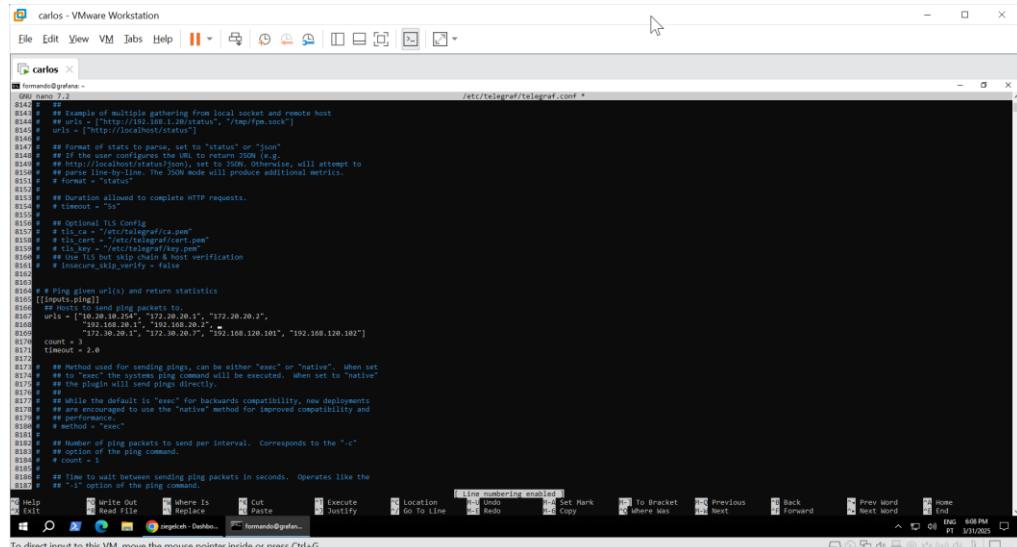


Imagen 103

```
sudo systemctl restart telegraf
```

Técnico Especialista Cibersegurança - CET93

No Grafana, temos que adicionar o **PostgreSQL** como data source.

- URL: 127.0.0.1
- Database: telegraf
- User: telegraf
- Password: Passw0rd

Como a visualização, através de Polysat, não se encontra instalada por omissão, temos que instalar o respetivo plugin:

```
grafana-cli plugins install grafana-polystat-panel
sudo systemctl restart grafana-server
```

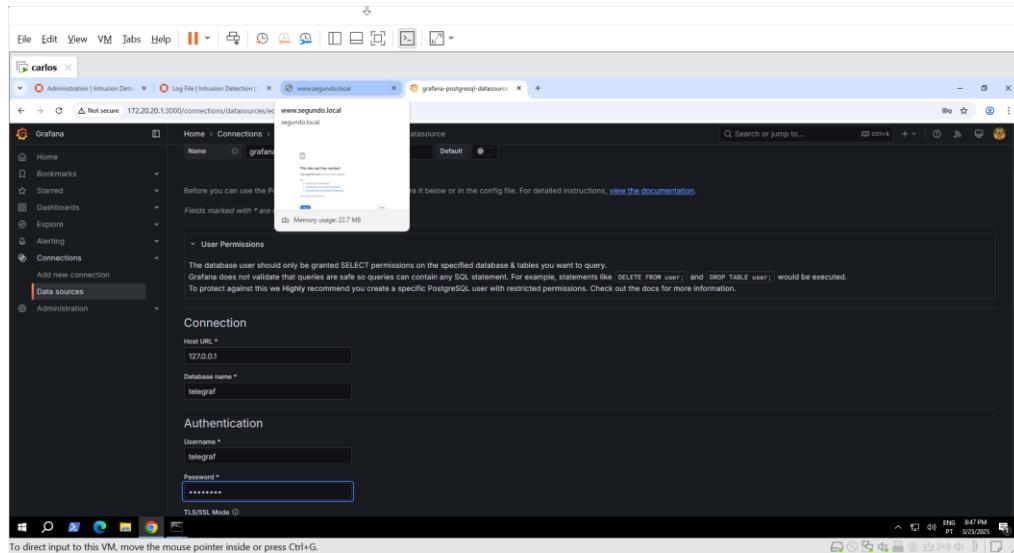


Imagen 104

Save & Test

Técnico Especialista Cibersegurança - CET93

No campo conde, inserimos código para obter os dados para popular o gráfico.

```

SELECT
    url,
    status
FROM (
    SELECT
        time,
        tags->>'url' AS url,
        CASE
            WHEN (fields->>'percent_packet_loss')::FLOAT = 0 THEN 1
            ELSE 0
        END AS status,
        (fields->>'average_response_ms')::FLOAT AS average_latency,
        ROW_NUMBER() OVER (PARTITION BY tags->>'url' ORDER BY time DESC) AS
row_num
    FROM ping
    WHERE $__timeFilter(time)
) subquery
WHERE row_num = 1
ORDER BY url;
    
```

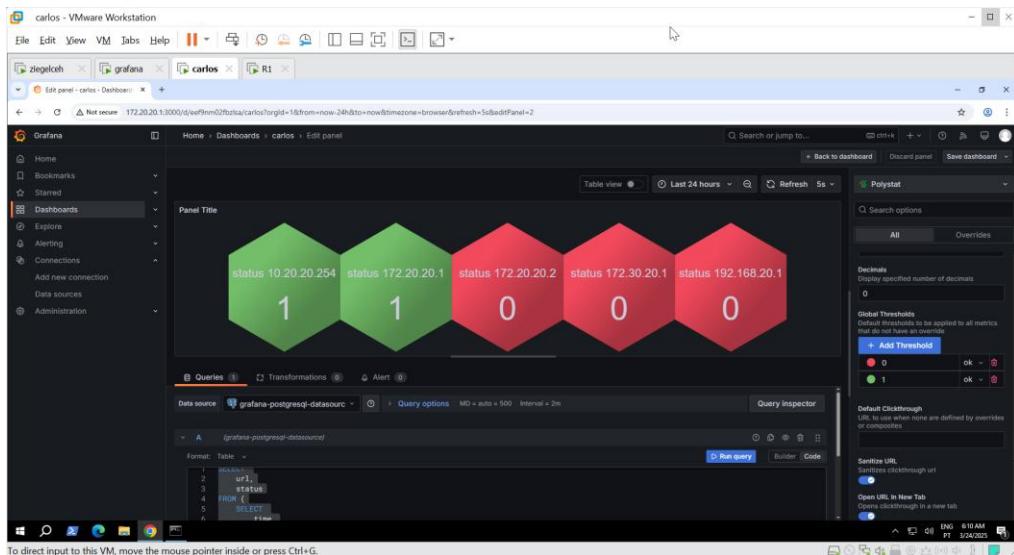


Imagen 105

Para mostrar os elementos em diferentes cores consoante o estado, definimos as cores em Global Thresholds.

Técnico Especialista Cibersegurança - CET93

Packet Sender

Para gerarmos tráfego, por forma a que o Grafana possa mostrar informação nos seu dashboard, usámos uma aplicação que permite gerar pedidos TCP, periódicos, o packet_sender.

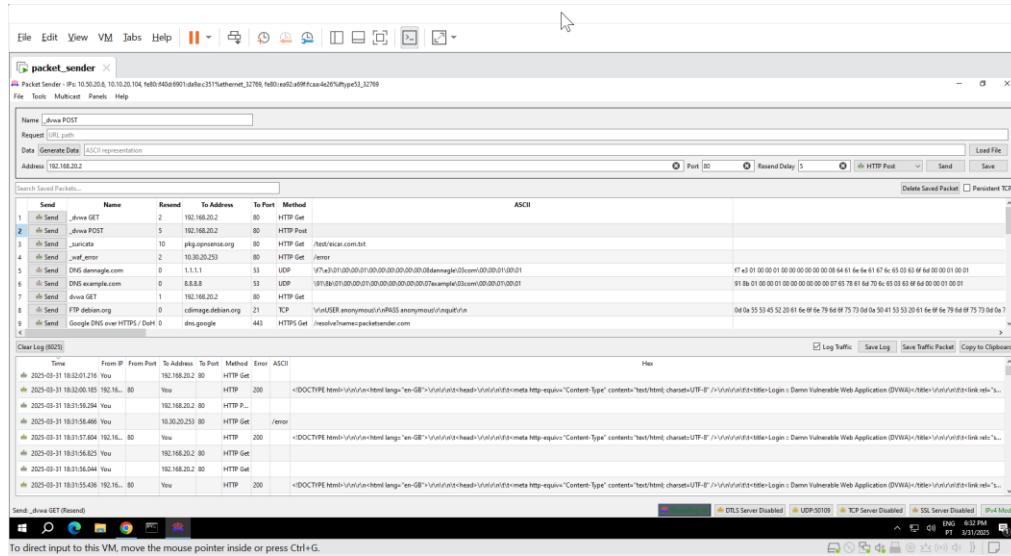


Imagen 106

Técnico Especialista Cibersegurança - CET93

CentOS

Configuramos o IP estático do CentOS:

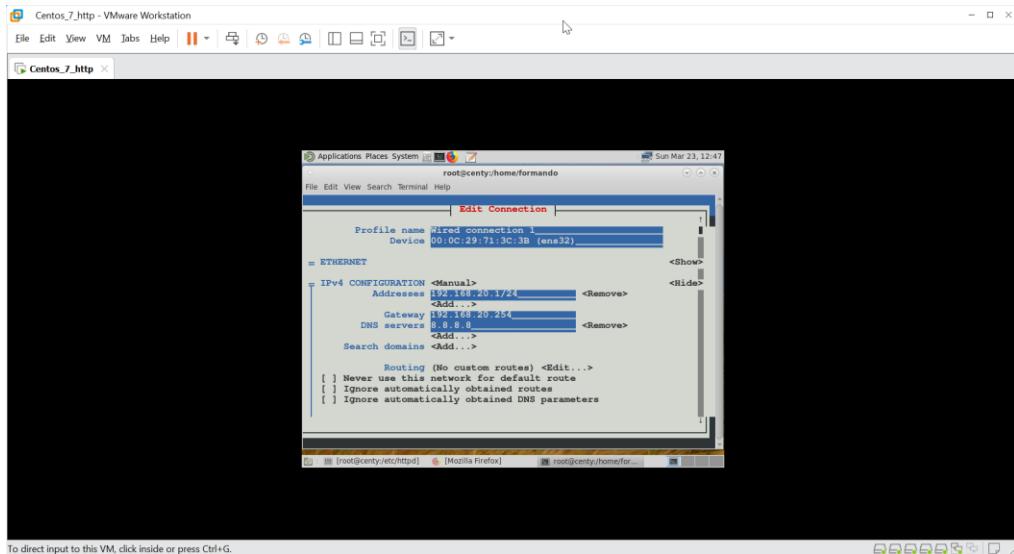


Imagen 107

Nos clientes, neste caso no Windows, configuramos o ficheiro de hosts:

```
192.168.20.1      www.primeiro.local
192.168.20.1      www.segundo.local
```

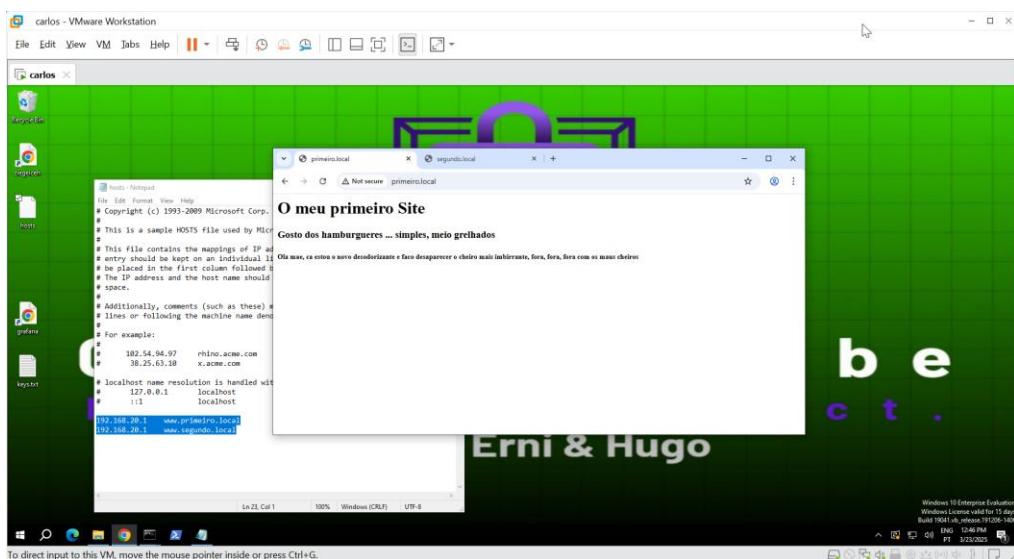


Imagen 108

Técnico Especialista Cibersegurança - CET93

Para podermos aceder, de fora da firewall aos sites do CentOS, criamos o NAT na Firewall:

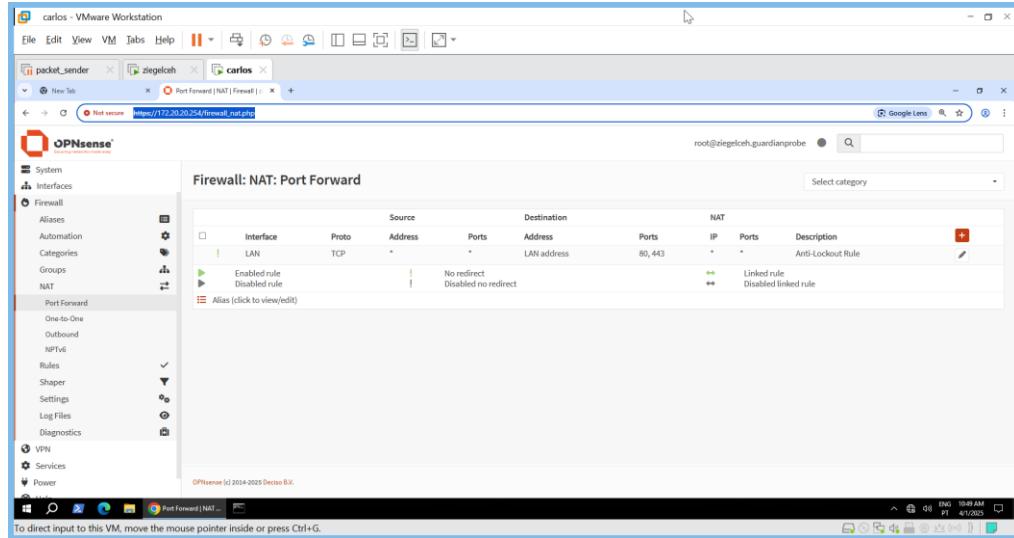


Imagen 109

Técnico Especialista Cibersegurança - CET93

Suricata

Ativar o Suricata e os Logs

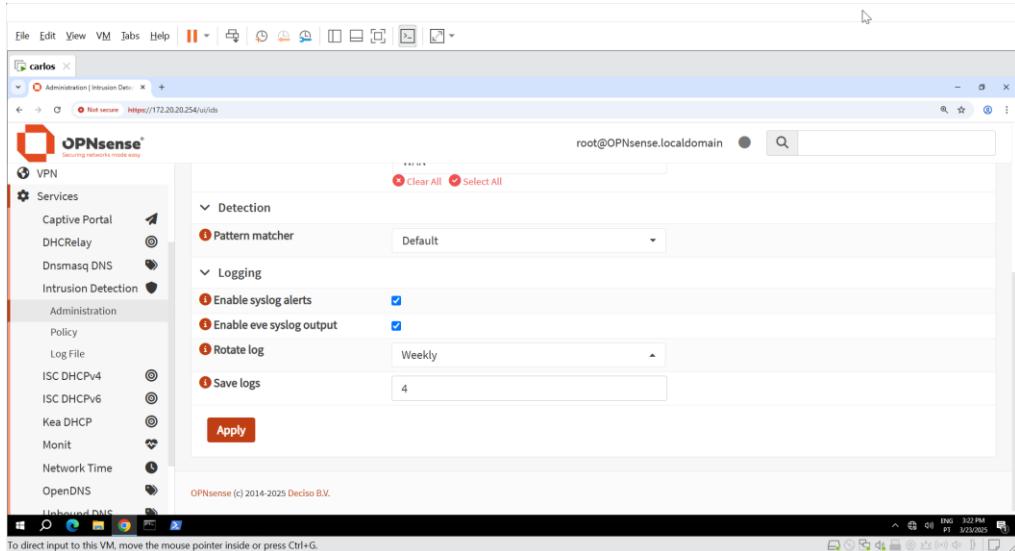


Imagen 110
Fazer o download das regras:

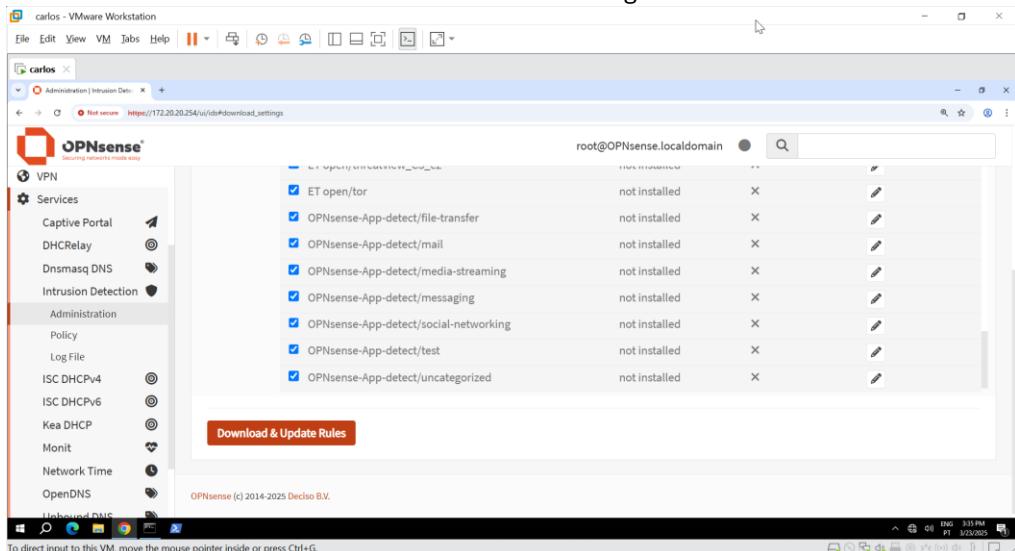


Imagen 111

<https://git.culbertreport.com/posts/Building-A-Detection-Lab-Around-Suricata/>

<https://docs.opnsense.org/manual/how-tos/proxyicapantivirus.html>

<http://pkg.opnsense.org/test/eicar.com.txt>

DVWA Server

Static IP

```
nano /etc/netplan
```

```
network:
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.20.2/24]
      gateway4: 192.168.20.254
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
  version: 2
```

```
netplan try
```

SSH

```
sudo apt update && sudo apt install openssh-server -y
sudo systemctl enable ssh
sudo systemctl start ssh
sudo systemctl status ssh
sudo ufw allow ssh
sudo ufw enable
sudo ufw status
sudo nano /etc/ssh/sshd_config
```

```
PermitRootLogin prohibit-password
PermitRootLogin yes
```

```
sudo systemctl restart ssh
```

Mudar a porta:

```
sudo nano /etc/ssh/sshd_config
```

```
Port 2222
```

```
sudo ufw allow 2222/tcp
sudo systemctl restart ssh
```

A partir de uma máquina remota:

```
ssh -p 2222 username@192.168.20.2
```

Instalação do DVWA

Instalar o Apache, a BD MariaDB e o PHP:

```
sudo apt update && sudo apt install apache2 mariadb-server php  
php-mysqli php-gd -y
```

Descarregar e instalar o DVWA:

```
cd /var/www/html  
sudo git clone https://github.com/digininja/DVWA.git  
sudo chown -R www-data:www-data DVWA
```

Configurar a Base de Dados:

```
sudo mysql -u root -p  
sql  
CREATE DATABASE dvwa;  
CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'Passw0rd';  
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';  
FLUSH PRIVILEGES;  
EXIT;
```

Configurar o DVWA (config.inc.php):

```
cd /var/www/html/DVWA/config/  
cp config.inc.php.dist config.inc.php  
sudo nano /var/www/html/DVWA/config/config.inc.php
```

Definir o user e a password:

```
$_DVWA[ 'db_user' ] = 'dvwa';  
$_DVWA[ 'db_password' ] = 'password';
```

Ativar e reiniciar os serviços:

```
sudo systemctl restart apache2  
sudo systemctl restart mysql
```

```
mv /var/www/html/DVWA/* /var/www/html/  
rm -rf /var/www/html/DVWA  
chown -R www-data:www-data /var/www/html/  
chmod -R 755 /var/www/html/  
systemctl restart apache2  
apt install php-mysql -y  
systemctl restart apache2
```

Técnico Especialista Cibersegurança - CET93

- [http://<ubuntu-ip>/DVWA/.](http://<ubuntu-ip>/DVWA/)
- Default Login:

User: admin

Pass: password

Técnico Especialista Cibersegurança - CET93

ZenMap

Varrimento através do ZenMap à rede ZiegelCEH_Green

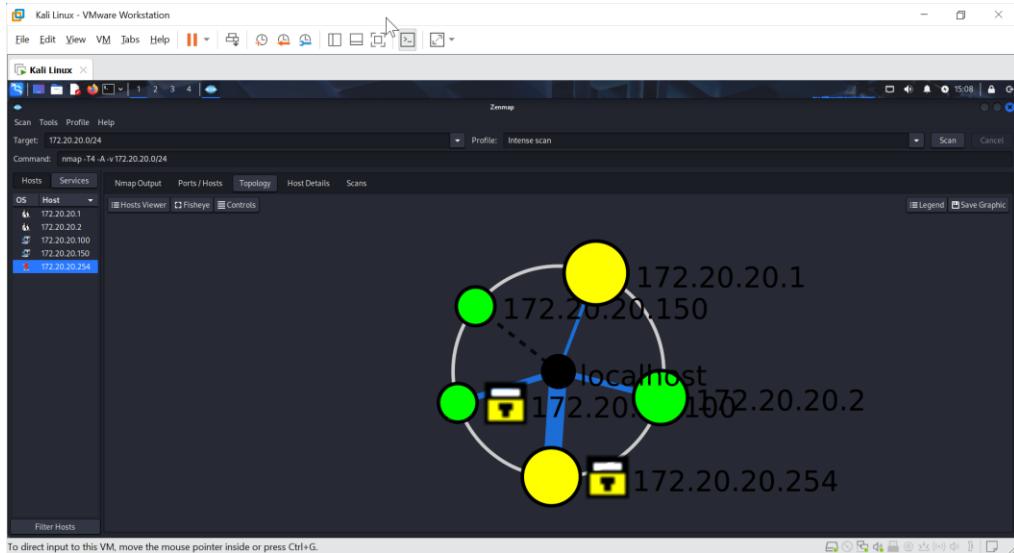


Imagen 112

Portas abertas por host:

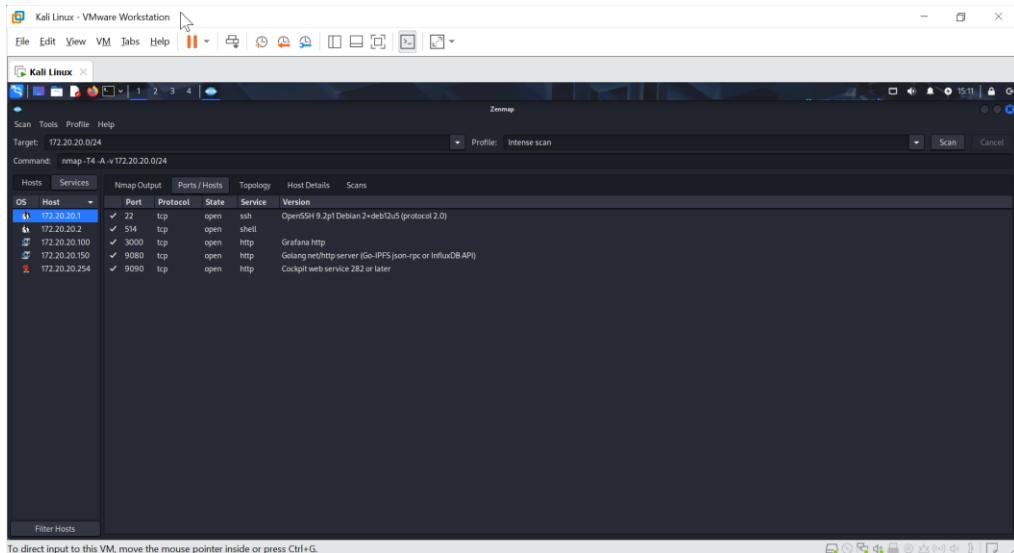


Imagen 113

Técnico Especialista Cibersegurança - CET93

Conclusão

Este projeto apresentou vários desafios, por um lado por ser um projeto de alguma dimensão, por se o primeiro CET de cibersegurança do Cinel e também por ser um trabalho de grupo. Consideramos que nenhum destes aspetos foi negativo, antes pelo contrário, foi uma oportunidade de aprendizagem, por forma a estarmos mais preparados para um de sucesso, no mundo do trabalho.

Este projeto permitiu, por um lado, aprofundar alguns conhecimentos adquiridos a longo do curso, mas também, por outro lado, sedimentar algumas matérias que não ficaram tão bem apreendidas.

Ao longo da realização deste Projeto Final do curso Técnico/a Especialista em Cibersegurança (CET93), nós, Carlos, Erni e Hugo, pudemos consolidar e aplicar os conhecimentos adquiridos durante a formação no CINEL. Este trabalho permitiu-nos aprofundar competências técnicas em áreas como configuração de redes, gestão de firewalls (PFsense e Opnsense), implementação de VPNs e utilização de ferramentas de segurança como Snort, Suricata, Wazuh e OpenVAS. Aprendemos a importância de uma documentação rigorosa, essencial para garantir a replicabilidade das configurações, e desenvolvemos uma maior capacidade de trabalho em equipa, fundamental para coordenar as diferentes tarefas e alcançar os objetivos propostos.

No entanto, o projeto não esteve isento de desafios. Enfrentámos dificuldades na configuração inicial das VLANs e na integração das VPNs, especialmente na garantia de que as políticas de segurança permitissem o acesso desejado sem comprometer a proteção da rede. A gestão do tempo também se revelou um obstáculo, dado o volume de configurações e testes necessários num prazo limitado, o que por vezes nos levou a priorizar certas tarefas em detrimento de uma análise mais aprofundada de algumas funcionalidades.

Como tentamos tirar partido de poder trabalhar remotamente, configurámos um router Vyos de forma a podermos simular a comunicação mesmo não estando nas instalações do Cinel.

Tentámos explorar um pouco a configuração do Grafana, através de uma base de dados, PostGres, para a qual configurámos o Telegraf, a escrever o resultado dos pings às máquinas. Constatámos posteriormente que havia maior integração com uma base dados do tipo InfluxDB. Sempre a andar e a aprender.

Se tivéssemos a oportunidade de realizar este projeto novamente, algumas melhorias poderiam ser implementadas. Em primeiro lugar, planeávamos com maior antecedência a divisão das tarefas, permitindo uma abordagem mais equilibrada entre a configuração prática e a elaboração do relatório. Além disso, investiríamos mais tempo na simulação prévia das soluções em ambientes de teste, de modo a identificar e resolver potenciais problemas antes da apresentação final. Por fim, exploraríamos de forma mais detalhada as sugestões de melhoria da segurança, como a implementação de políticas de autenticação mais robustas ou a otimização das regras de firewall, para reforçar a fiabilidade e a usabilidade da infraestrutura.

Este projeto foi uma experiência enriquecedora que nos preparou para os desafios do mercado de trabalho na área da cibersegurança, deixando-nos mais confiantes nas nossas capacidades e conscientes das áreas onde podemos continuar a evoluir.

Finalmente, como o fizemos ao longo do curso, temos a noção de que a aquisição de conhecimentos não é algo estático, e que devemos continuar o nosso processo de aprendizagem.

Agradecimentos

Queremos agradecer a todos os formadores que nos acompanharam ao longo desta formação, pelo seu esforço, dedicação e paciência.

Agradecemos, também, ao Cinel, coordenador e equipa.

Esperamos continuar a defender o nome da instituição, através do nosso empenho e valorização dos conhecimentos adquiridos.

Referências

Instalação do Cockpit

<https://cockpit-project.org/running>

Installing the Wazuh server step by step

<https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html>

Wazuh installation assistant

(para ver a versão atual, à data deste relatório era a 4.10)

<https://github.com/wazuh/wazuh-installation-assistant?tab=readme-ov-file#user-guide>

Netplan config usando static IP

<https://netplan.readthedocs.io/en/stable/using-static-ip-addresses/>

Ubuntu UFW

<https://help.ubuntu.com/community/UFW>

SQL Server Firewall Windows Server

<https://learn.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver15>

Debia OpenVas GreenBone

<https://github.com/itilgent/Easy-OpenVAS-Installer>

Configurações Router e Switch

<https://www.cisco.com/c/en/us/td/docs/routers/access/800M/software/800MSCG/routconf.html>

<https://community.cisco.com/t5/networking-knowledge-base/how-to-configure-vlans-on-the-catalyst-switches/ta-p/3131780>

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-10/configuration_guide/sec/b_1610_sec_9500_cg/b_1610_sec_9500_cg_chapter_0101010.html

Técnico Especialista Cibersegurança - CET93

OpenVPN cliente

<https://openvpn.net/>