

Workshop – Projeto Connor

# Firewall UTM



Gelson Filho



Renato Junior



# 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, Switch, 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) ...

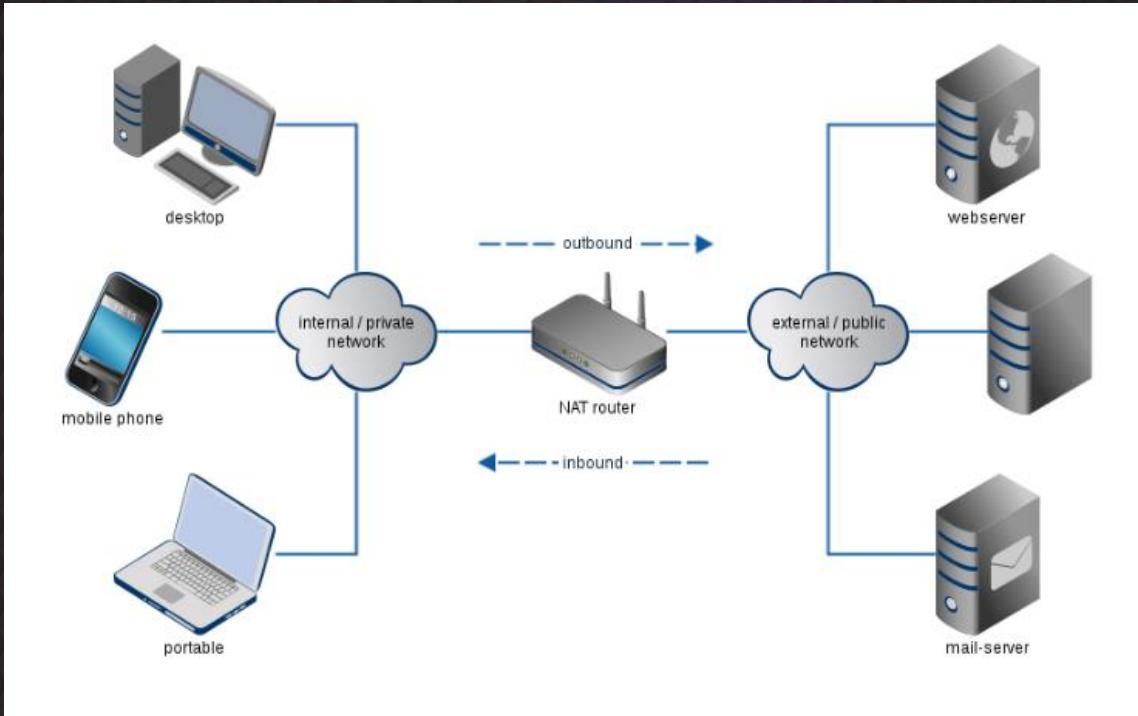
SSL - TLS

TCP - UDP

IPV4 - IPV6

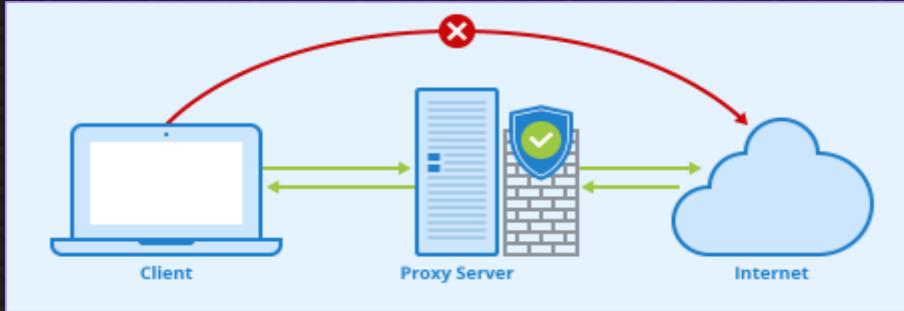
\* Em parênteses a porta do serviço a ser transportado conforme a camada de transporte (via UDP ou TCP) segundo a IANA

# 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:

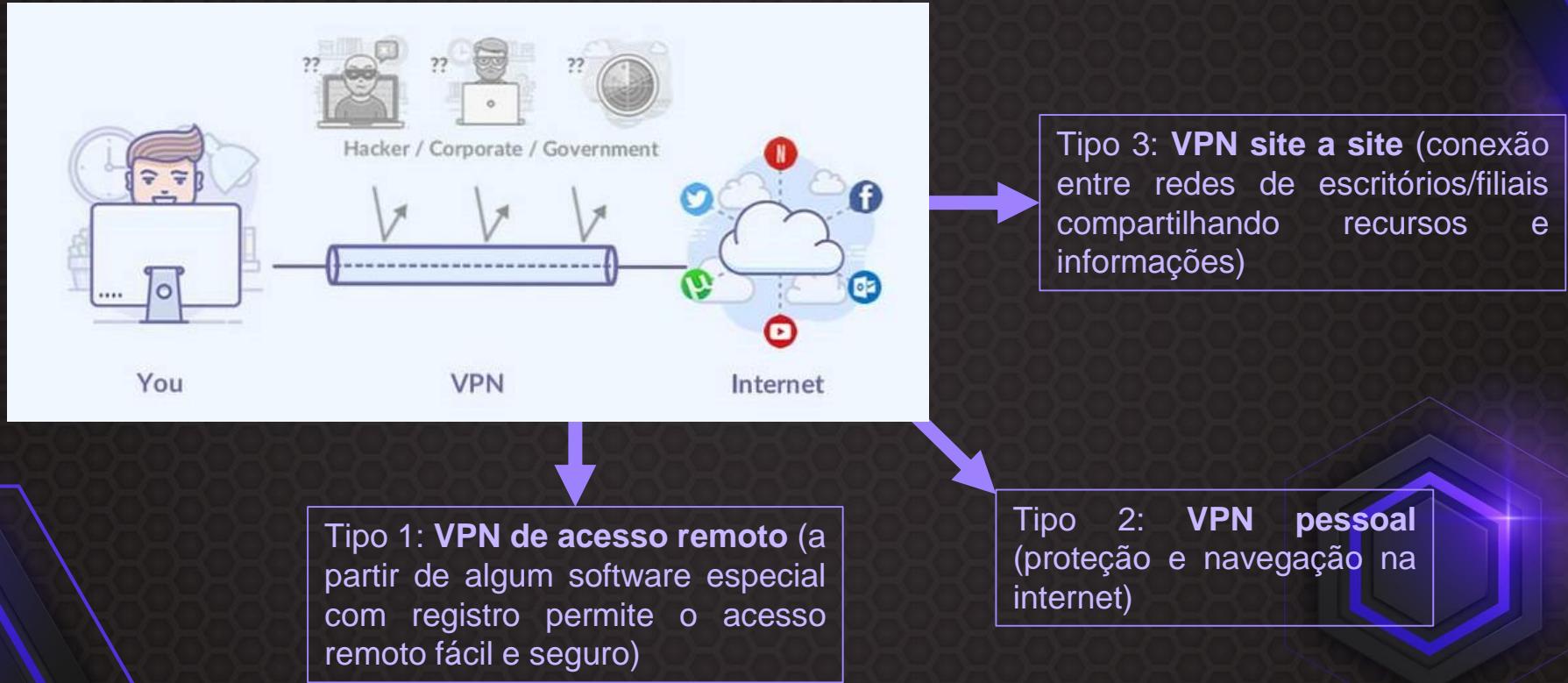
- **Transparente** (não dificulta autenticações de usuário – usuário nem sabe que ele existe)
- **Não transparente** (normal – o que tem que configurar no navegador)

- Problema em https – tráfego 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-length do http, expressões regulares, horário, porta TCP/UDP, login de usuário, etc)

# VPN – Virtual Private Network

“Túnel criptografado para envio/recebimento de informações”



# 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)

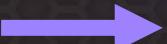
Tipo 2: **Proxy Services**  
(Firewall de aplicação)

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

**pf**sense®



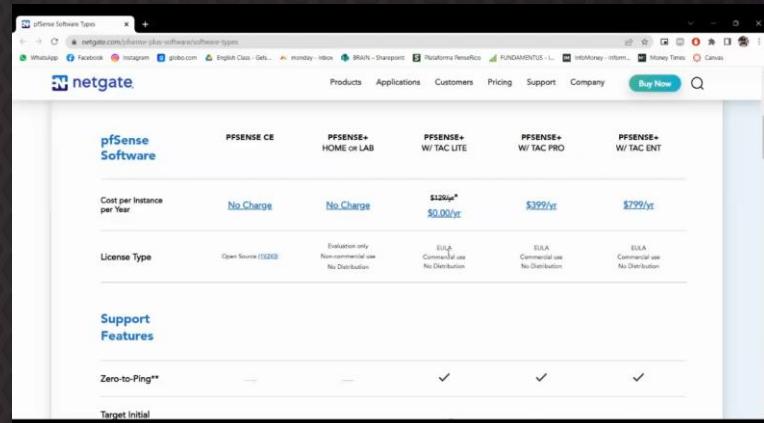
# UTM





- 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:



A screenshot of a web browser showing the pfSense software licensing page on netgate.com. The page compares five versions: pfSense Software, pfSense CE, pfSense+ HOME or LAB, pfSense+ WiTAC LITE, pfSense+ WiTAC PRO, and pfSense+ WiTAC ENT. It details the cost per instance per year and the license type (Open Source or EULA). The pfSense+ versions include support features like Zero-to-Ping\*\* and Target-Initial.

pfSense Software	pfSense CE	pfSense+ HOME or LAB	pfSense+ WiTAC LITE	pfSense+ WiTAC PRO	pfSense+ WiTAC ENT
Cost per Instance per Year	No Charge	No Charge	\$1299*	\$399/yr	\$799/yr
License Type	Open Source (BSD)	Evaluation only Non-commercial use No Distribution	EULA Commercial use No Distribution	EULA Commercial use No Distribution	EULA Commercial use No Distribution
Support Features					
Zero-to-Ping**	—	—	✓	✓	✓
Target-Initial					

# Configurações de rede na VM

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

# 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

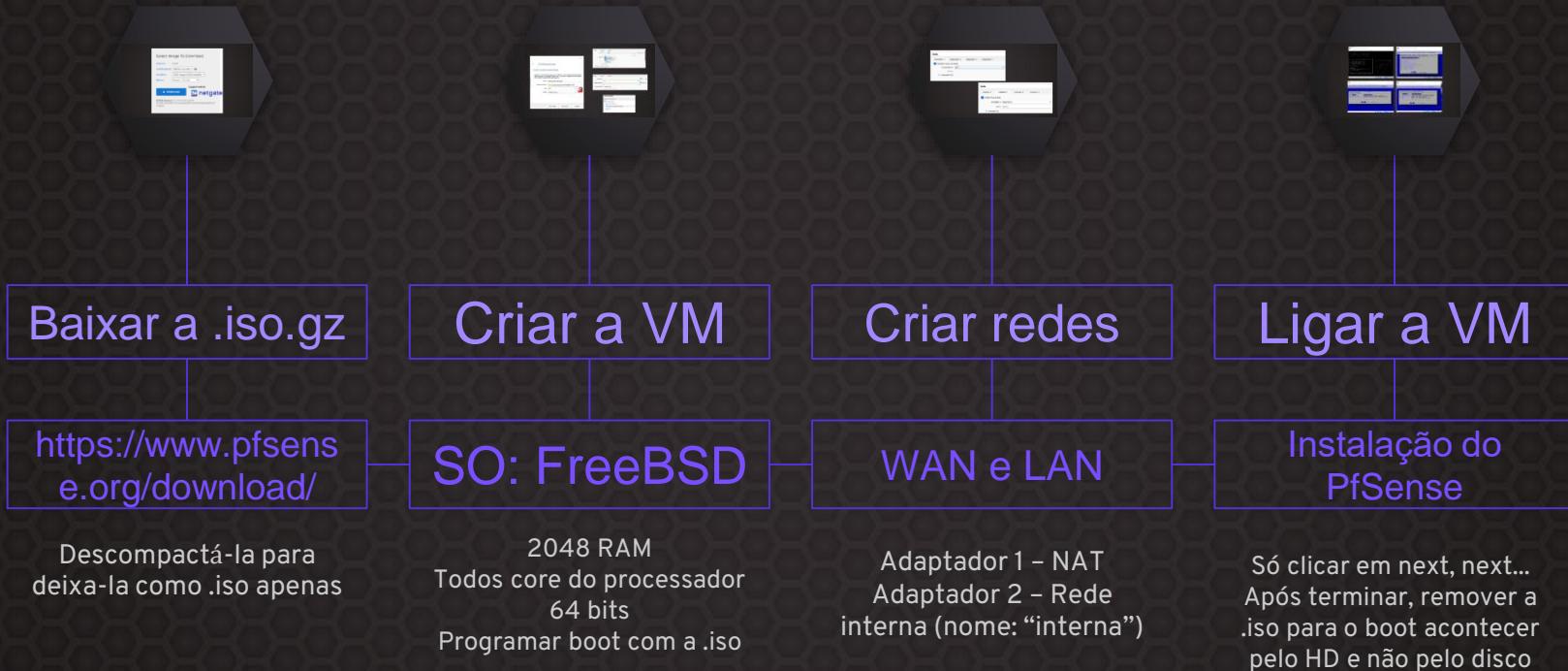
# Vamos praticar um pouco?



Mãos na massa!



# Instalação e Configuração



## Select Image To Download

Version: 2.6.0

Architecture: AMD64 (64-bit) 

Installer: DVD Image (ISO) Installer

Mirror: Austin, TX USA

Supported by

 DOWNLOAD



[SHA256 Checksum](#) for compressed (.gz) file:

941a68c7f20c4b635447cceda429a027f816bdb78d54b8252bb87abf  
1fc22ee3

## Criar Máquina Virtual

### Nome e Sistema Operacional

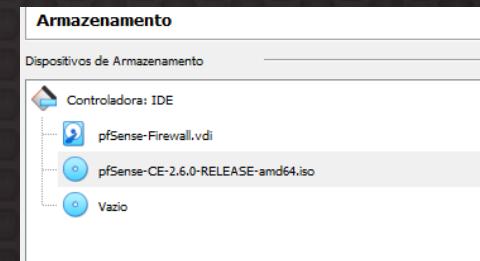
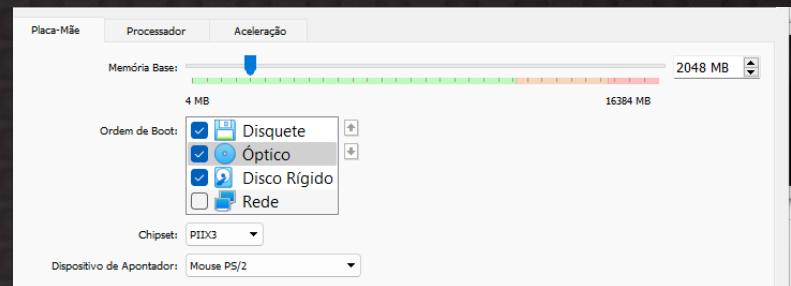
Escolha um nome descriptivo para a nova máquina virtual e selecione o tipo de sistema operacional que você pretende instalar nela. O nome que você escolher será utilizado pelo VirtualBox para identificar esta máquina.

Nome:

Pasta da Máquina:

Tipo:  

Versão:



## 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

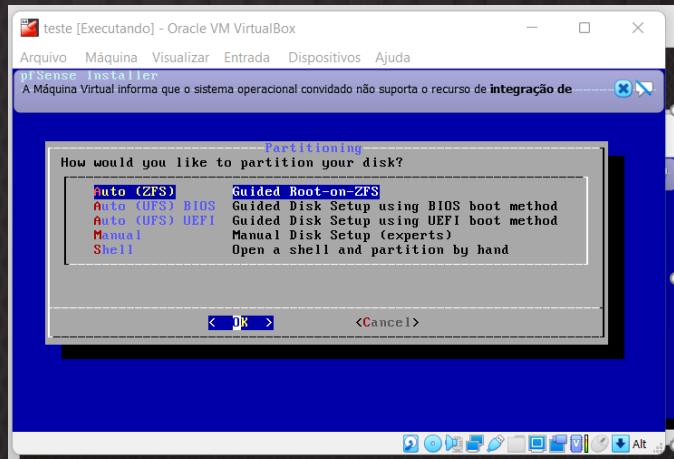
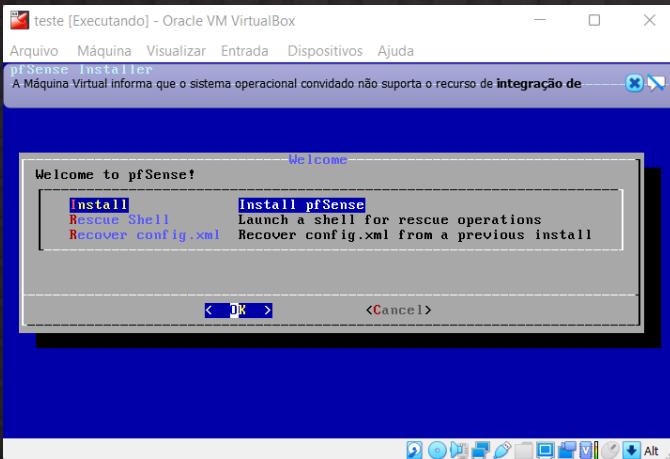
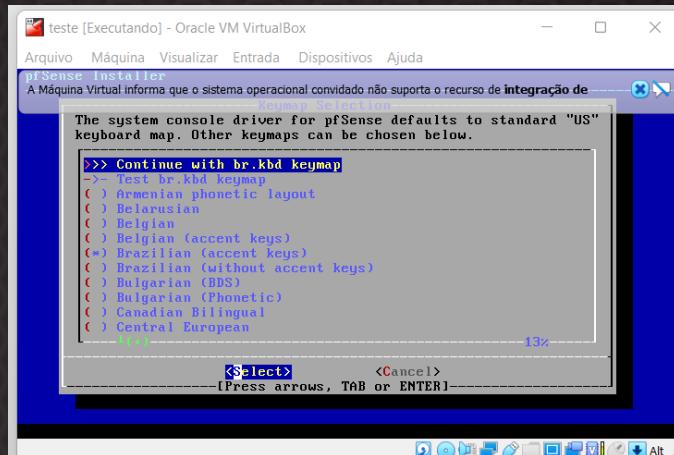
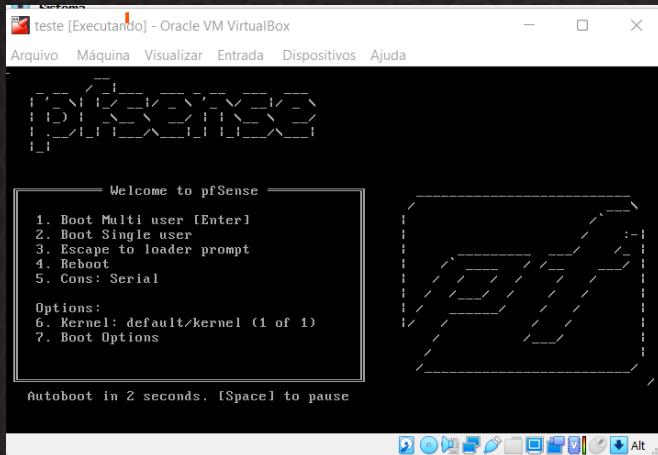
Adaptador 4

Habilitar Placa de Rede

Conectado a: Rede Interna

Nome: Interna

► Avançado (D)



# Funções da Console (CLI)

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSensefw ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.9/24
LAN (lan)      -> em1          -> v4: 192.168.0.1/24

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

Enter an option: █
```

# 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

Status / Dashboard

+ ? -

### Available Widgets

- + Captive Portal Status
- + Gateways
- + Interfaces
- + OpenVPN
- + Services Status
- + Traffic Graphs
- + CARP Status
- + GEOM Mirror Status
- + IPsec
- + Picture
- + Squid Antivirus Status
- + Wake-on-Lan
- + Dynamic DNS Status
- + Installed Packages
- + Netgate Services And Support
- + RSS
- + System Information
- + Firewall Logs
- + Interface Statistics
- + NTP Status
- + S.M.A.R.T. Status
- + Thermal Sensors

Other dashboard settings are available from the [General Setup](#) page.

System Information	
Name	pfSensereno(pfSense.renato.com.br)
User	admin@192.168.0.100 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 9bb9ba3ff33a219ef5c8
BIOS	Vendor: innoteck GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.6.0-R-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
<p>The system is on the latest version. Version information updated at Sun Oct 2 17:54:59 -03 2022</p>	
CPU Type	Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2 CPUs: 1 package(s) x 2 cache groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

Interfaces	
WAN	1000baseT <full-duplex> 192.168.1.4
LAN	1000baseT <full-duplex> 192.168.0.1

- 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

Hardware crypto			
Kernel PTI	Disabled		
MDS Mitigation	Inactive		
Uptime	03 Hours 32 Minutes 36 Seconds		
Current date/time	Sun Oct 2 19:12:07 -03 2022		
DNS server(s)	<ul style="list-style-type: none"><li>• 127.0.0.1</li><li>• 8.8.4.4</li><li>• 8.8.8.8</li></ul>		
Last config change	Sun Oct 2 18:54:35 -03 2022		
State table size	0% (72/403000) <a href="#">Show states</a>		
MBUF Usage	0% (3026/1000000)		
Load average	0.58, 0.50, 0.48		
CPU usage	<div style="width: 1%;">1%</div>		
Memory usage	<div style="width: 11%;">11%</div> of 4031 MiB		
SWAP usage	0% of 1024 MiB		
Disks			
Mount	Used	Size	Usage
> /	734M	13G	<div style="width: 6%; background-color: #00ff00;">6%</div> of 13G (zfs)

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



# Vídeo criando uma “alias”

The screenshot shows the pfSense Community Edition interface running on a Windows 10 host. The main window displays the 'Status / Dashboard' page. On the left, there's a sidebar with various links like 'System', 'Interfaces', 'Firewall', etc. The main content area is divided into sections: 'System Information' (listing details such as Name: pfSense.connor.com, User: admin@192.168.1.100, System: VirtualBox Virtual Machine, BIOS: Intel(R) Core(TM) i7-7500U CPU @ 2.60GHz, Version: 2.6.0-RELEASE (amd64), CPU Type: Intel(R) Core(TM) i7-7500U CPU @ 2.60GHz, and Uptime: 00 Hour 02 Minutes 44 Seconds), 'Netgate Services And Support' (Contract type: Community Support Only), and 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES'. The bottom of the screen shows a taskbar with icons for File Explorer, Task View, Control Panel, and a browser window.

**Status / Dashboard**

**System Information**

Name	pfSense.connor.com
User	admin@192.168.1.100 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: a075b6691a526e8ab317
BIOS	Vendor: innostek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
CPU Type	Intel(R) Core(TM) i7-7500U CPU @ 2.60GHz 12 CPUs: 1 package(s) x 12 cache @ groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 02 Minutes 44 Seconds
Current date/time	Wed Oct 5 1:06:08 -03 2022
DNS server(s)	+ 127.0.1 + 192.168.0.1
Last config change	Fri Sep 30 22:43:08 -03 2022

**Netgate Services And Support**

Contract type: Community Support Only

**NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES**

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x65 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).

**Interfaces**

WAN: 1000baseT <full-duplex> 10.0.2.15  
16°C Pred. limpo 01:06 POR P782 05/10/2022

# Vídeo criando uma “schedule”

The screenshot shows the pfSense Status / Dashboard page. The left sidebar lists various system components and their details:

- Name:** pfSense.connor.com
- User:** admin@192.168.1.100 (Local Database)
- System:** VirtualBox Virtual Machine  
Netgate Device ID: a075b6691a526e8ab317
- BIOS:** Vendor: innoteck GmbH  
Version: VirtualBox  
Release Date: Fri Dec 1 2006
- Version:** 2.6.0-RELEASE (amdf4)  
built on Mon Jan 31 19:57:53 UTC 2022  
FreeBSD 12.3-STABLE
- CPU Type:** Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz  
12 CPUs: 1 package(s) x 12 cache groups x 1 core(s)  
AES-NI CPU Crypto: Yes (inactive)  
QAT Crypto: No
- Hardware crypto:** None
- Kernel PTI:** Disabled
- MDS Mitigation:** Inactive
- Uptime:** 00 Hour 15 Minutes 02 Seconds
- Current date/time:** Wed Oct 5 1:06:08 -03 2022
- DNS server(s):** 127.0.1.1, 192.168.0.1
- Last config change:** Wed Oct 5 1:15:11 -03 2022

The right sidebar contains sections for Netgate Services And Support and Netgate and pfSense Community Support Resources.

**Netgate Services And Support:**

- Contract type: Community Support  
Community Support Only

**NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES:**

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

**Interfaces:**

- WAN: 1000baseT <full-duplex>, 10.0.2.15
- IP: 192.168.0.1
- Temperature: 16°C
- Date: Wed Oct 5 1:06:08 -03 2022

# Vídeo criando uma “rule”

The screenshot shows the pfSense Status / Dashboard interface. On the left, there is a sidebar titled "System Information" containing various hardware and software details. In the center, there is a "Netgate Services And Support" section with a "Community Support Only" contract type. Below this, there is a "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" section with links to upgrade support, community resources, and professional services. At the bottom, there is a "Interfaces" section showing network configuration for the WAN port.

**System Information**

- Name: pfSense.connor.com
- User: admin@192.168.1.100 (Local Database)
- System: VirtualBox Virtual Machine  
Netgate Device ID: a075b6691a526e8ab317
- BIOS: Vendor: innostek GmbH  
Version: VirtualBox  
Release Date: Fri Dec 1 2006
- Version: 2.6.0-RELEASE (amdf4)  
built on Mon Jan 31 19:57:53 UTC 2022  
FreeBSD 12.3-STABLE
- CPU Type: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz  
12 CPUs: 1 package(s) x 12 cache @ groups x 1 core(s)  
AES-NI CPU Crypto: Yes (inactive)  
QAT Crypto: No
- Hardware crypto
- Kernel PTI: Disabled
- MDS Mitigation: Inactive
- Uptime: 00 Hour 21 Minutes 51 Seconds
- Current date/time: Wed Oct 5 1:27:08 -03 2022
- DNS server(s): 127.0.1  
192.168.0.1
- Last config change: Wed Oct 5 1:24:37 -03 2022

**Netgate Services And Support**

Contract type: Community Support  
Community Support Only

**NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES**

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x65 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).

**Interfaces**

WAN: 1000baseT <full-duplex> 10.0.2.15  
16°C Pred. limpo 01:27 POR P782 05/10/2022

# Exceções e subordinação entre regras

#	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1 /399 KiB	*	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
✗ 0 /0 B 	IPv4+6	*	BotNetRussia	*	LAN net	*	*	*	none	bloquear rede russa	
✗ 0 /0 B 	IPv4 TCP		publicitario	*	siteFacebook	443 (HTTPS)	*	none		exceção regra face - publicitario	
✗ 0 /0 B 	IPv4 TCP		LAN net	*	siteFacebook	443 (HTTPS)	*	none	horario_almoco	Libera face no almoco	
✗ 0 /0 B 	IPv4 TCP		LAN net	*	siteFacebook	443 (HTTPS)	*	none		Bloqueia facebook	
✓ 0 /10 KiB	IPv4 UDP		LAN net	*	*	53 (DNS)	*	none		Permitir DNS	
✓ 0 /27 KiB	IPv4 TCP		LAN net	*	*	80 (HTTP)	*	none		Permitir HTTP Ativar o Windows	
✓ 0 /564 KiB	IPv4 TCP		LAN net	*	*	443 (HTTPS)	*	none		Acesse Configurações para ativar o Permitir HTTPS Windows.	

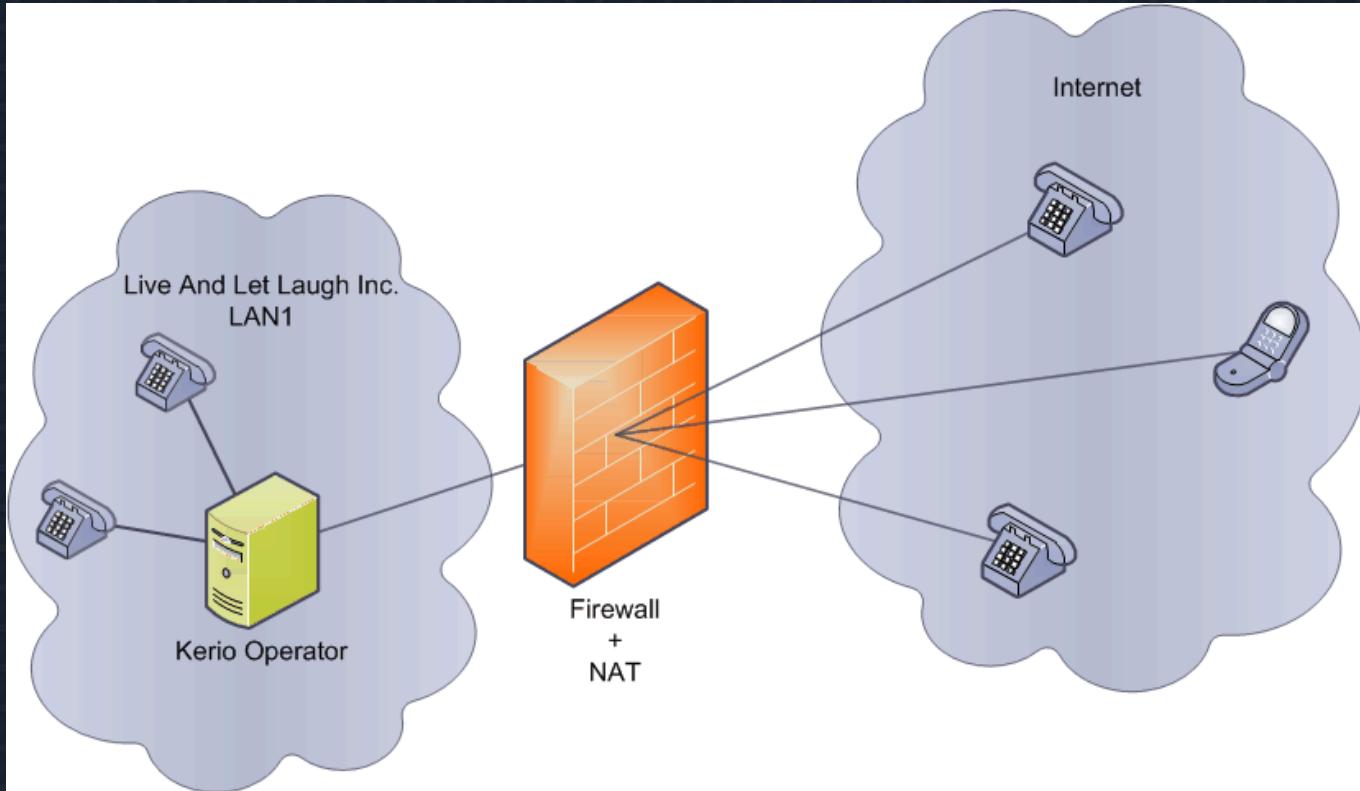
Regra de exceção que permite acesso do facebook se o usuário for publicitário

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

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: Enter the VHD group password.

VHD Group: 1

Advertising frequency: 1 Base 0 Skew

Description: Nat de saída-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 saída-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	
Address:	/ 128	Description:		

# 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  
Source network for the outbound NAT mapping.  
Type: Subnet

**Destination** Any / 24  
Destination network for the outbound NAT mapping.  
Type: Subnet

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

Firewall / NAT / Port Forward / Edit

**Edit Redirect Entry**

**Disabled**  Disable this rule

**No RDR (NOT)**  Disable redirection for traffic matching this rule  
This option is rarely needed. Don't use this without thorough knowledge of the implications.

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

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

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

**Source** [Display Advanced](#)

**Destination**  Invert match. **WAN address**  Type  Address/mask

**Destination port range** **HTTP** From port  To port   
Custom Custom

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

**Redirect target IP** **Single host**  **servidor** **Type**  **Address**

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, it must be from the same "scope",  
i.e. it is not possible to redirect from link-local addresses scope (fe80\*) to local scope (::1)

**Redirect target port** **HTTP** **Port**  **Custom**

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).  
This is usually identical to the "From port" above.

**Description**  acesso ao web server  
A description may be entered here for administrative reference (not parsed).

**No XMLRPC Sync**  Do not automatically sync to other CARP members  
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

**NAT reflection**  Use system default

**Filter rule association** Rule NAT acesso ao web server  View the filter rule

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

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

**External subnet IP**    
Type Address  
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 Address/mask  
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 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**  Select the Internet Protocol version this rule applies to.

**Protocol**  Choose which IP protocol this rule should match.

**Source**

**Source**  Invert match   /

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   /   
**Destination Port Range**  From  To   
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**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**   
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

System / Package Manager / Available Packages

Installed Packages Available Packages

Search term: squid

Enter a search string or \*nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
Lightsquid	3.0.6_9	Lightsquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SOStat). Requires Squid package.
		Package Dependencies: lighttpd-1.4.63 lightsquid-1.8_5
squidGuard	1.16.18_20	High performance web proxy URL filter.
		Package Dependencies: squidguard-1.4_15 pfSense-pkg-squid-0.4.45_9

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

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

Diagnostics / Command Prompt

Advanced Users Only  
The capabilities offered here can be dangerous. No support is available. Use them at your own risk!

Execute Shell Command

```
squid -f /usr/local/etc/squid/squid.conf -k parse
```

« Execute » Clear

# Cache Local

## Configuração rápida para o cache local

Package / Proxy Server: Cache Management / Local Cache

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

**Squid Cache General Settings**

**Disable Caching**  Disable caching completely.  
This may be required if Squid is only used as a proxy to audit website access.

**Cache Replacement Policy** Heap LFUDA  
The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. Default: heap LFUDA [i](#)

**Low-Water Mark in %** 90  
The low-water mark for AUFS/UFS/diskd cache object eviction by the cache\_replacement\_policy algorithm. [i](#)

**High-Water Mark in %** 95  
The high-water mark for AUFS/UFS/diskd cache object eviction by the cache\_replacement\_policy algorithm. [i](#)

**Do Not Cache**  
Enter domain(s) and/or IP address(es) that should never be cached. Put each entry on a separate line.

**Squid Hard Disk Cache Settings**

**Hard Disk Cache Size** 500  
Amount of disk space (in megabytes) to use for cached objects.

**Squid Memory Cache Settings**

**Memory Cache Size** 256  
Specifies the ideal amount of physical RAM (in megabytes) to be used for In-Transit objects, Hot Objects and Negative-Cached objects.  
Minimum value: 1 (MB). Default: 64 (MB) [i](#)

# Configuração do Squid

Package / Proxy Server: General Settings / General

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

### Squid General Settings

**Enable Squid Proxy**  Check to enable the Squid proxy.  
**Important:** If unchecked, ALL Squid services will be disabled and stopped.

**Keep Settings/Data**  If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.  
**Important:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

**Listen IP Version** IPv4  
Select the IP version Squid will use to select addresses for accepting client connections.

**CARP Status VIP** none  
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.  
**Important:** Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.

**Proxy Interface(s)** WAN LAN loopback  
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

**Outgoing Network Interface** Default (auto)  
The interface the proxy server will use for outgoing connections.

**Proxy Port** 3128  
This is the port the proxy server will listen on. Default: 3128

### Headers Handling, Language and Other Customizations

**Visible Hostname** proxy-teste  
This is the hostname to be displayed in proxy server error messages.

**Administrator's Email** pfsenserato@domain.com  
This is the email address displayed in error messages to the users.

**Error Language** pt-br  
Select the language in which the proxy server will display error messages to users.

**X-Forwarded Header Mode** on  
Choose how to handle X-Forwarded-For headers. Default: on

**Disable VIA Header**  If not set, Squid will include a Via header in requests and replies as required by RFC2616.

**URI Whitespace Characters Handling** strip  
Choose how to handle whitespace characters in URL. Default: strip

**Suppress Squid Version**  Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

- 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

**Allow Users on Interface**  If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.  
There will be no need to add the interface's subnet to the list of allowed subnets.

**Patch Captive Portal** This feature was removed - see Bug #5594 for details!

**Resolve DNS IPv4 First**  Enable this to force DNS IPv4 lookup first.  
This option is very useful if you have problems accessing HTTPS sites.

Habilita Log de Acessos

### Logging Settings

**Enable Access Logging**  This will enable the access log.  
**Warning:** Do NOT enable if available disk space is low.

**Log Store Directory** /var/squid/logs  
The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs  
**Important:** Do NOT include the trailing / when setting a custom location.

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

# ACL – Access Control List

Package / Proxy Server: Access Control / ACLs

General Remote Cache Local Cache Antivirus **ACLs** Traffic Mgmt Authentication Users Real Time Status Sync

**Squid Access Control Lists**

**Allowed Subnets**

Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy.  
Put each entry on a separate line.

When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.

**Unrestricted IPs**

192.168.0.101

Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page.  
Put each entry on a separate line. [i](#)

**Banned Hosts Addresses**

Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy.

- 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

**Whitelist**

Destination domains that will be accessible to the users that are allowed to use the proxy.  
Put each entry on a separate line. You can also use regular expressions.

**Blacklist**

facebook.com  
globo.com  
cobasi

Destination domains that will be blocked for the users that are allowed to use the proxy.  
Put each entry on a separate line. You can also use regular expressions.

**Block User Agents**

Enter user agents that will be blocked for the users that are allowed to use the proxy.  
Put each entry on a separate line. You can also use regular expressions.

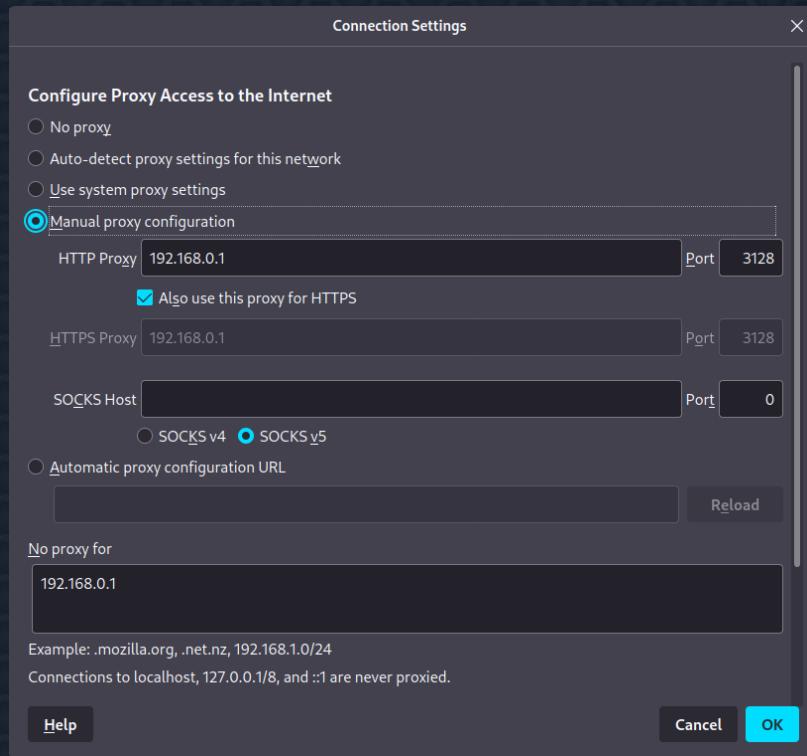
**Block MIME Types (Reply Only)**

Enter MIME types that will be blocked for the users that are allowed to use the proxy. Useful to block javascript (application/javascript).  
Put each entry on a separate line. You can also use regular expressions.

# Instalação do proxy não transparente no browser

A screenshot of the Firefox Network Settings page. At the top, a message says "Your browser is being managed by your organization." Below it is a search bar with "proxy". The main section is titled "Network Settings" with the subtitle "Configure how Firefox connects to the internet." A "Learn more" link is present. A yellow box highlights the "Settings..." button next to the "proxy" label. The "proxy" label is also highlighted with a yellow box.

- 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 [pfsensereno@domain.com](mailto:pfsensereno@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



System / Certificate Manager / CAs / Edit

**CAs**   **Certificates**   **Certificate Revocation**

**Create / Edit CA**

**Descriptive name**: CA-Teste

**Method**: Create an internal Certificate Authority

**Trust Store**:  Add this Certificate Authority to the Operating System Trust Store  
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

**Randomize Serial**:  Use random serial numbers when signing certificates  
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

**Internal Certificate Authority**

**Key type**: RSA

**2048**: The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

**Digest Algorithm**: sha256  
The digest method used when the CA is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

**Lifetime (days)**: 3650

**Common Name**: ca-testes



System / Certificate Manager / Certificates / Edit

**CAs**   **Certificates**   **Certificate Revocation**

**Add/Sign a New Certificate**

**Method**: Create an internal Certificate

**Descriptive name**: Certificado do Firewall PFSense

**Internal Certificate**

**Certificate authority**: CA-Teste

**Key type**: RSA

**2048**: The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

**Digest Algorithm**: sha256  
The digest method used when the certificate is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

**Lifetime (days)**: 3650  
The length of time the signed certificate will be valid, in days.  
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

**Certificate Attributes**

**Attribute Notes**: The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.  
For Internal Certificates, these attributes are added directly to the certificate as shown.  
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

**Certificate Type**: Server Certificate

**Alternative Names**:  

email address	pfSense.renato.com.br	
IP address	192.168.0.1	

  
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

**Add**

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

SSL Man In the Middle Filtering

HTTPS/SSL Interception  Enable SSL filtering.

SSL/MITM Mode  The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled. Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#)

SSL Intercept Interface(s)  WAN  LAN  
The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

SSL Proxy Port  This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

SSL Proxy Compatibility Mode  The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. [Click Info for details.](#)

DHParams Key Size  DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA  Select Certificate Authority to use when SSL interception is enabled.

SSL Certificate Daemon Children  This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5

Remote Cert Checks   Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.

Certificate Adapt



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.

Block MIME Types (Reply Only)

```
^(.*)video(.*)$  
application/octet-stream  
application/x-msdos-program
```

Enter MIME types that will be blocked for the users that are allowed to use the proxy. Useful to block javascript (application/javascript). Put each entry on a separate line. You can also use regular expressions.

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

# Backup e Restauração

Diagnostics / Backup & Restore / Backup & Restore

Backup & Restore Config History

### Backup Configuration

Backup area: All

Skip packages:  Do not backup package information.

Skip RRD data:  Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)

Include extra data:  Backup extra data.  
Backup extra data files for some services. ⓘ

Backup SSH keys:  Backup SSH keys (otherwise clients would fail to recognize the host keys after restore)

Encryption:  Encrypt this configuration file.

[Download configuration as XML](#)

### Restore Backup

Open a pfSense configuration XML file and click the button below to restore the configuration.

Restore area: All

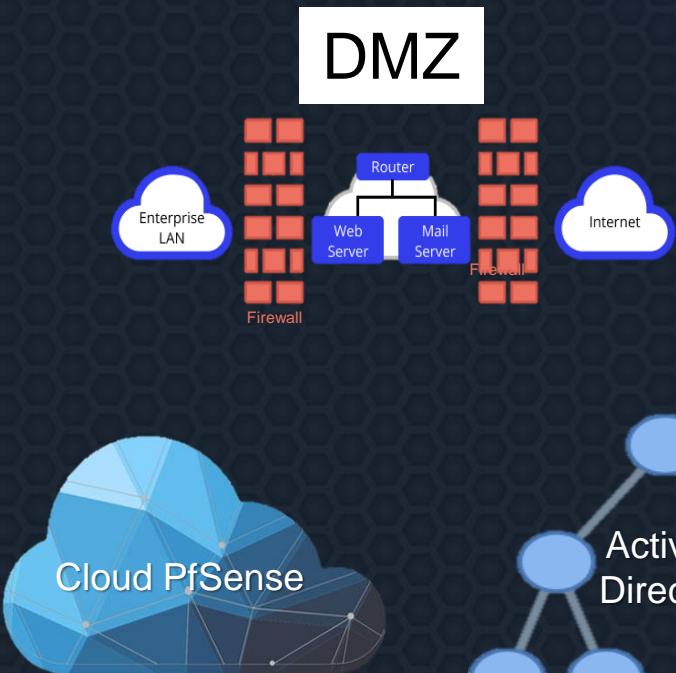
Configuration file:  No file selected.

Encryption:  Configuration file is encrypted.

[Restore Configuration](#)

The firewall will reboot after restoring the configuration.

# Outras Aplicações



# 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](http://www.instagram.com); [www.facens.br](http://www.facens.br) e [www.facebook.com](http://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](http://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=PLozhsZB1ILUN7vHnCDA2NF6rMfTBs-vAs>

**Curso oficial para certificação:**

<https://www.netgate.com/training/pfsense-fundamentals-and-advanced-application>



# THANK YOU!



Gelson Filho



Renato Junior

