Workshop – Projeto Connor

Firewall UTM

pfsense®

Gelson Filho

Renato Junior

Facens

lenovo

Connor

Planejamento para parte teórica

01

Protocolos no modelo OSI

02

NAT

03

Proxy

04

VPN

05

Definição de Firewall

06

Firewall X UTM X PfSense

07

Configurações de rede na VM

08

Exercícios

Planejamento para a parte prática

01
Instalação e configuração

02
Funções na console

03
Funções na interface gráfica

04
Criação de regras

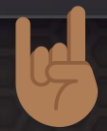
05
Configurações de NAT

06
Configurações de Proxy

07
Backup e Restauração, Outras Aplicações

08
Exercícios

Protocolos no modelo OSI



Camadas		Protocolos	Função
1	Aplicação	HTTP, RTP, SMTP,FTP,SSH, Telenet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS...	Prover serviços de rede às aplicações
2	Apresentação	XDR, TLS...	Criptografia, codificação, compressão e formatos de dados
3	Sessão	NetBIOS...	Iniciar, manter e finalizar sessões de comunicação
4	Transporte	NetBEUI, TCP, UDP, SCTP, DCCP, RIP...	Transmissão confiável de dados, segmentação
5	Rede	IP, (IPv4, IPv6), Ipsec, ICMP, ARP, RARP, NAT	Endereçamento lógico e roteamento; Controle de tráfego
6	Enlace	Ethernet, IEEE 802. 1Q, HDLC, Token ring, FDDI, PPP, Swicth, Frame, relay, ATM...	Endereçamento físico; Transmissão confiável de quadros
7	Física	Modem, 802. 11 WIFI, RDIS, RS-232, EIA-422, RS-449, Bluetooth, USB, 10BASE-T, 100BASE, TX, ISDN, SONET, DSL...	Interface com meios de transmissão e sinalização

FTP(21) – Telnet(23) – SMTP(25) – HTTP (80) – POP3(110) – IMAP(143) – HTTPS(443) – SSH(22) – DNS(53) – RDP(3389) – DHCP_v4_server(67) – DHCP_v4_client(68) ...

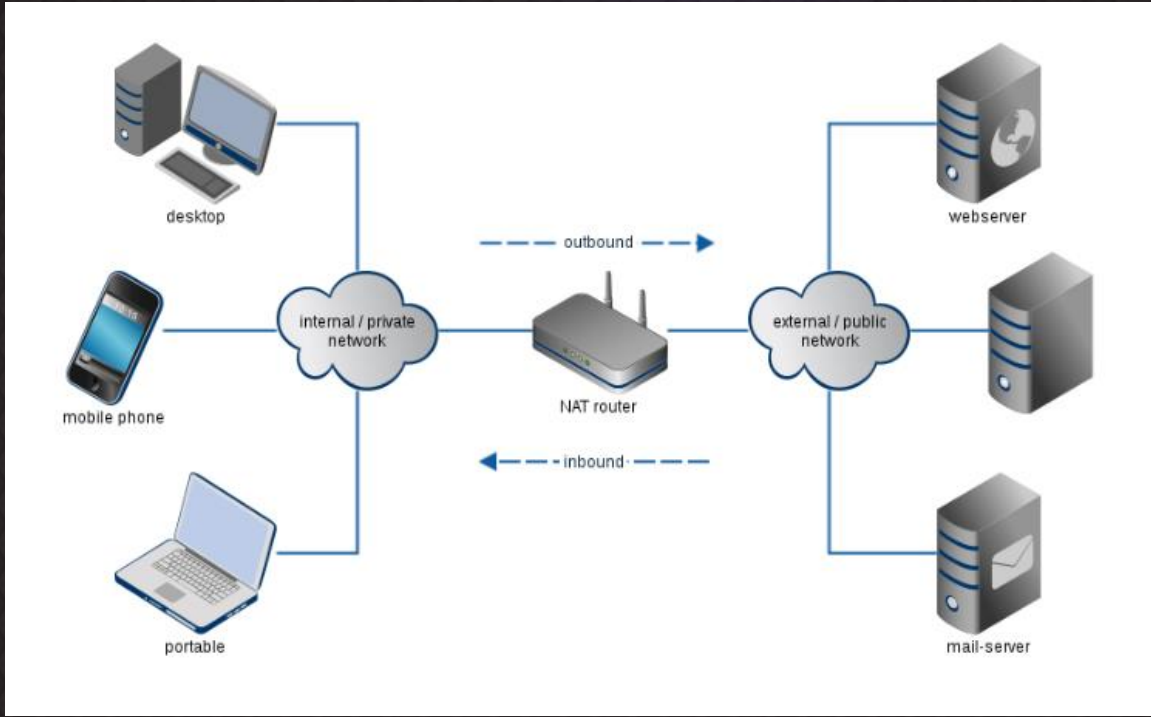
SSL - TLS

TCP - UDP

IPV4 - IPV6

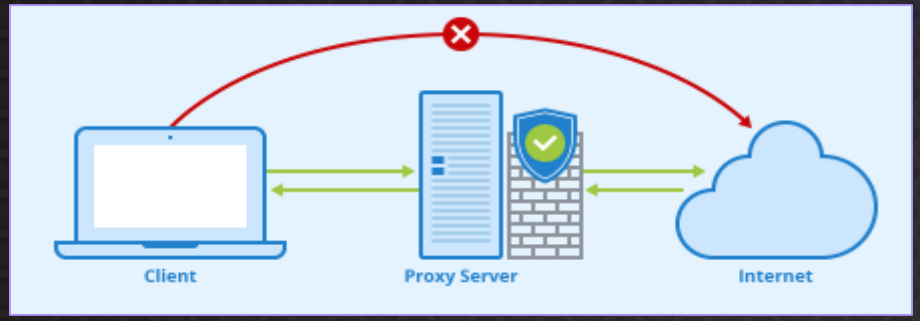
* Em parênteses a porta do serviço a ser transportado conforme a camada de transporte (via UDP ou TCP) segundo a IANA

NAT – Network Address Translation



“O NAT protocolo aplicado na camada de rede e tem como função fazer a tradução dos endereços IP e Portas TCP da rede local para o mundo (Internet)”

Proxy



Tipos:

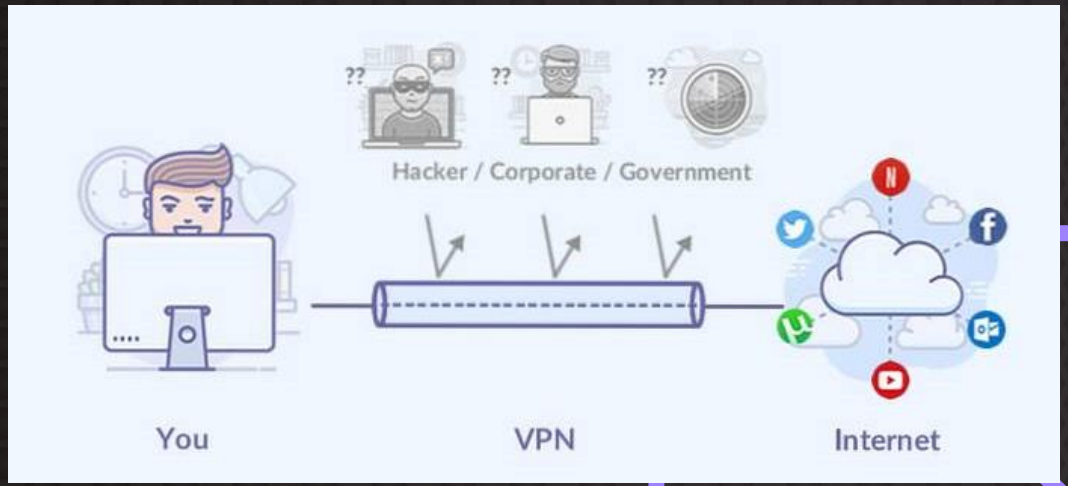
- **Transparente** (não dificulta autenticações de usuário – usuário nem sabe que ele existe)
- **Não transparente** (normal – o que tem que configurar no navegador)

- Problema em https – trafego criptografado
- Solução: MITM - man-in-the-middle

- Conhecido como “intermediador”, “gateway de aplicação” ou “firewall de aplicação” – ele entende muito bem os protocolos da camada de aplicação
- Impõe política de segurança (o que pode o que não pode)
- Armazena dados de aplicações em cache (ganho de desempenho)
- Restringe acesso (por URL, content-type, content-lenght do http, expressões regulares, horário, porta TCP/UDP, login de usuário, etc)

VPN – Virtual Private Network

“Túnel criptografado para envio/recebimento de informações”



Tipo 3: **VPN site a site** (conexão entre redes de escritórios/filiais compartilhando recursos e informações)

Tipo 1: **VPN de acesso remoto** (a partir de algum software especial com registro permite o acesso remoto fácil e seguro)

Tipo 2: **VPN pessoal** (proteção e navegação na internet)

O que é um Firewall?

"Um **firewall** é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança."

Tipo 1: **Packet Filtering** (Filtragem de pacotes – atuação mais superficial, regras de IP, tipo de pacote, número de porta apenas, etc)

Tipo 2: **Proxy Services** (Firewall de aplicação)

Tipo 3: **Stateful Inspection** (Inspeção de estados – atuação na camada de rede)

UTM

(Unified Threat Manager)

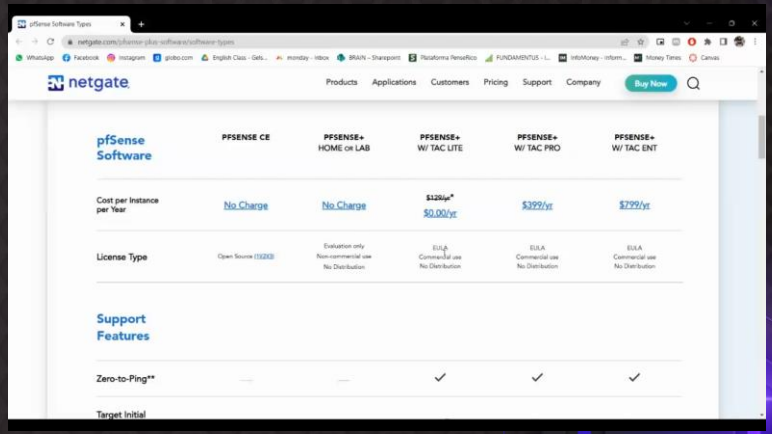
→ Engloba muito mais aplicações para segurança de redes

Firewall ≠ UTM

pfsense → UTM

- Possui versão open-source de excelente usabilidade
- Recomendado principalmente para empresas pequenas e médias
- Instalado em appliance (hardware e software integrados especificamente para a UTM)
- Instalado em FreeBSD (SO baseado em UNIX)
- Foi desenvolvido para ser extremamente fácil de usar

Versões:



Configurações de rede na VM

Mode	VM→Host	VM←Host	VM1↔VM2	VM→Net/LAN	VM←Net/LAN
Host-only	+	+	+	–	–
Interna	–	–	+	–	–
Bridge	+	+	+	+	+
NAT	+	Port forward	–	+	Port forward
Rede NAT	+	Port forward	+	+	Port forward

Vamos exercitar?

Qual alternativa apresenta apenas protocolos da camada de aplicação?

A SMTP, HTTP, HTTPs, RDP, SSH e DNS

B ISDN - 802.11 - DSL - Ethernet - NetBios e RIP

C SSL, SMTP, HTTP, IPV4, IPV6 e USB

D NAT - IEEE 802 - Modem - ICMP - HTTP e IPV6

Qual finalidade no emprego de certificados SSL/TLS na comunicação web?

A Proteger o usuário contra vírus

B Permitir um canal seguro de comunicação entre o usuário e o website

C Proteger a empresa contra ransomware

D Realizar cache do website, agilizando futuros acessos

Um usuário reclama que não está conseguindo acessar o “google”, a mensagem sempre é: "Could not resolve address www.google.com". Em qual Serviço/Protocolo está o problema?

A HTTP

B DHCP

C DNS

D ICMP

Com relação à camada de transporte (TCP/UDP), segundo a IANA quais são as portas para os protocolos HTTP, HTTPs, SSH e DNS consecutivamente?

A 45, 85, 666, 8080

B 443, 92, 500, 65535

C 10, 11, 16, 80

D 80, 443, 22, 53

A VPN não pode ser utilizada para:

A Bloquear acesso à sites do governo

B Conectar de maneira segura duas empresas através de um link público de internet

C Permitir que usuários fora da empresa se conectem de maneira segura na internet

D Assistir NETFLIX quando o acesso direto ao site estiver bloqueado

Sobre Proxy é correto afirmar que:

A No tipo "não transparente" o usuário não precisa configurar absolutamente nada no navegador

B Ele não só impõe políticas de segurança como também armazena dados em cache para aumento de desempenho na web

C Libera acesso para todos na LAN e na WAN pois não analisa o content-type e outros atributos do HTTP

D Ao utilizá-lo como man-in-the-middle você está praticando um crime

Sobre PfSense é correto afirmar que:

A Ele é um Firewall de dispositivo final criado para banir automaticamente ações maliciosas do usuários

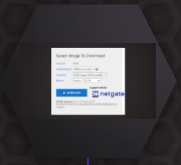
B Ele é uma aplicação remota de detecção de vírus e malwares

C Ele é um Firewall UTM de código aberto baseado no FreeBSD criado para ser fácil de usar

D Ele é uma máquina virtual que restringe os usuários de acessos à cloud computing

Vamos praticar um pouco?

Instalação e Configuração



Baixar a .iso.gz

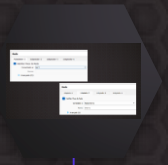
https://www.pfsense.org/download/

Descompactá-la para deixa-la como .iso apenas

Criar a VM

SO: FreeBSD

2048 RAM
Todos core do processador
64 bits
Programar boot com a .iso



Criar redes

WAN e LAN

Adaptador 1 – NAT
Adaptador 2 – Rede interna (nome: “interna”)

Ligar a VM

Instalação do PfSense

Só clicar em next, next...
Após terminar, remover a .iso para o boot acontecer pelo HD e não pelo disco

Select Image To Download

Version: 2.6.0

Architecture: AMD64 (64-bit)

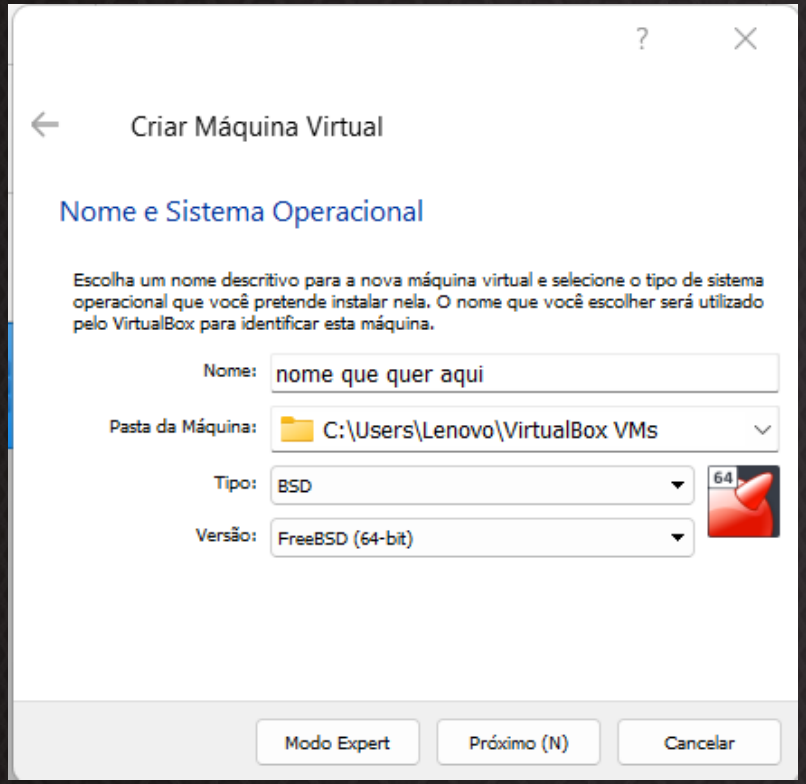
Installer: DVD Image (ISO) Installer

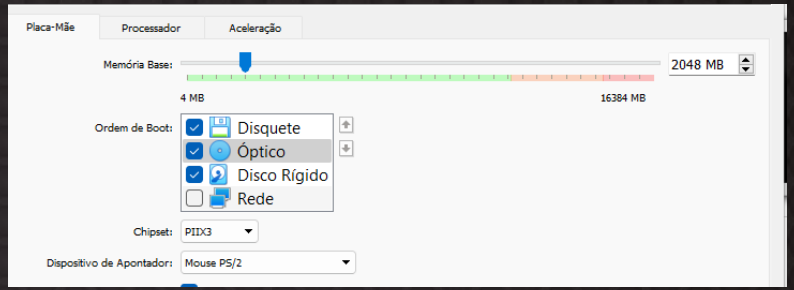
Mirror: Austin, TX USA

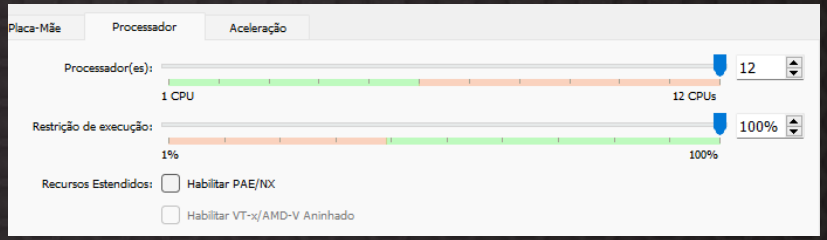
DOWNLOAD

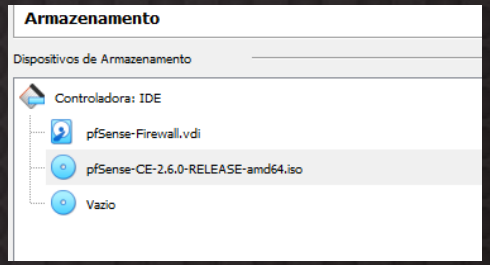
Supported by

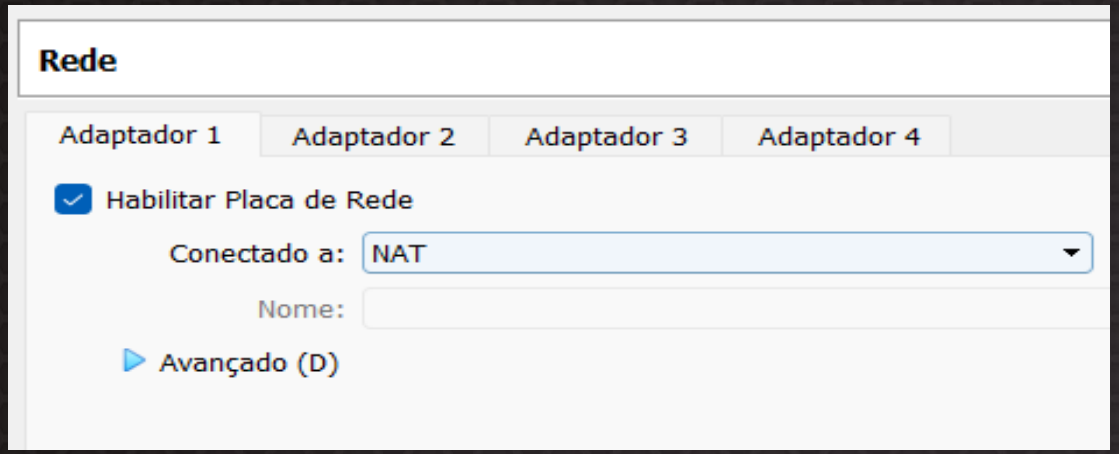
SHA256 Checksum for compressed (.gz) file:
941a68c7f20c4b635447cceda429a027f816bdb78d54b8252bb87abf1fc22ee3

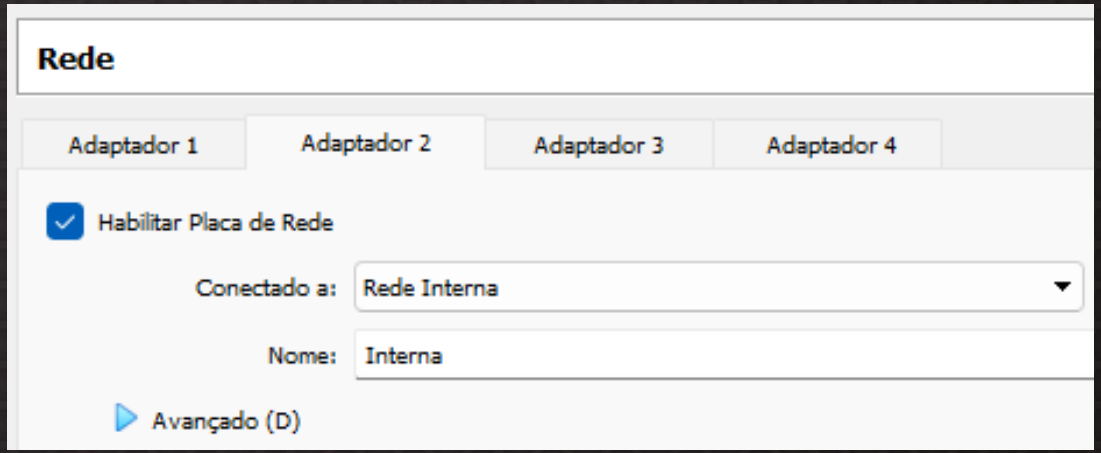

Criar Máquina Virtual
Nome e Sistema Operacional
Escolha um nome descritivo para a nova máquina virtual e selecione o tipo de sistema operacional que você pretende instalar nela. O nome que você escolher será utilizado pelo VirtualBox para identificar esta máquina.
Nome:
nome que quer aqui
Pasta da Máquina:
C:\Users\Lenovo\VirtualBox VMs
Tipo:
BSD
Versão:
FreeBSD (64-bit)
Modo Expert
Próximo (N)
Cancelar

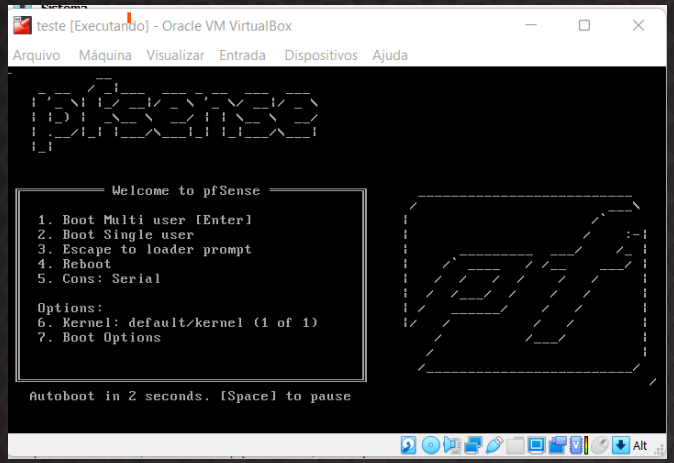

Placa-Mãe
Processador
Aceleração
Memória Base:
2048 MB
4 MB
16384 MB
Ordem de Boot:
Disquete
Óptico
Disco Rígido
Rede
Chipset:
PIIX3
Dispositivo de Apontador:
Mouse PS/2

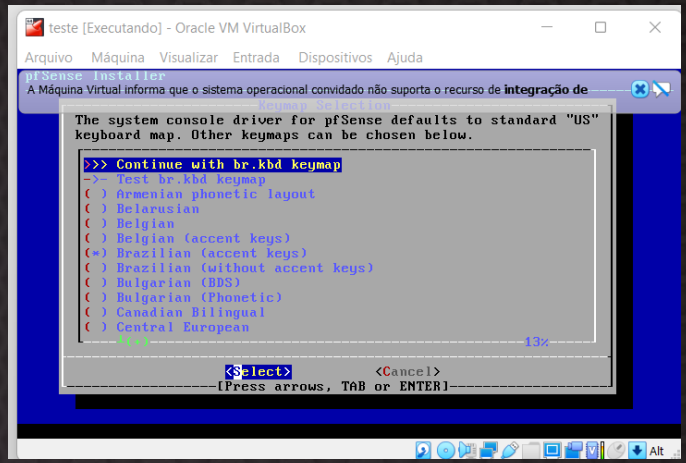

Placa-Mãe
Processador
Aceleração
Processador(es):
12
1 CPU
12 CPUs
Restrição de execução:
100%
1%
100%
Recursos Estendidos:
Habilitar PAE/NX
Habilitar VT-x/AMD-V Aninhado

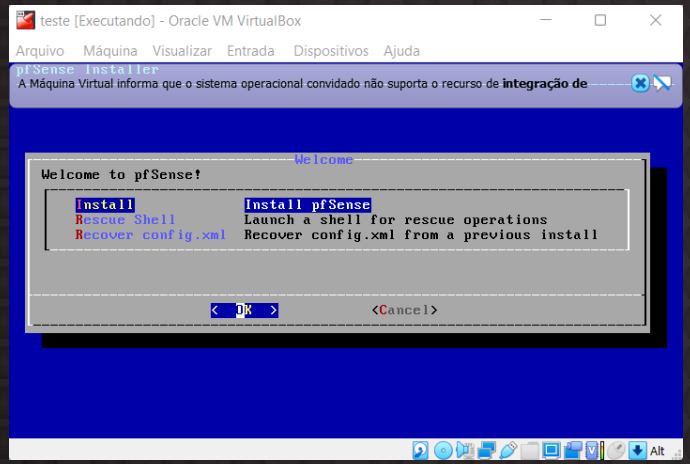

Armazenamento
Dispositivos de Armazenamento
Controladora: IDE
pfSense-Firewall.vdi
pfSense-CE-2.6.0-RELEASE-amd64.iso
Vazio

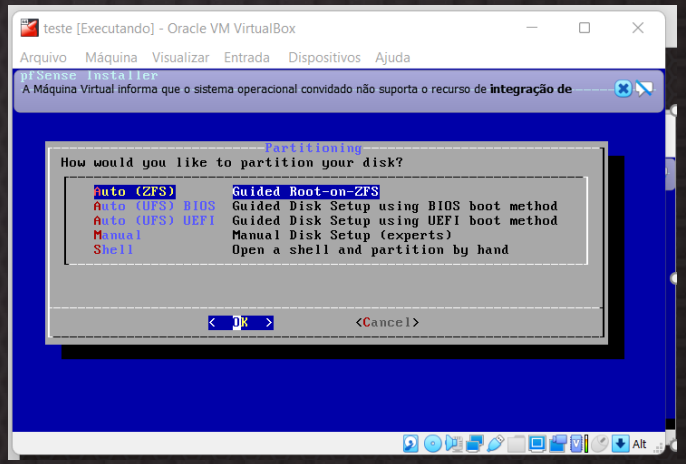

Rede
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar Placa de Rede
Conectado a:
NAT
Nome:
Avançado (D)


Rede
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar Placa de Rede
Conectado a:
Rede Interna
Nome:
Interna
Avançado (D)

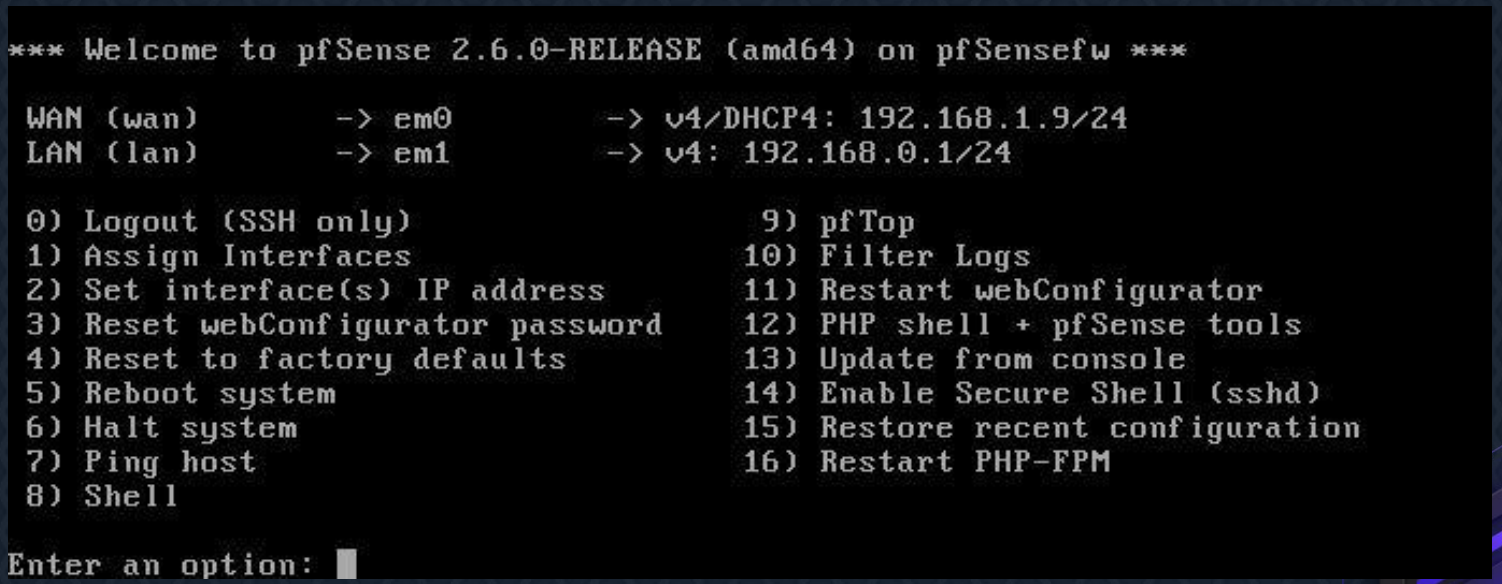

teste [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Welcome to pfSense
1. Boot Multi user [Enter]
2. Boot Single user
3. Escape to loader prompt
4. Reboot
5. Cons: Serial
Options:
6. Kernel: default/kernel (1 of 1)
7. Boot Options
Autoboot in 2 seconds. [Space] to pause


teste [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
pfSense Installer
A Máquina Virtual informa que o sistema operacional convidado não suporta o recurso de integração de
Keymap Selection
The system console driver for pfSense defaults to standard "US" keyboard map. Other keymaps can be chosen below.
>>> Continue with br.kbd keymap
-> Test br.kbd keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
(*) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
13%
<Select> <Cancel>
[Press arrows, TAB or ENTER]


teste [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
pfSense Installer
A Máquina Virtual informa que o sistema operacional convidado não suporta o recurso de integração de
Welcome
Welcome to pfSense!
Install Install pfSense
Rescue Shell Launch a shell for rescue operations
Recover config.xml Recover config.xml from a previous install
< OK > <Cancel>


teste [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
pfSense Installer
A Máquina Virtual informa que o sistema operacional convidado não suporta o recurso de integração de
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) BIOS Guided Disk Setup using BIOS boot method
Auto (UFS) UEFI Guided Disk Setup using UEFI boot method
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK > <Cancel>

Funções da Console (CLI)



Funções da Console (CLI)

0) Logout (SSH only)
Usado para se desconectar no acesso via SSH

1) Assign Interfaces
Caso deseje criar uma nova interface

2) Set interface(s) IP Address
Atribui IPs as interfaces

3) Reset webConfigurator password
Reseta a senha da interface web

4) Reset to factory defaults
Reseta para o padrão de fábrica

5) Reboot System
Reinicia o Sistema

6) Halt System
Desliga o sistema

7) Ping Host
Realiza ping para o host

8) Shell
Terminal do Shell

9) pfTop
Mostra as conexões que estão ocorrendo no momento

10) Filter Logs
Mostra os logs referente ao firewall

11) Restart webConfigurator
Reinicia o webConfigurator

12) PHP shell + pfSense tools
Terminal Shell para desenvolvedores

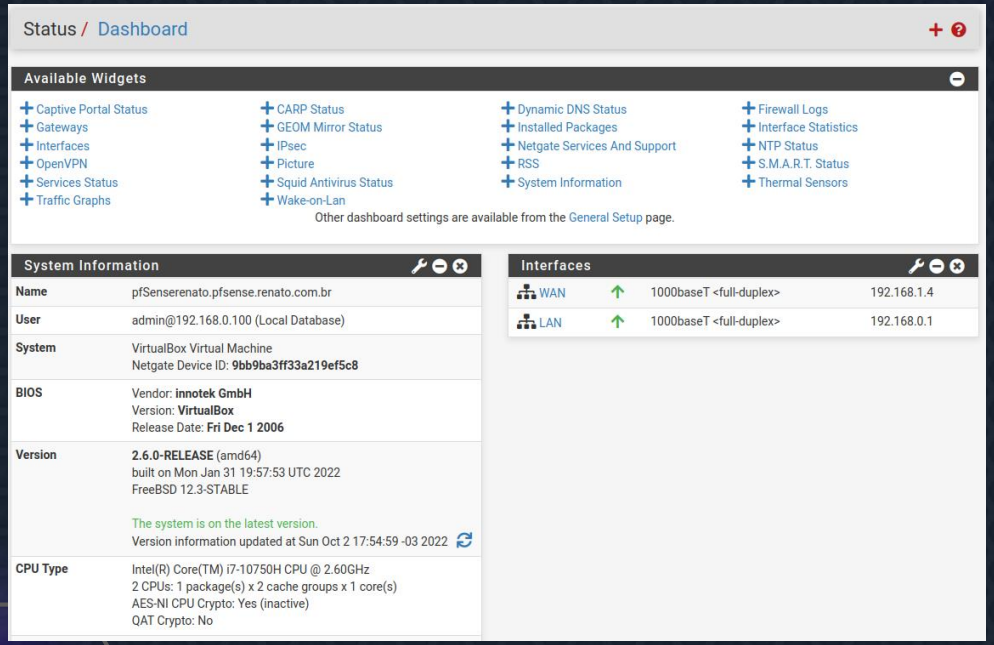
13) Update from console
Atualiza o pfSense

14) Enable segure shell (sshd)
Habilita/desabilita a configuração remota via ssh

15) Restore recent configurator
Restaura backups

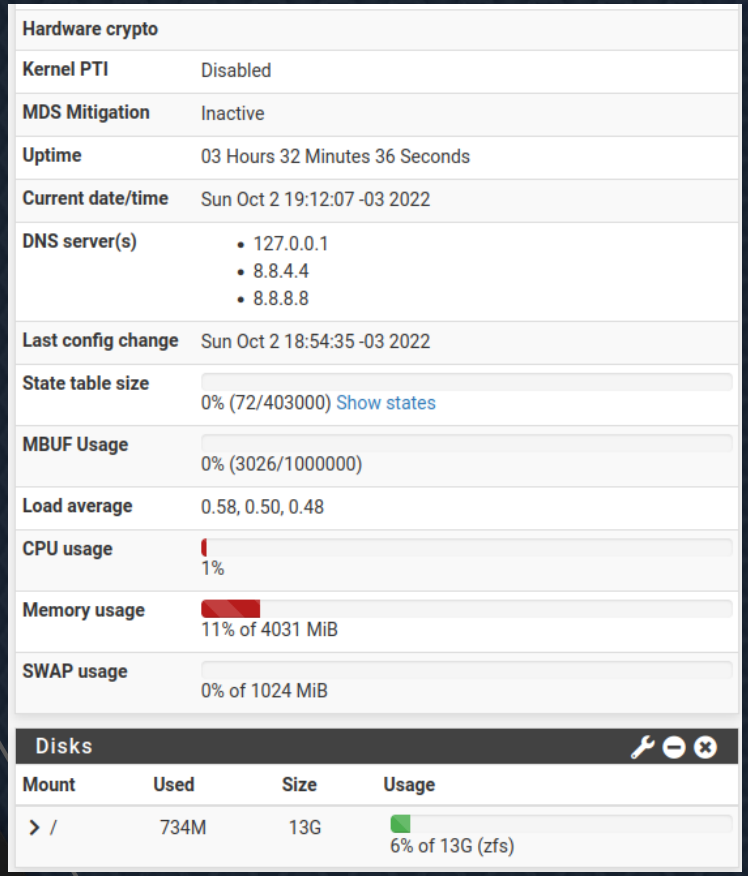
16) Restart PHP-FPM
Reinicia o web server PHP

Funções na Interface gráfica



- Na interface é possível adicionar diversos status em seu dashboard;
- Das informações padrão temos as placas de rede instaladas, no caso WAN e LAN;
- Nome de domínio;
- Status de BIOS, versão do PfSense;
- Hardware utilizado.

Funções na Interface gráfica



Das informações mais importantes temos:

- Tempo de atividade;
- Servidor DNS sendo utilizado;
- Uso de CPU;
- Uso de memória;
- Uso de memória em disco.

Regras de Conectividade

Criação de Aliases

“Variáveis”

Nomes, sites, IPs, redes, portas, conjuntos de urls que constantemente serão utilizados em regras

Criação de Schedules

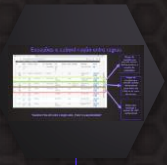
“Laços de tempo”

Seriam como variáveis porém guardam intervalos de tempo para serem aplicadas em regras

Criação de Rules

“Comandos”

São as regras em si com tudo o que se quer restringir ou liberar considerando ou não as Aliases e Schedules

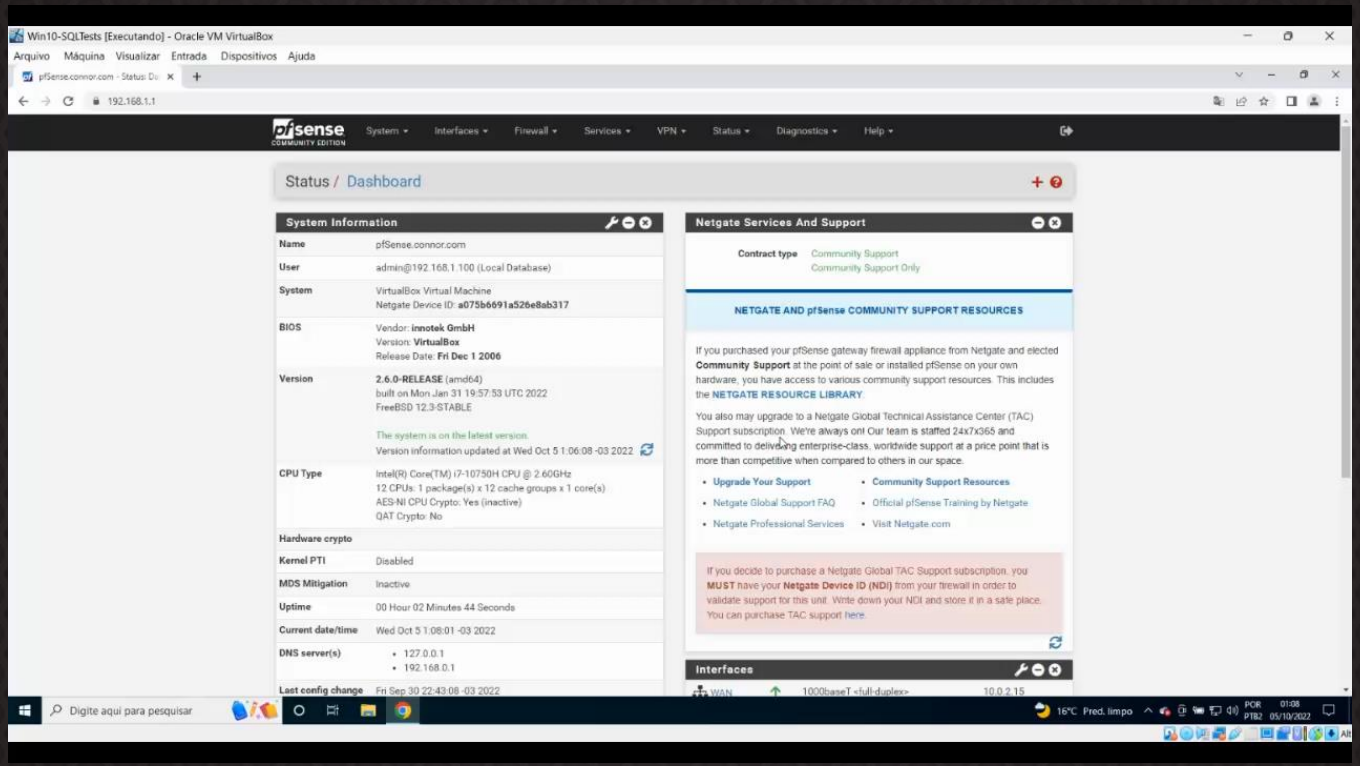


Criação de exceptions

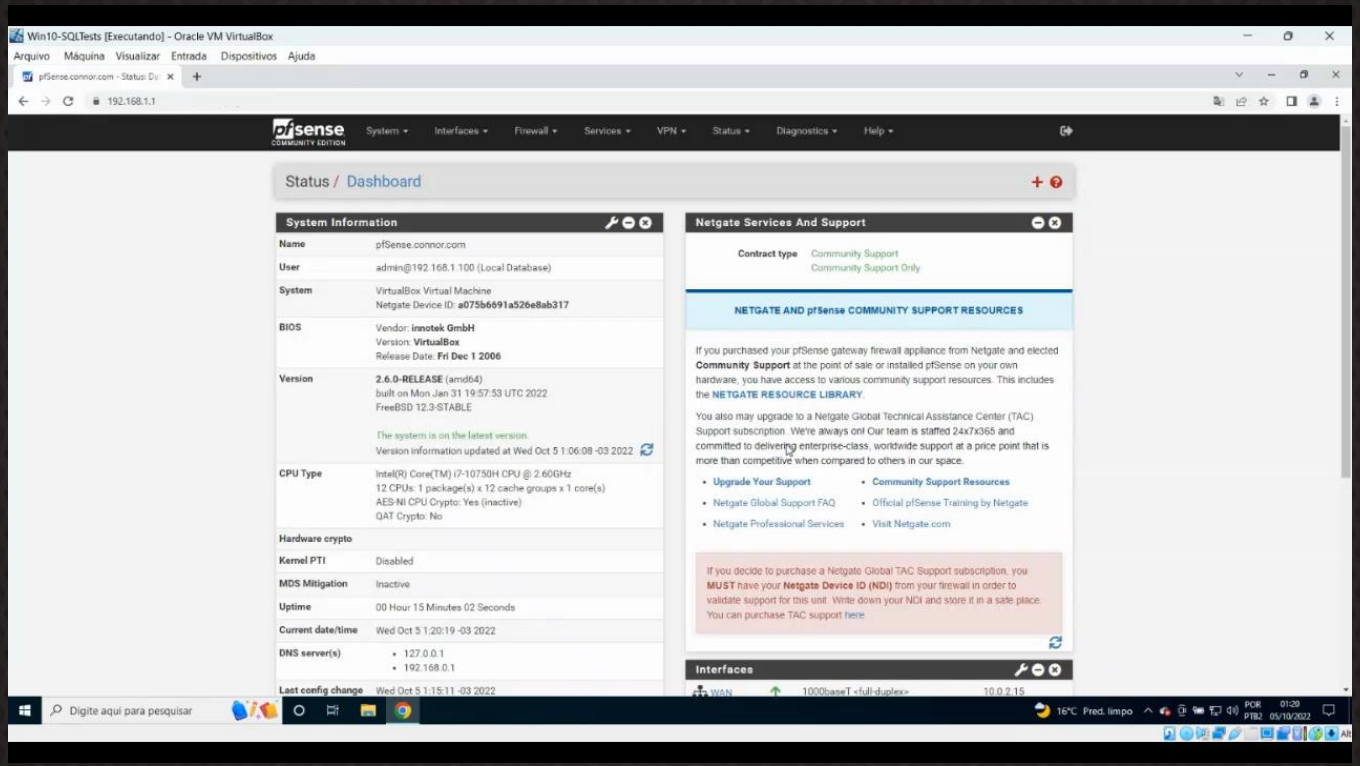
“Exceções”

Controlando a ordem de prioridade entre regras pode-se liberar um site específico pra um IP específico em um horário específico cuja regra subordinada está restringindo, por exemplo

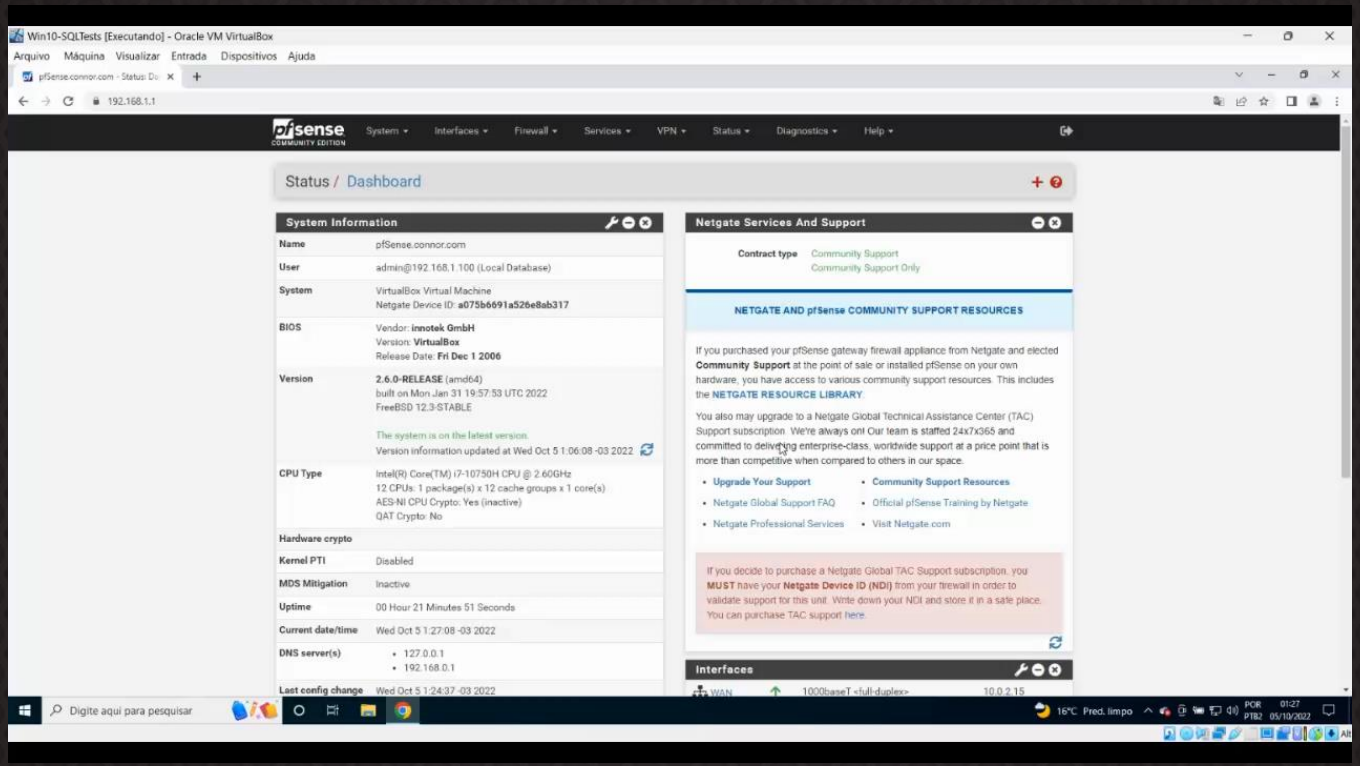
Vídeo criando uma “alias”



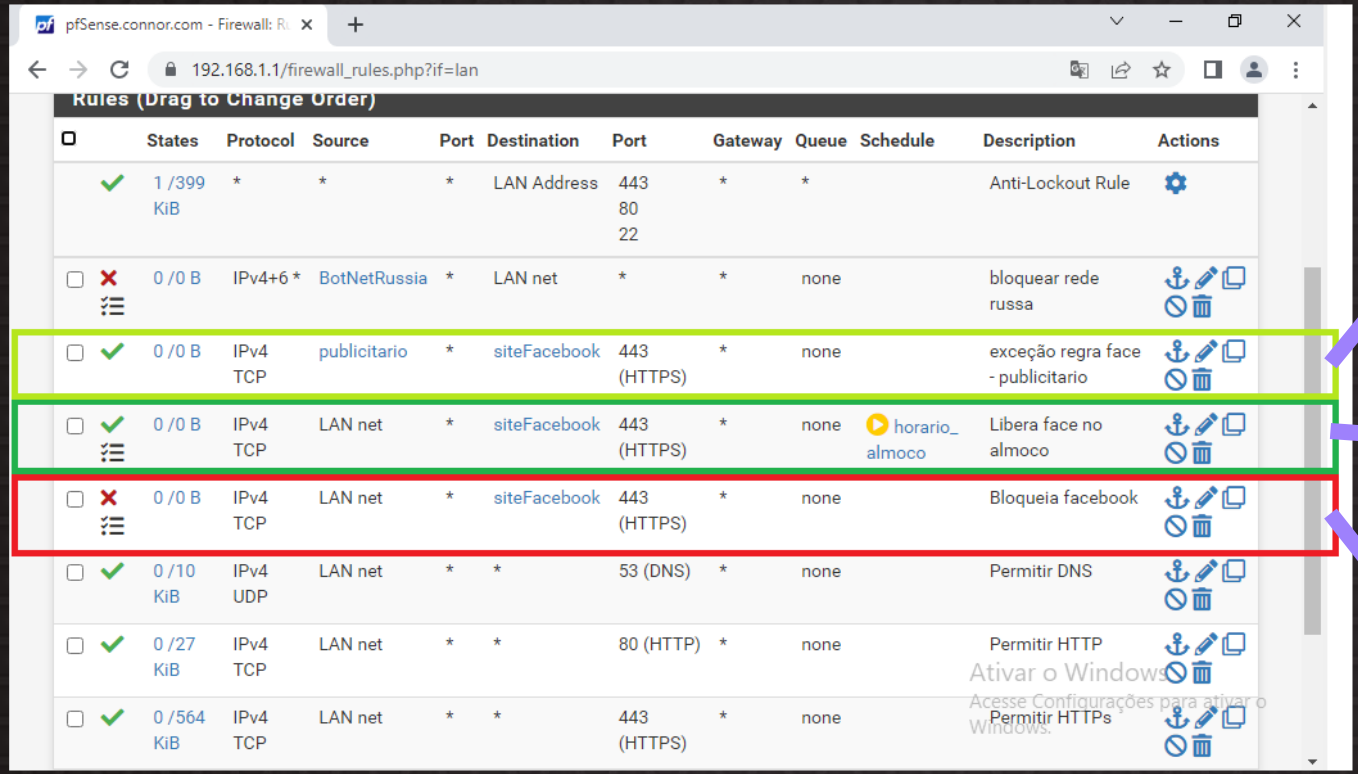
Vídeo criando uma “schedule”



Vídeo criando uma “rule”



Exceções e subordinação entre regras



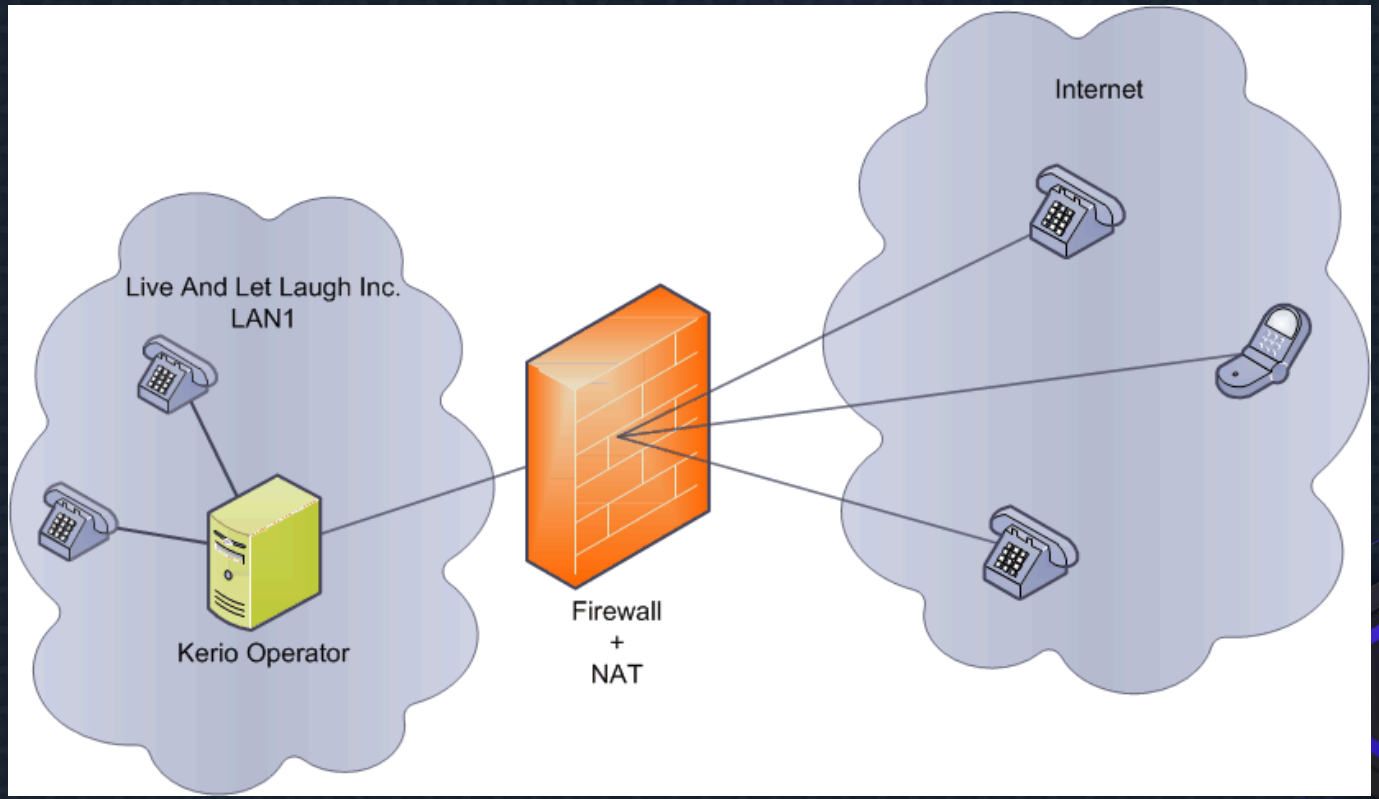
Regra de exceção que permite acesso do facebook se o usuário for publicitário

Regra de exceção que permite acesso do facebook para todos da LAN se for hora do almoço

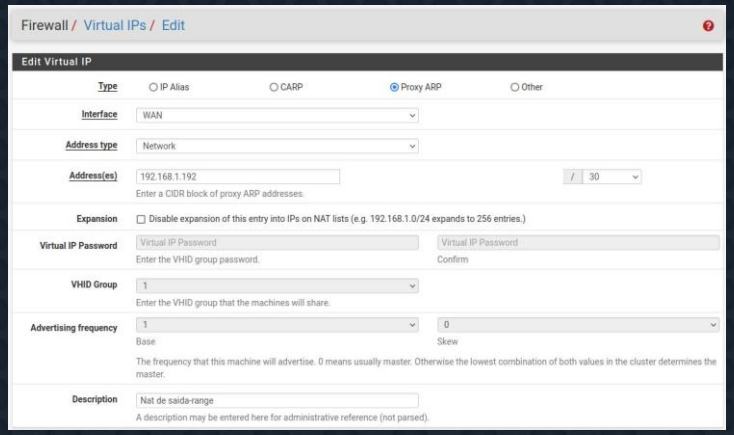
Regra que restringe o acesso da LAN ao facebook

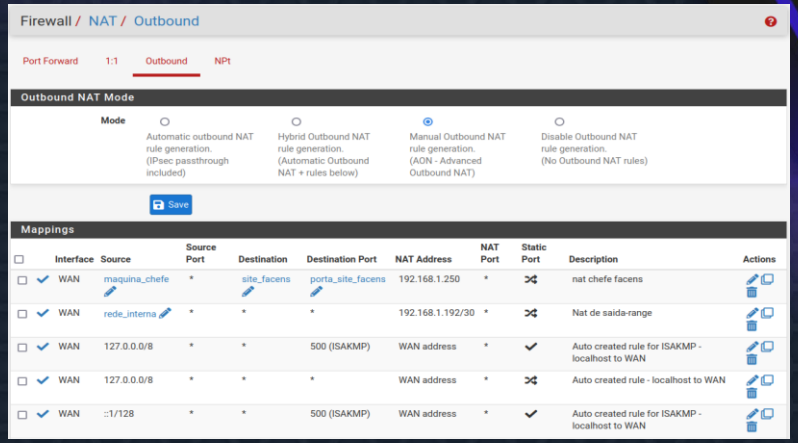
"Quanto mais em cima a regra está, maior a sua prioridade"

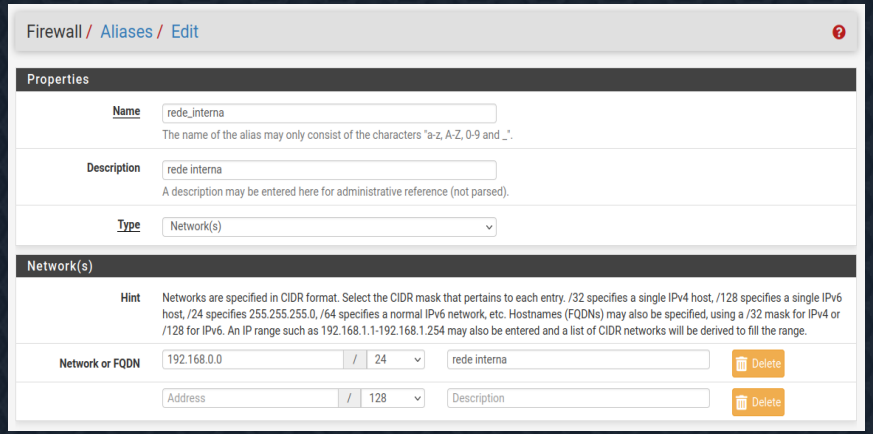
Configurações de NAT



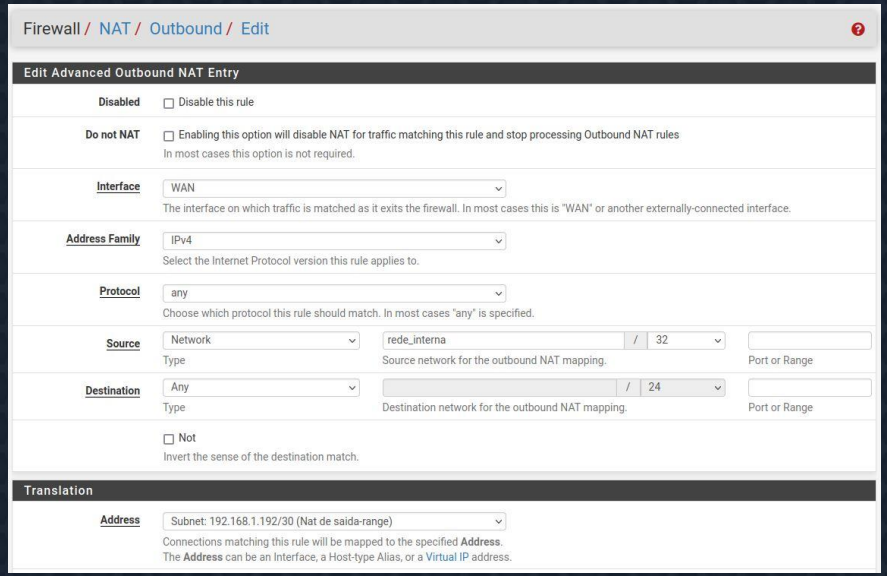
NAT de saída

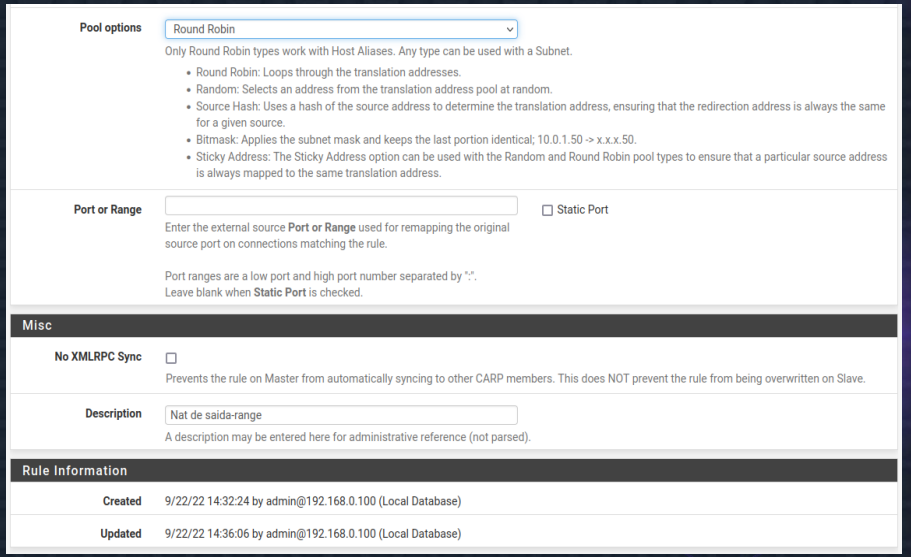

Firewall / Virtual IPs / Edit
Edit Virtual IP
Type
IP Alias
CARP
Proxy ARP
Other
Interface
WAN
Address type
Network
Address(es)
192.168.1.192
/ 30
Enter a CIDR block of proxy ARP addresses.
Expansion
Disable expansion of this entry into IPs on NAT lists (e.g. 192.168.1.0/24 expands to 256 entries.)
Virtual IP Password
Virtual IP Password
Virtual IP Password
Enter the VHID group password.
Confirm
VHID Group
1
Enter the VHID group that the machines will share.
Advertising frequency
1
0
Base
Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.
Description
Nat de saida-range
A description may be entered here for administrative reference (not parsed).


Firewall / NAT / Outbound
Port Forward
1:1
Outbound
NPt
Outbound NAT Mode
Mode
Automatic outbound NAT rule generation. (IPsec passthrough included)
Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
Disable Outbound NAT rule generation. (No Outbound NAT rules)
Save
Mappings
Interface
Source
Source Port
Destination
Destination Port
NAT Address
NAT Port
Static Port
Description
Actions
WAN
maquina_chefe
*
site_facens
porta_site_facens
192.168.1.250
*
nat chefe facens
WAN
rede_interna
*
*
*
192.168.1.192/30
*
Nat de saida-range
WAN
127.0.0.0/8
*
*
500 (ISAKMP)
WAN address
*
Auto created rule for ISAKMP - localhost to WAN
WAN
127.0.0.0/8
*
*
*
WAN address
*
Auto created rule - localhost to WAN
WAN
::1/128
*
*
500 (ISAKMP)
WAN address
*
Auto created rule for ISAKMP - localhost to WAN

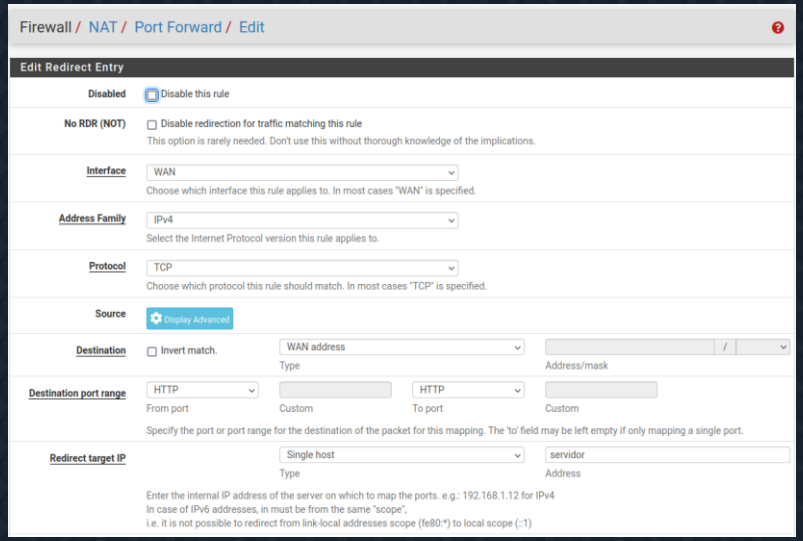

Firewall / Aliases / Edit
Properties
Name
rede_interna
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description
rede interna
A description may be entered here for administrative reference (not parsed).
Type
Network(s)
Network(s)
Hint
Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.
Network or FQDN
192.168.0.0
/ 24
rede interna
Delete
Address
/ 128
Description
Delete

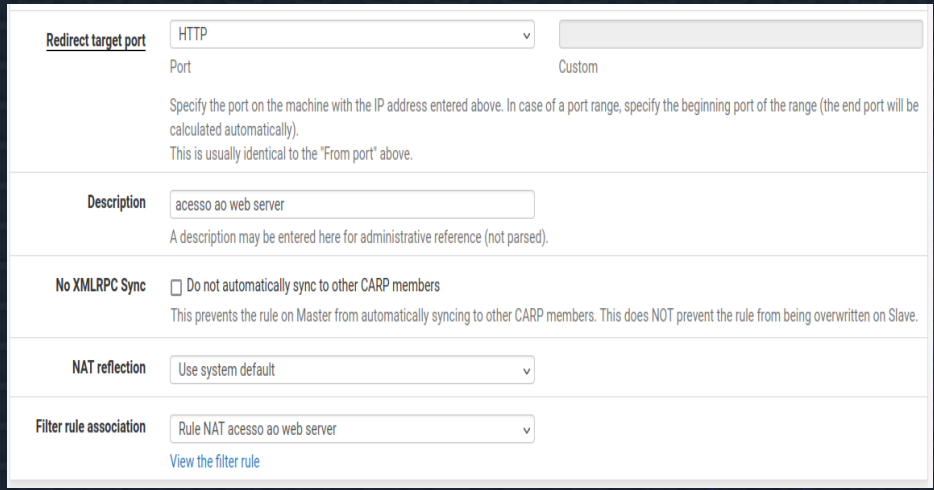
NAT de saída


Firewall / NAT / Outbound / Edit
Edit Advanced Outbound NAT Entry
Disabled
Disable this rule
Do not NAT
Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.
Interface
WAN
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
any
Choose which protocol this rule should match. In most cases "any" is specified.
Source
Network
rede_interna
/ 32
Type
Source network for the outbound NAT mapping.
Port or Range
Destination
Any
/ 24
Type
Destination network for the outbound NAT mapping.
Port or Range
Not
Invert the sense of the destination match.
Translation
Address
Subnet: 192.168.1.192/30 (Nat de saida-range)
Connections matching this rule will be mapped to the specified Address.
The Address can be an Interface, a Host-type Alias, or a Virtual IP address.


Pool options
Round Robin
Only Round Robin types work with Host Aliases. Any type can be used with a Subnet.
Round Robin: Loops through the translation addresses.
Random: Selects an address from the translation address pool at random.
Source Hash: Uses a hash of the source address to determine the translation address, ensuring that the redirection address is always the same for a given source.
Bitmask: Applies the subnet mask and keeps the last portion identical; 10.0.1.50 -> x.x.x.50.
Sticky Address: The Sticky Address option can be used with the Random and Round Robin pool types to ensure that a particular source address is always mapped to the same translation address.
Port or Range
Static Port
Enter the external source Port or Range used for remapping the original source port on connections matching the rule.
Port ranges are a low port and high port number separated by ":".
Leave blank when Static Port is checked.
Misc
No XMLRPC Sync
Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
Description
Nat de saida-range
A description may be entered here for administrative reference (not parsed).
Rule Information
Created
9/22/22 14:32:24 by admin@192.168.0.100 (Local Database)
Updated
9/22/22 14:36:06 by admin@192.168.0.100 (Local Database)

NAT – Port Forward





NAT - Estático 1x1

Firewall / NAT / 1:1 / Edit

Edit NAT 1:1 Entry

Disabled — Disable this rule
When disabled, the rule will not have any effect.

No BINAT (NOT) — Do not perform binat for the specified address
Excludes the address from a later, more general, rule.

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

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

External subnet IP — Type: Single host; Address: 192.168.1.250
Enter the external (usually on a WAN) subnet's starting address or interface for the 1:1 mapping.

Internal IP — Not: Invert the sense of the match. Type: Single host; Address/mask: 192.168.0.102
Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.

Destination — Not: Invert the sense of the match. Type: Any; Address/mask:
The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually "Any".

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

Protocol — TCP
Choose which IP protocol this rule should match.

Source

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

Destination

Destination — Invert match: Single host or alias; 192.168.0.102

Destination Port Range — From: any; Custom: ; To: any; Custom:
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

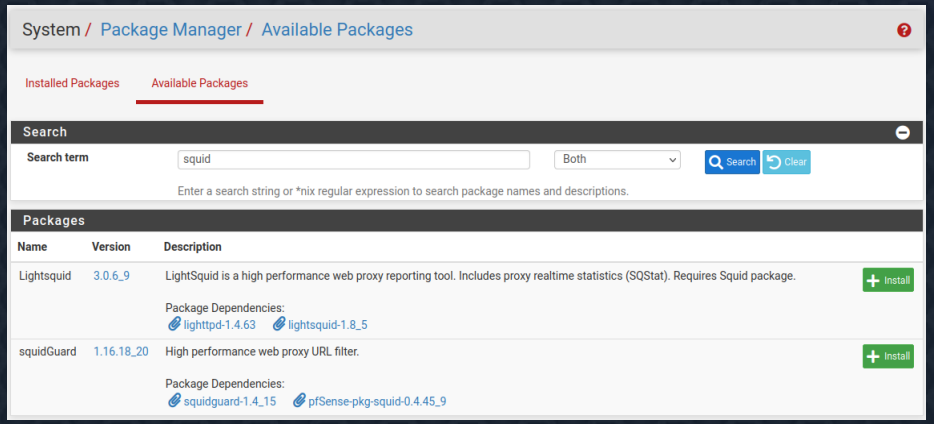
Extra Options

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

Description — permitir acesso ao servidor interno
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

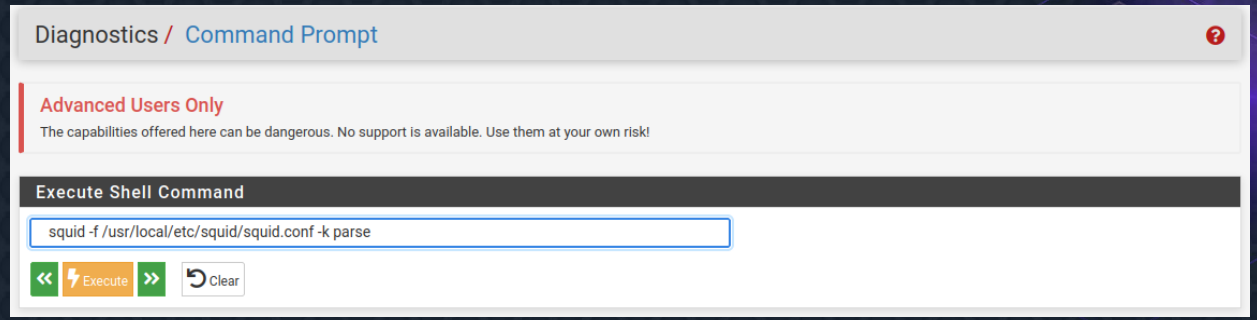
Advanced Options — Display Advanced

Configurações de Proxy



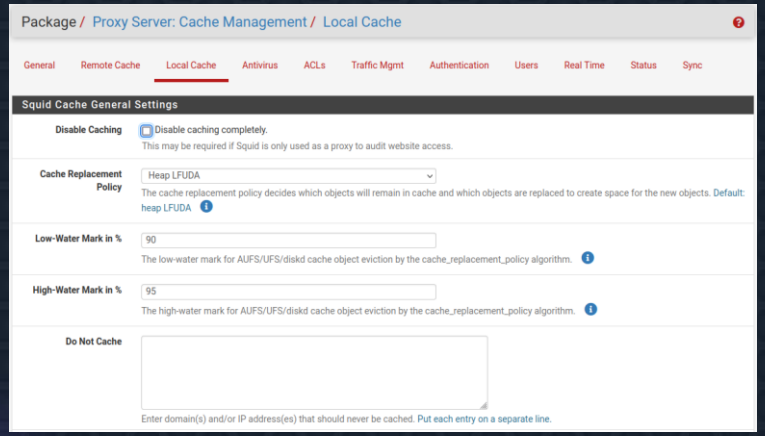
É necessário fazer a criação do cache, para isso se utiliza o comando via prompt

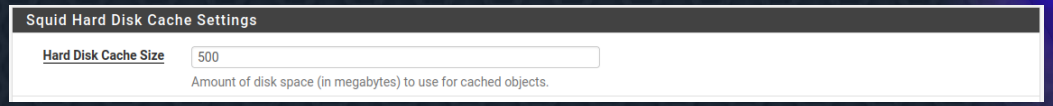
Comand Prompt: squid -f /usr/local/etc/squid/squid.conf -k parse

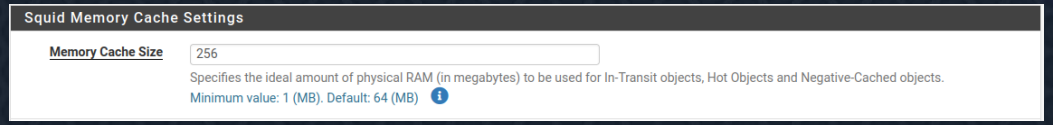


Cache Local

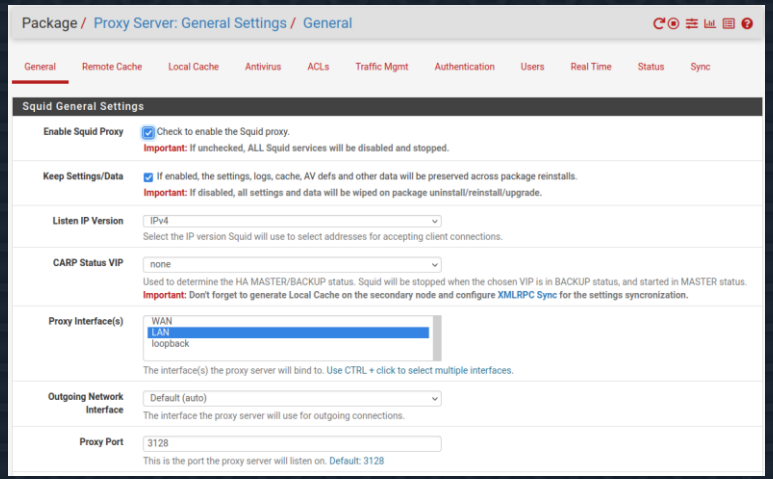
Configuração rápida para o cache local



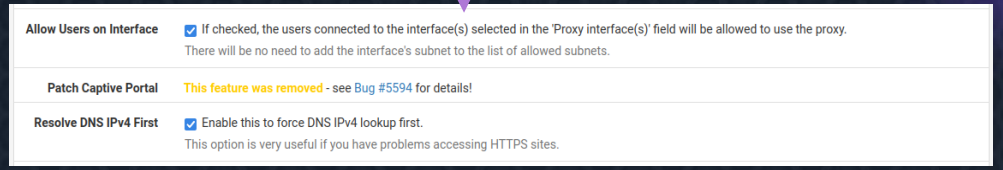


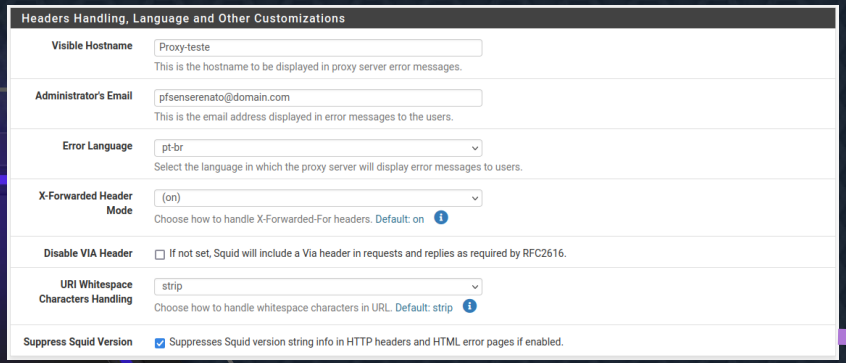


Configuração do Squid

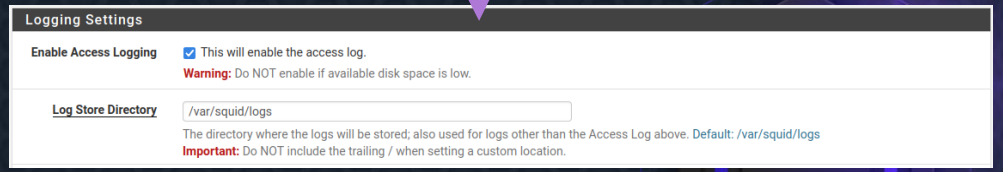


1) Permite que usuários na rede se conectem sem solicitação,no caso usuários da rede LAN
2) Caso o tráfego esteja lento prioriza tráfego IPV4



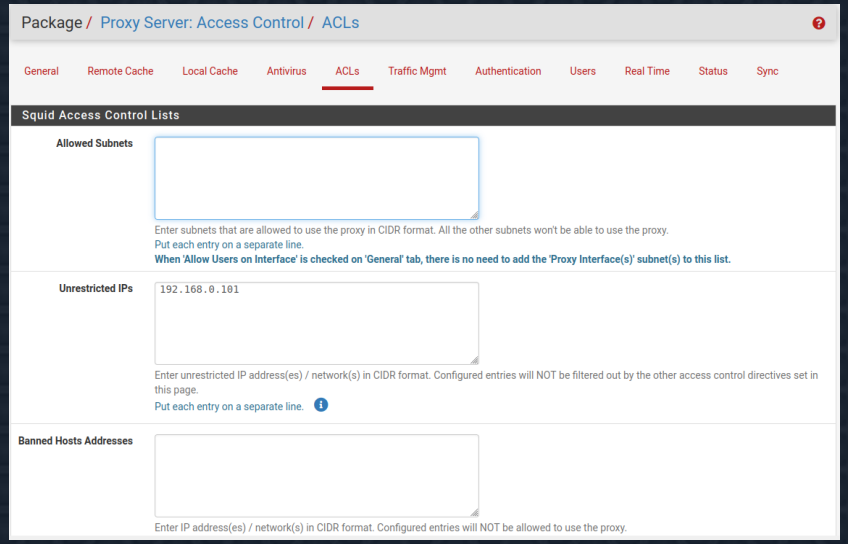


Habilita Log de Acessos

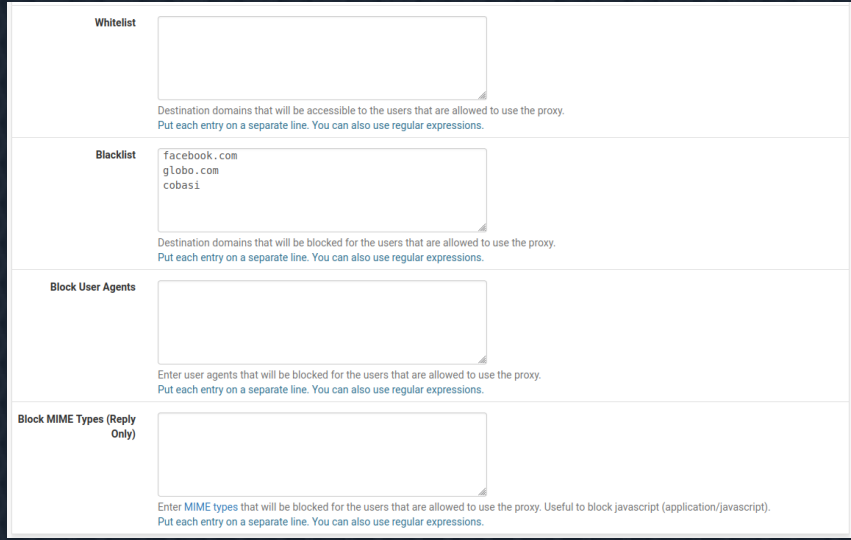


Suppress Squid Version deve estar habilitado para não enviar informações sobre a versão do Squid

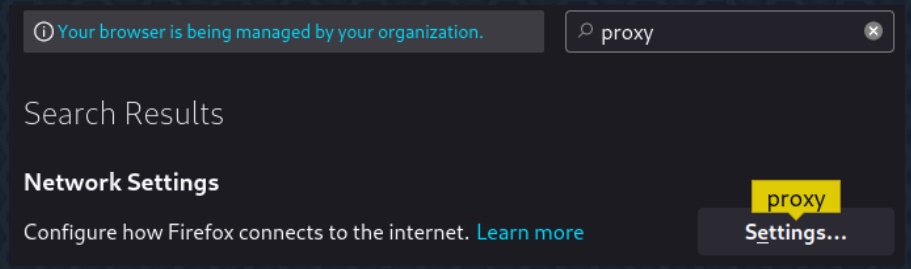
ACL – Access Control List



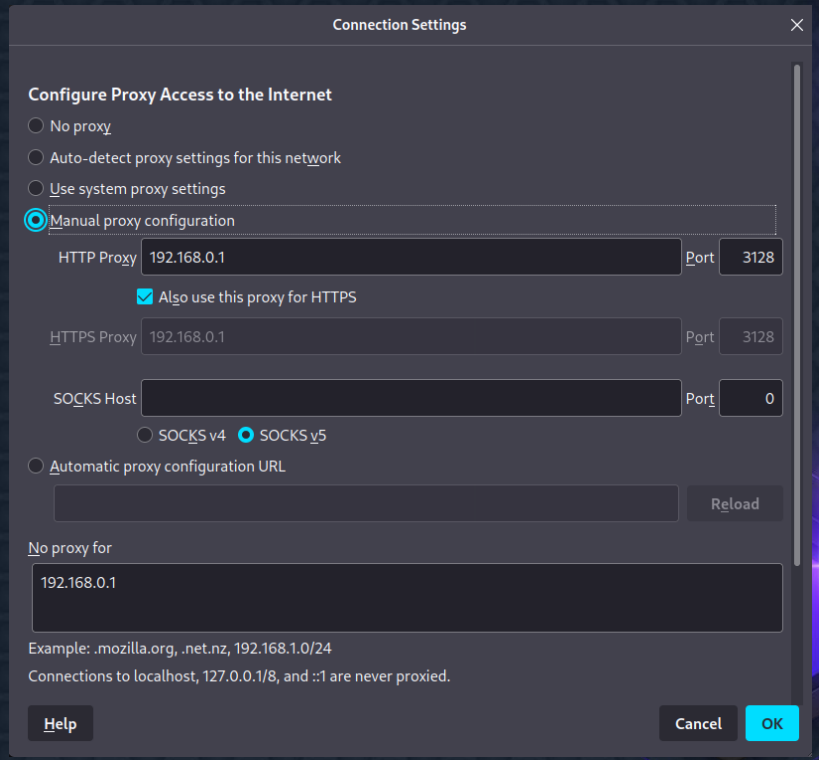
1) Permite IPs de outras redes
2) IPs que não serão filtrados na rede
3) IPs Banidos
4) Acessos permitidos
5) Acessos negados
6) Bloqueia agentes do usuário. Ex:Browser do android
7) Bloqueia tipos de Arquivos. Ex: .exe. ..js



Instalação do proxy não transparente no browser



- Seleciona a configuração manual;
- Adiciona o IP do proxy e a porta;
- Habilita também com HTTPS;
- Em, no proxy for, adiciona o IP novamente do proxy para que ele não filtre a página web do mesmo.



Página de Erro

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://www.facebook.com/

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

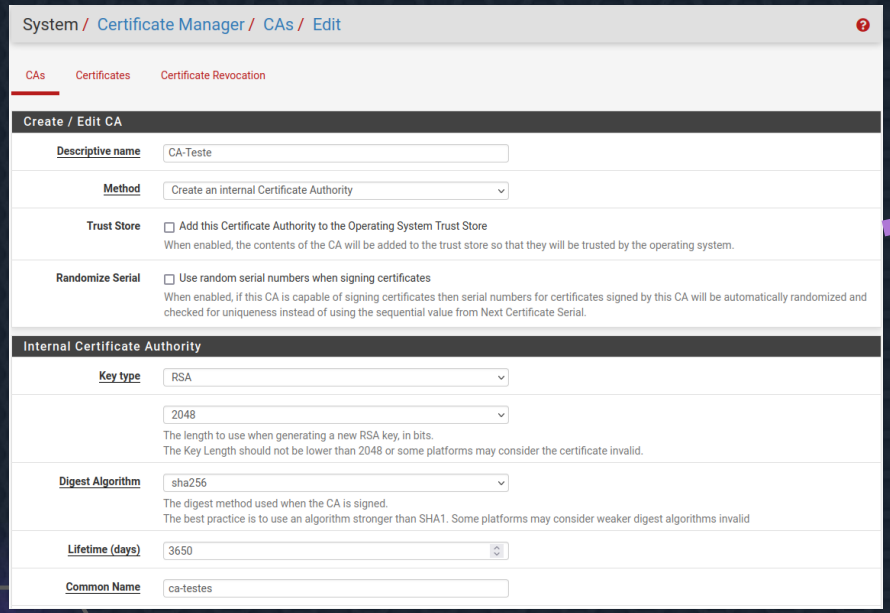
Your cache administrator is pfsenserenato@domain.com.

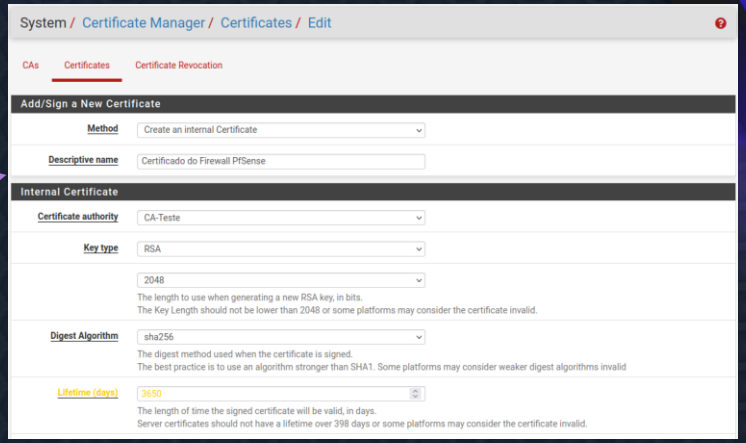
Generated Sun, 02 Oct 2022 19:39:49 GMT by Proxy-teste (squid)

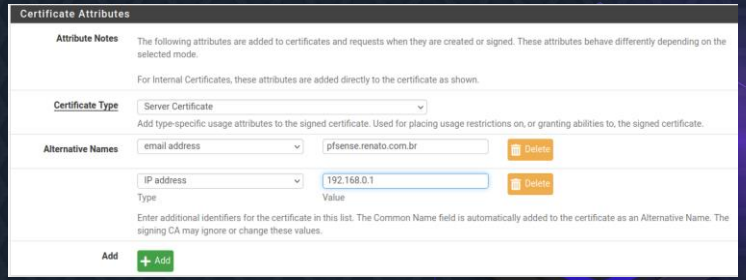
Interceptação de tráfego com SSL

SSL (Secure Sockets Layer) técnica que permite entender os dados que são enviados criptografados quando utilizado o HTTPS. Basicamente, consiste em se passar pelo site que o cliente irá realizar o acesso. Isso é feito através da emissão de um certificado digital.

Certificado Digital

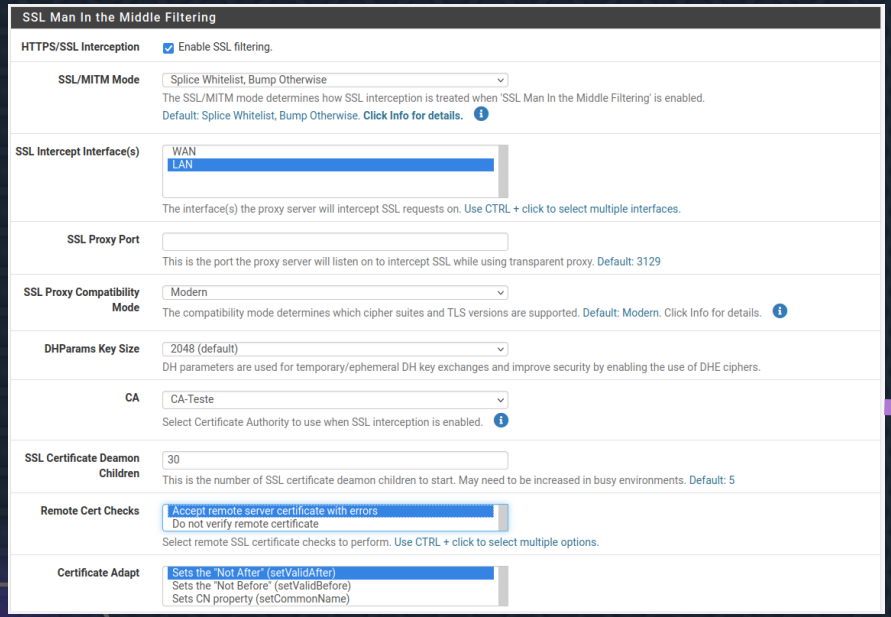




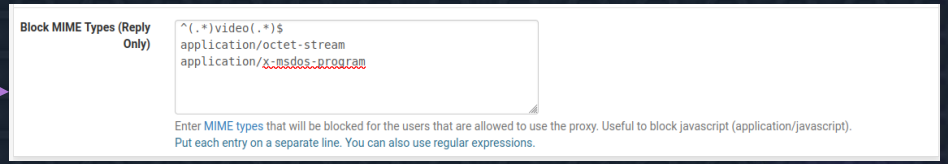


Para instalar o certificado é necessário exportá-lo no menu CA e depois é preciso instalar o mesmo no diretório de certificados da sua máquina, ou então instalar em seu browser

Interceptação de tráfego com SSL

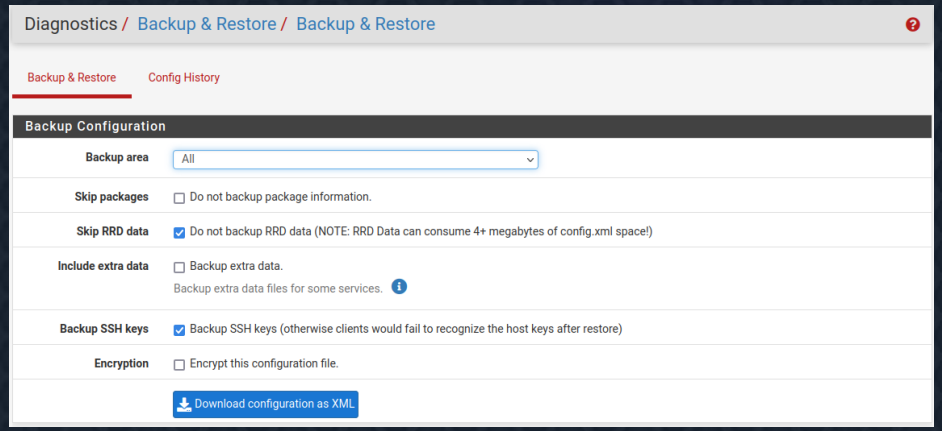


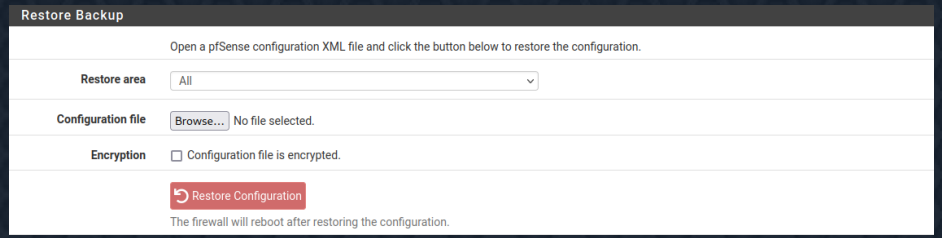
Depois do certificado ser instalado.
Na parte das ACLs, em Block MIMES podemos adicionar as MIMES que irão bloquear um determinado arquivo de ser exibido através do proxy, como no exemplo abaixo, arquivos .exe e arquivos de vídeo.



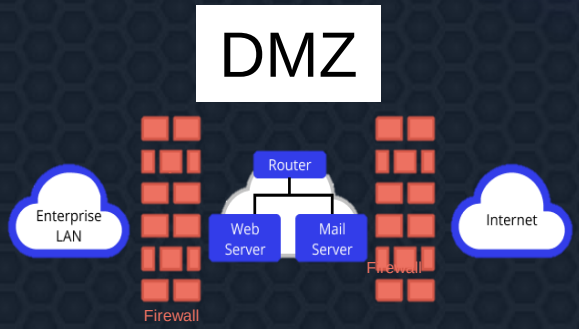
Dessa forma conseguimos fazer a conexão SSL de forma criptografada em qualquer site através do proxy

Backup e Restauração





Outras Aplicações



SquidGuard

Cloud PfSense

Activity Director

OPENVPN

Vamos exercitar?

Exercício Prático

O reitor de uma universidade solicitou a liberação do acesso a alguns sites para o computador do publicitário da instituição: www.instagram.com; www.facens.br e www.facebook.com. A equipe de TI prontamente deve seguir para a criação de uma *alias* para a máquina do “publicitário” a fim de desenvolver uma *rule* que permita que este host tenha acesso privilegiado sobre as demais *rules* para que somente ele consiga acessar tais domínios. Outro problema é que nos últimos meses reparou-se um descontrolável acesso ao www.tiktok.com em horário comercial por parte de todos funcionários, portanto é necessário à todos da rede o bloqueio de acesso a esse site entre as 08:00 e 12:00 hrs e entre as 13:00 e 18:00 hrs. Além disso, alguns fãs de uma universidade concorrente com más intenções, construíram uma rede de botnets com o objetivo de infectar a rede interna da Facens para posterior furto de dados, se faz necessário o bloqueio da mesma.

Algumas referências

Playlist Cavalcante Treinamentos:
https://youtube.com/playlist?list=PLQ7gVTPc8Kmij4-2RpiQMAQjkj3XkolGI

Mesmo curso da playlist anterior porém com certificado:
https://www.learncafe.com/cursos/curso-completo---como-instalar-e-configurar-o-pfsense

Playlist do canal “Luciano Rodrigues”:
https://www.youtube.com/playlist?list=PLFajyb7NamFDsGaj09kdTHX3T9GMPTNA0

Playlist do canal “Bora pra Prática”:
https://youtube.com/playlist?list=PLozhsZB1lLUN7vHnCDA2NF6rMfTBs-vAs

Curso oficial para certificação:
https://www.netgate.com/training/pfsense-fundamentals-and-advanced-application

THANK YOU!

Gelson Filho

Renato Junior

Facens

lenovo

Connor