



**CENTRO UNIVERSITÁRIO**

**INSTITUTO DE EDUCAÇÃO SUPERIOR DE BRASÍLIA - IESB**

**CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO**

**IESB PROJETO INTEGRADOR – IMPLEMENTAÇÃO DE FIREWALL**

Aluno: Diego de Sá Bachega

Professor: Eustáquio Mendes Guimarães

Brasília

Novembro/2018

1.	VERSÕES DO DOCUMENTO .....	3
2.	INTRODUÇÃO.....	3
3.	OBJETIVO .....	3
4.	JUSTIFICATIVA.....	3
5.	DESENVOLVIMENTO .....	4
I.	REDES.....	4
II.	AMBIENTE DE DESENVOLVIMENTO E PRODUÇÃO .....	5
III.	ESTAÇÕES DE TRABALHO .....	11
IV.	FIREWALL – LINHA DE DEFESA .....	16
V.	SERVIDORES.....	22
VI.	SERVIDOR MYSQL + APACHE .....	22
VII.	SERVIDOR FTP .....	25
6	REGISTROS DE LOGS.....	28
7	CONCLUSÃO.....	28
8	REFERÊNCIAS BIBLIOGRÁFICAS.....	29

## 1. Versões do documento

Versão	Data	Autor(es)	Histórico
1.0	21/Setembro/18	Diego	Pré-Projeto
2.0	Outubro/18*	Diego	Preparação do Ambiente Virtual
3.0	Novembro/18*	Diego	Instalação dos Servidores
4.0	Novembro/18*	Diego	Instalação do Firewall
5.0	23/Novembro/18	Diego	Entrega do Projeto

\*Não houve uma data exata, uma vez que o ambiente foi refeito varias vezes.

## 2. Introdução

Este projeto foi desenvolvido em uma máquina comum com processador Intel i7, 8Gb de memória Ram, com capacidade de 1 Tb de armazenamento em HD e um sistema Operacional Windows 10. Para controle, registro e versionamento de documentos e arquivos de configuração foi utilizada uma conta GitHub, link <https://github.com/diegobachega/Projeto-Integrador-Implementacao-de-Seguranca>.

No meio do projeto a máquina utilizada para construção foi substituída devido a falhas no processamento no dispositivo de armazenamento. O ambiente virtual foi migrado para um dispositivo HD Externo em uma máquina virtual instalada em um Intel Dual Core, 4Gb de Ram, com capacidade de 1 Tb, no qual foi finalizada toda arquitetura de rede projetada com um firewall do tipo Pfsense appliance..

## 3. Objetivo

Um Projeto de Segurança da Informação fornece informações essenciais para o gerenciamento da segurança da informação em empresas modernas que estão em constante evolução. Este projeto tem por objetivo a implementação de uma solução de segurança, do tipo Firewall, que pode ser aplicado em uma rede empresarial de pequeno porte para melhorar a proteção dos dados do negócio, reduzir custos com licenças e melhorar a performance da rede.

## 4. Justificativa

Um Firewall consiste em um filtro que controla todas as comunicações que passam de uma rede a outra, permitindo ou negando seu acesso a outra rede. Entre as várias ações de segurança capaz de implementação em um firewall pode-se citar o bloqueio de portas específicas, endereços IP, sites, ou mesmo pacotes de tipo/conteúdo específicos. Com esta solução, é possível simular no virtual box uma maneira de monitorar todo o tráfego que está entrando e saindo da rede corporativa evitando invasões, ataques e outros tipos de ameaças para a rede corporativa.

## 5. Desenvolvimento

O Linux, é um sistema operacional voltado tanto para uso comum quanto para o comercial, dentre suas principais características, podemos destacar o fato de ser um software livre, menos vulnerável a ataques e por apresentar diferentes modelos de implementação para infraestruturas diferentes. Durante o desenvolvimento do trabalho, foram encontradas poucas complicações com relação a usabilidade do Linux, ou melhor, não existe complexidade em usar o sistema em modo gráfico, as dificuldades estão ligadas aos momentos e circunstâncias que precisamos atualizar, instalar e configurar hardwares e softwares através de linhas de comando do terminal Linux.

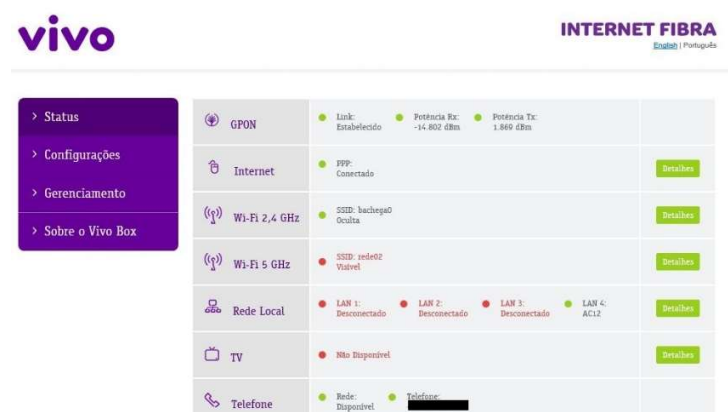
Para a construção e desenvolvimento do projeto foram utilizadas as seguintes ferramentas:

## I. Redes

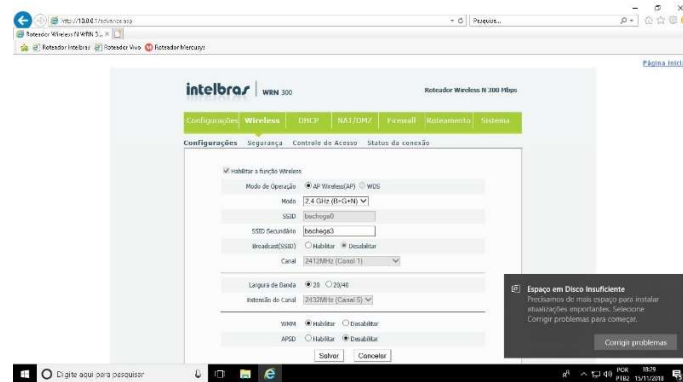
- Link Internet Fibra 100MB;
- Roteador Padrão Vivo;
- Roteador Secundário Intelbras



Tela Vivo Fibra (Fonte: Site [www.minhaconexao.com.br](http://www.minhaconexao.com.br))



Roteador1 192.168.15.1 ( padrão da vivo)

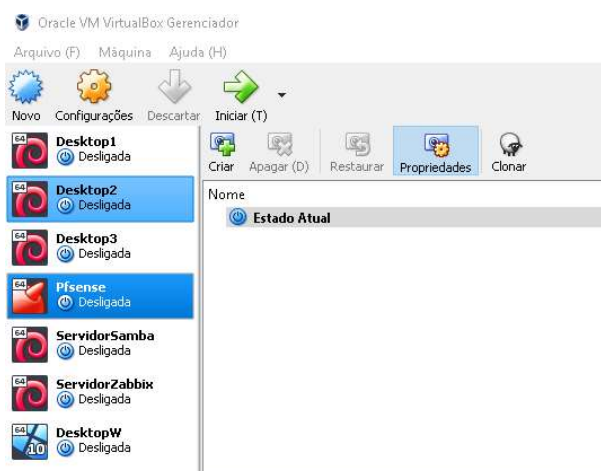


Roteador 2 – IP 10.0.0.1

O roteador 2 ficou responsável por distribuir a internet (Wan) para o Firewall PfSense. O roteador 1(Vivo Fibra) distribui a internet para o roteador 2(Intelbras- usado nos testes) e para um terceiro roteador ligado direto na porta Lan do Modem Vivo. Esta configuração foi necessária para separar a rede doméstica da rede utilizada para o projeto, afim de evitar indisponibilidade na rede causada pelos testes. A configuração completa (telas) esta no Github.

## II. Ambiente de Desenvolvimento e Produção

- Notebook Acer F5-573G Intel Core i7 2.7Ghz, 8Gb Ram W10;
- Desktop Intel Dual Core; 4Gb Ram, de 1TB HD e W10Home;
- HD Externo com capacidade de 1TB e outro com 750GB;
- Software Virtual Box 5.2.22;
- Oracle VM VirtualBox Extension Pack 5.2.20;
- Software Developer Kit (SDK) 5.2.22;
- Pacote Office;
- GitHub;
- HD Regenerator;
- MVDiSize;
- VMWare Player( testes);
- 7Zip;
- Outros.



virtual box

Observação: o Desktop W10 não fez parte do projeto devido a falta de recursos (CPU e RAM) para configura-lo.

## Exibir informações básicas sobre o computador

### Edição do Windows

Windows 10 Home Single Language

© 2018 Microsoft Corporation. Todos os direitos reservados.

### Sistema

Fabricante: Acer  
Modelo: Aspire F5-573G  
Processador: Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz 2.90 GHz  
Memória instalada (RAM): 8,00 GB (utilizável: 7,87 GB)  
Tipo de sistema: Sistema Operacional de 64 bits, processador com base em x64  
Caneta e Toque: Nenhuma Entrada à Caneta ou por Toque está disponível para este vídeo

### Suporte Acer

Site: [Suporte online](#)

### Nome do computador, domínio e configurações de grupo de trabalho

Nome do computador: LAPTOP-FE00RKC4  
Nome completo do computador: LAPTOP-FE00RKC4  
Descrição do computador:  
Grupo de trabalho: WORKGROUP

## Tela Acer

## Exibir informações básicas sobre o computador

### Edição do Windows

Windows 10 Home Single Language

© 2017 Microsoft Corporation. Todos os direitos reservados.

### Sistema

Fabricante: Positivo Informatica S.A.  
Modelo: Stilo  
Processador: Intel(R) Celeron(R) CPU J1800 @ 2.41GHz 2,42 GHz  
Memória instalada (RAM): 4,00 GB (utilizável: 3,89 GB)  
Tipo de sistema: Sistema Operacional de 64 bits, processador com base em x64  
Caneta e Toque: Nenhuma Entrada à Caneta ou por Toque está disponível para este vídeo

### Suporte Positivo Informatica S.A.

Site: [Suporte online](#)

### Nome do computador, domínio e configurações de grupo de trabalho















Nome do computador: DESKTOP-KACEEDQ  
Nome completo do computador: DESKTOP-KACEEDQ  
Descrição do computador:  
Grupo de trabalho: WORKGROUP

## Tela Desktop


















### Dispositivos e unidades (4)



## Dispositivos de Armazenamento

Nome	Data de modific...	Tipo
 01.09.18 Ambiente de Desenvolvimento	19/11/2018 09:52	Pasta de
 02.11.18 GitHub	12/11/2018 22:53	Pasta de
 03.11 PfSense	12/11/2018 22:54	Pasta de
 03.11.18 Passo a Passo	12/11/2018 22:54	Pasta de
 03.11.18 Sql	12/11/2018 22:54	Pasta de
 03.11.18 Windows 10 bkp	12/11/2018 22:54	Pasta de
 04.11.18 IpTables	19/11/2018 08:41	Pasta de
 04.11.18 Sistema de Email	04/11/2018 17:13	Pasta de
 04.11.18 VMWare	19/11/2018 09:52	Pasta de
 16.11 Fase Final Entrega do Projeto	19/11/2018 10:42	Pasta de
 30.10.18 Notebook Acer ( Rec HD) Drivers	19/11/2018 09:45	Pasta de
 Download Material Ead	12/11/2018 22:57	Pasta de
 Programas	19/11/2018 10:35	Pasta de
 Roteador Mercusys	15/11/2018 18:34	Pasta de
 Roteadores Vivo e Intelbras	19/11/2018 10:37	Pasta de
 Teste de Velocidade	12/11/2018 22:50	Pasta de
 Versionamento 1 2 3 ( Subir o Git Hub)	12/11/2018 23:23	Pasta de
 Pfsense	18/11/2018 20:33	Docume
 Rede Diego	15/11/2018 02:55	Docume

### Ambiente de Produção e Desenvolvimento

Nome	Data de modific...	Tipo
 01.10.18 Virtual 5.2.22	19/11/2018 10:05	Pasta de arquivo:
 01.11.18 Free Star Burner DVD	19/11/2018 10:23	Pasta de arquivo:
 01.11.18 Guiformat	19/11/2018 10:23	Pasta de arquivo:
 01.11.18 Linux Live Usb	19/11/2018 10:23	Pasta de arquivo:
 01.11.18 unetbootin-windows-661	19/11/2018 10:23	Pasta de arquivo:
 02.11.18 Debian 9.5 Manual e ISOs	19/11/2018 10:32	Pasta de arquivo:
 04.11.18 HD Regenerator	12/11/2018 22:57	Pasta de arquivo:
 04.11.18 MVDiSize	12/11/2018 22:57	Pasta de arquivo:
 29.10.18 DirSize	19/11/2018 09:41	Pasta de arquivo:
 29.10.18 VirtualBox Versão 4.3 ( recuperaç	19/11/2018 09:51	Pasta de arquivo:
 Boot Linux Debian	19/11/2018 10:03	Pasta de arquivo:
 Menu Concatenado com Diversos Boots ...	19/11/2018 10:35	Pasta de arquivo:
 unetbootin	19/11/2018 10:35	Pasta de arquivo:
 7z1805-x64	18/11/2018 11:07	Aplicativo
 Quick Access_Acer_2.01.3003_W10x64_A	11/11/2018 12:36	Arquivo ZIP do V
 VirtualBoxSDK-5.2.22-126460	10/11/2018 22:03	Arquivo ZIP do V
 winrar-x64-550br-RATON	04/11/2018 13:04	Aplicativo

### Ambiente de Produção e Desenvolvimento

## Sistema Operacional Utilizado








Debian é uma das distribuições Linux mais antigas e populares que começou nos anos 90 com um grupo pequeno de desenvolvedores de Software Livre e cresceu gradualmente para se tornar uma comunidade grande e bem organizada de desenvolvedores e usuários. O kernel do Linux e outros softwares livres importantes formam uma distribuição de software única chamada Debian GNU/Linux. Esta distribuição é composta por um grande número de pacotes de softwares. Cada pacote na distribuição contém executáveis, scripts, documentação e informações de configuração, e tem um mantenedor que é o principal responsável por manter o pacote atualizado, rastrear relatórios de bugs e comunicar-se com os colaboradores que juntos fazem um trabalho de rastreamento de erros e garantem que os problemas sejam encontrados, corrigidos e distribuídos de forma rápida e gratuita através das atualizações automáticas.

Desde o início do projeto, o Debian foi escolhido devido a quantidade de manuais e materiais, por exemplo as videoaulas, que serviriam como guias, para desenvolvimento do projeto, com fácil acesso através da Internet.

A instalação apenas em modo script, através de dispositivo USB, mostrou-se vantajosa, em um primeiro momento, por ser uma pequena imagem de instalação e por ser baixada necessitando apenas de uma máquina com uma conexão de Internet. Mas apresentou muitas falhas durante o processo de configuração e instalação de pacotes adicionais para configuração do firewall IPTABLES, sendo difícil encontrar a solução dos problemas devido aos conhecimentos ainda serem limitados, proporcional ao tempo de convivência com o sistema.

Desta forma optou-se por trabalhar com as imagens maiores que contém a instalação completa, ou seja, juntas possuem mais pacotes que facilitam a instalação em máquinas sem a necessidade de conexão com a Internet tornando assim, este modelo ainda mais propício para quem precisa de uma máquina recheada..

logia em Segurança da Informação > 2018 > 2º Semestre > Projeto Integrador Implementação de Segurança > C				
Nome	Data de modific...	Tipo	Tamanho	
 debian-9.5.0-amd64-DVD-1.iso	03/11/2018 15:07	Arquivo TORRENT	69 KB	
 debian-9.5.0-amd64-DVD-2.iso	03/11/2018 15:07	Arquivo TORRENT	88 KB	
 debian-9.5.0-amd64-DVD-3.iso	03/11/2018 15:07	Arquivo TORRENT	88 KB	
 debian-9.5.0-amd64-netinst	27/10/2018 15:03	Arquivo de Image...	297,984 KB	
 Manual Debian	03/11/2018 13:52	Adobe Acrobat D...	717 KB	

Tela dos Arquivos utilizados

Observação: verificar a capacidade de processamento da máquina real na fase pré-projeto.



## Configurações de Instalação

Os equipamentos do tipo Desktop e Servidores tiveram uma configuração inicial bem semelhante, através de Discos Virtuais. A principal diferença foi na utilização de um espaço maior no disco para que as três imagens ISO Debian 9 (DVD1, DVD2 e DVD3) fossem disponibilizadas para os servidores e apenas a imagem ISO DVD1 para configuração dos equipamentos desktops, uma vez que a proposta para esses equipamentos é serem mais leves. Mas, os servidores não conseguiram rodar em conjunto com os desktops, fazendo com que o projeto dos servidores retornasse para a instalação mais simples e muito mais leve, sem o ambiente gráfico, para não consumir os recursos necessários para processar o Debian Desktop1 Desktop2 e Desktop3 projetados nesta rede.

VG LVM debiandiego-vg, LV home - 4.4 GB Linux device-mapper (linear)					
>	#1	4.4 GB	f	ext4	/home
VG LVM debiandiego-vg, LV root - 2.1 GB Linux device-mapper (linear)					
>	#1	2.1 GB	f	ext4	/
VG LVM debiandiego-vg, LV swap_1 - 532.7 MB Linux device-mapper (linear)					
>	#1	532.7 MB	f	swap	swap
VG LVM debiandiego-vg, LV tmp - 260.0 MB Linux device-mapper (linear)					
>	#1	260.0 MB	f	ext4	/tmp
VG LVM debiandiego-vg, LV var - 1.0 GB Linux device-mapper (linear)					
>	#1	1.0 GB	f	ext4	/var
SCSI1 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK					
>	#1	primária	254.8 MB	f	ext2 /boot
>	#5	lógica	8.3 GB	K	lvm

Configurações de Hardware

```
root@debiandiego:~# hostnamectl
  Static hostname: debiandiego
        Icon name: computer-vm
        Chassis: vm
        Machine ID: 4dcb9193ac964240aa2fd722baee7be6
        Boot ID: 80e03385ea304903ad586f9bcddad494
        Virtualization: oracle
        Operating System: Debian GNU/Linux 9 (stretch)
        Kernel: Linux 4.9.0-7-amd64
        Architecture: x86-64
root@debiandiego:~#
```

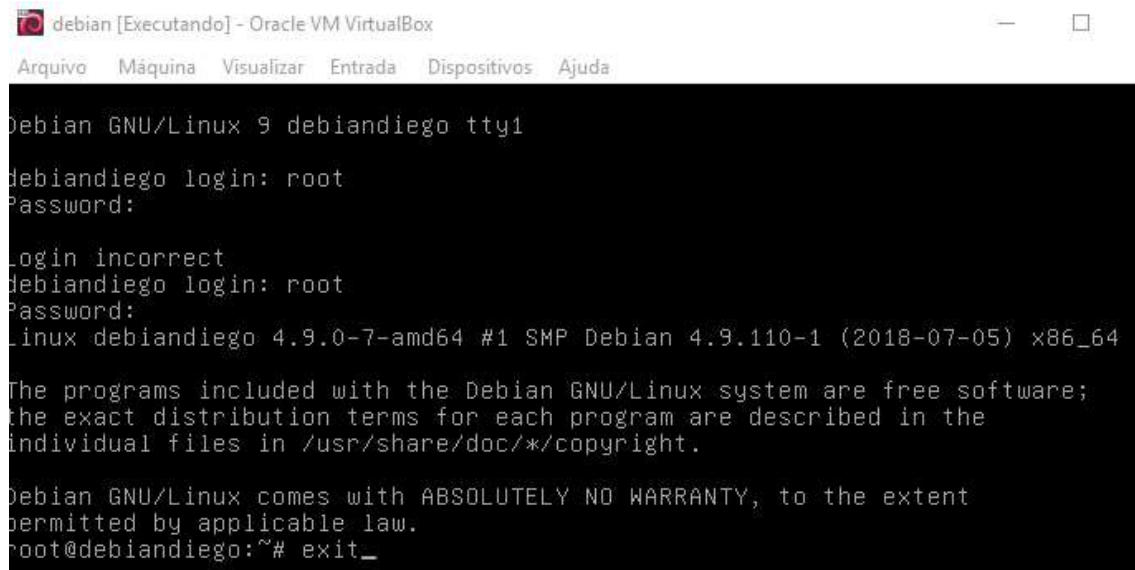
Configurações de Software

```
root@debiandiego:~# systemd-analyze
-bash: systemd-analyze: comando não encontrado
root@debiandiego:~# systemd-analyze
Startup finished in 3.637s (kernel) + 7.854s (userspace) = 11.492s
root@debiandiego:~# _
```

Tempo de Carregamento do Sistema: 11,49segundos

## Configurações Utilizadas

Root 123456 / Nome usuário: diegobachega ou diego ou debiandiego

A terminal window titled 'debian [Executando] - Oracle VM VirtualBox' with a menu bar (Arquivo, Máquina, Visualizar, Entrada, Dispositivos, Ajuda). The terminal output shows the login process for the 'root' user. It starts with 'Debian GNU/Linux 9 debiandiego tty1', followed by 'debiandiego login: root' and 'Password:'. After an incorrect login attempt, it shows 'Login incorrect' and 'debiandiego login: root' followed by 'Password:'. The system then displays the kernel version 'Linux debiandiego 4.9.0-7-amd64 #1 SMP Debian 4.9.110-1 (2018-07-05) x86\_64', a copyright notice, and a warranty disclaimer. The prompt is 'root@debiandiego:~#' and the user enters 'exit\_'.

```
Debian GNU/Linux 9 debiandiego tty1

debiandiego login: root
Password:

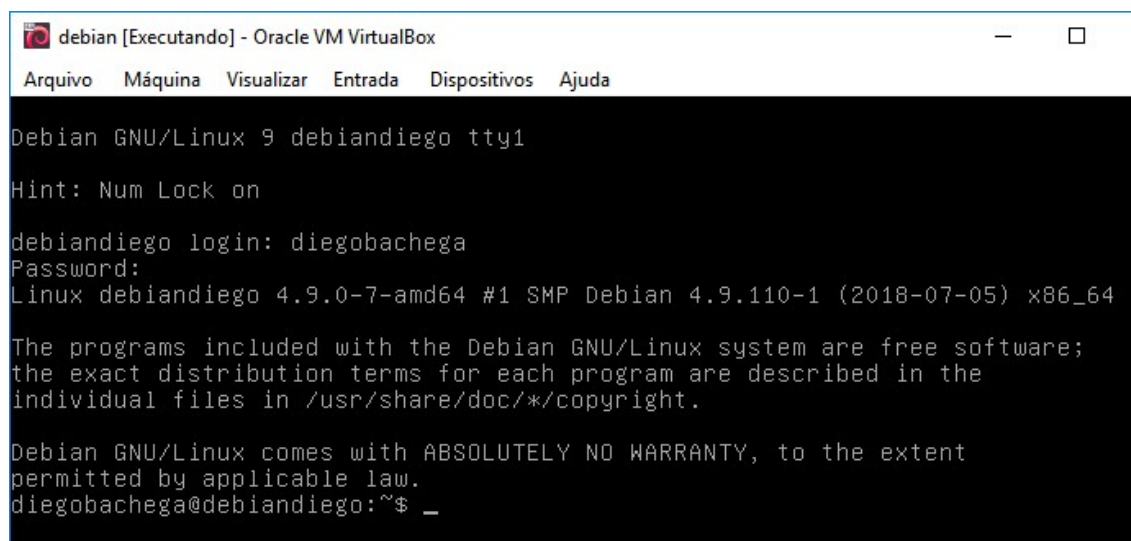
Login incorrect
debiandiego login: root
Password:

Linux debiandiego 4.9.0-7-amd64 #1 SMP Debian 4.9.110-1 (2018-07-05) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debiandiego:~# exit_
```

Tela do usuário root

A terminal window titled 'debian [Executando] - Oracle VM VirtualBox' with a menu bar (Arquivo, Máquina, Visualizar, Entrada, Dispositivos, Ajuda). The terminal output shows the login process for the 'diegobachega' user. It starts with 'Debian GNU/Linux 9 debiandiego tty1', followed by 'debiandiego login: diegobachega' and 'Password:'. The system then displays the kernel version 'Linux debiandiego 4.9.0-7-amd64 #1 SMP Debian 4.9.110-1 (2018-07-05) x86\_64', a copyright notice, and a warranty disclaimer. The prompt is 'diegobachega@debiandiego:~\$' and the user enters an underscore '\_'.

```
Debian GNU/Linux 9 debiandiego tty1

debiandiego login: diegobachega
Password:

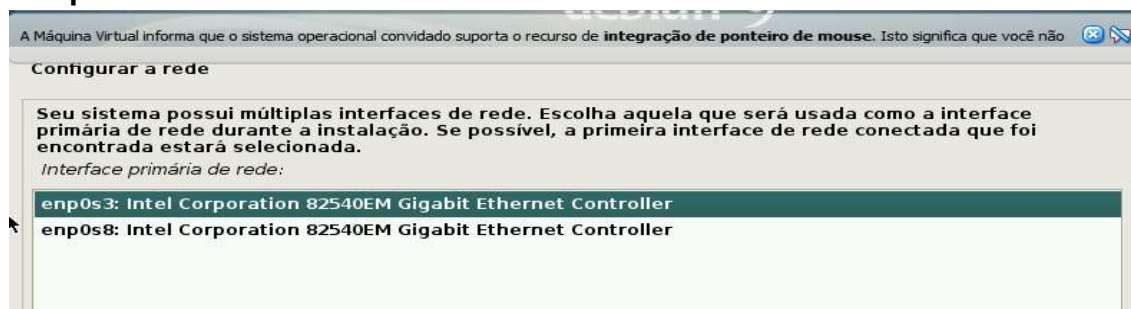
Linux debiandiego 4.9.0-7-amd64 #1 SMP Debian 4.9.110-1 (2018-07-05) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
diegobachega@debiandiego:~$ _
```

Tela do usuário diegobachega

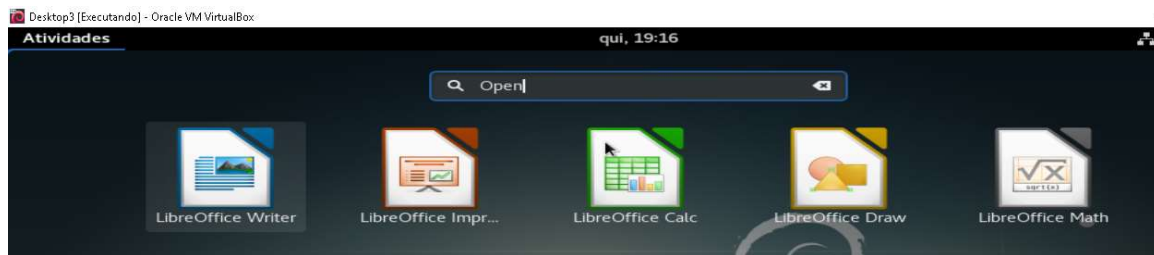
## Adaptadores de Rede



Duas placas de Redes habilitadas

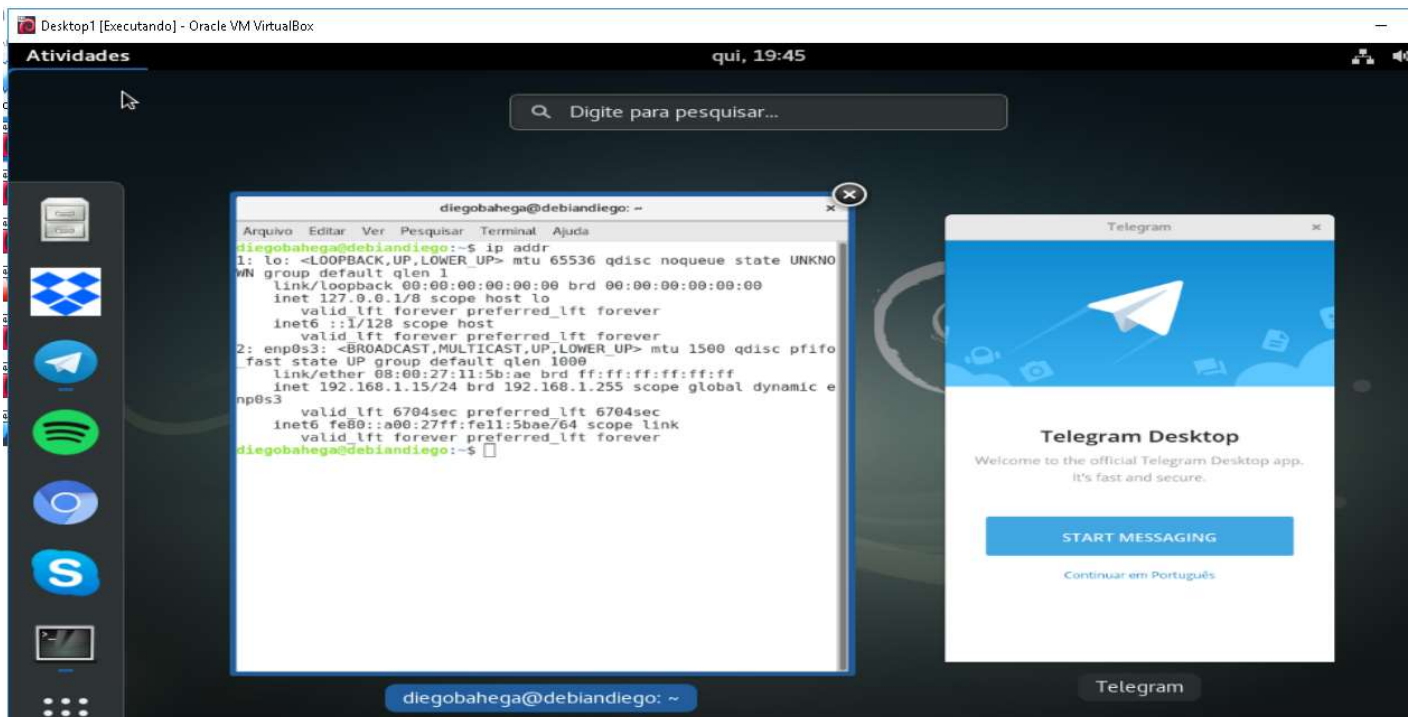
### III. Estações de Trabalho

Para configurar os desktops, foram projetadas 3 estações, com aplicações voltadas para a área administrativa da empresa fictícia. Um conjunto importante e comuns para quem trabalha em escritórios, é o pacote office. Assim, na empresa fictícia as três máquinas possuem a suíte instalada LibreOffice, que até já vem embarcado no Debian 9 Stretch ( DVD1 .ISO).

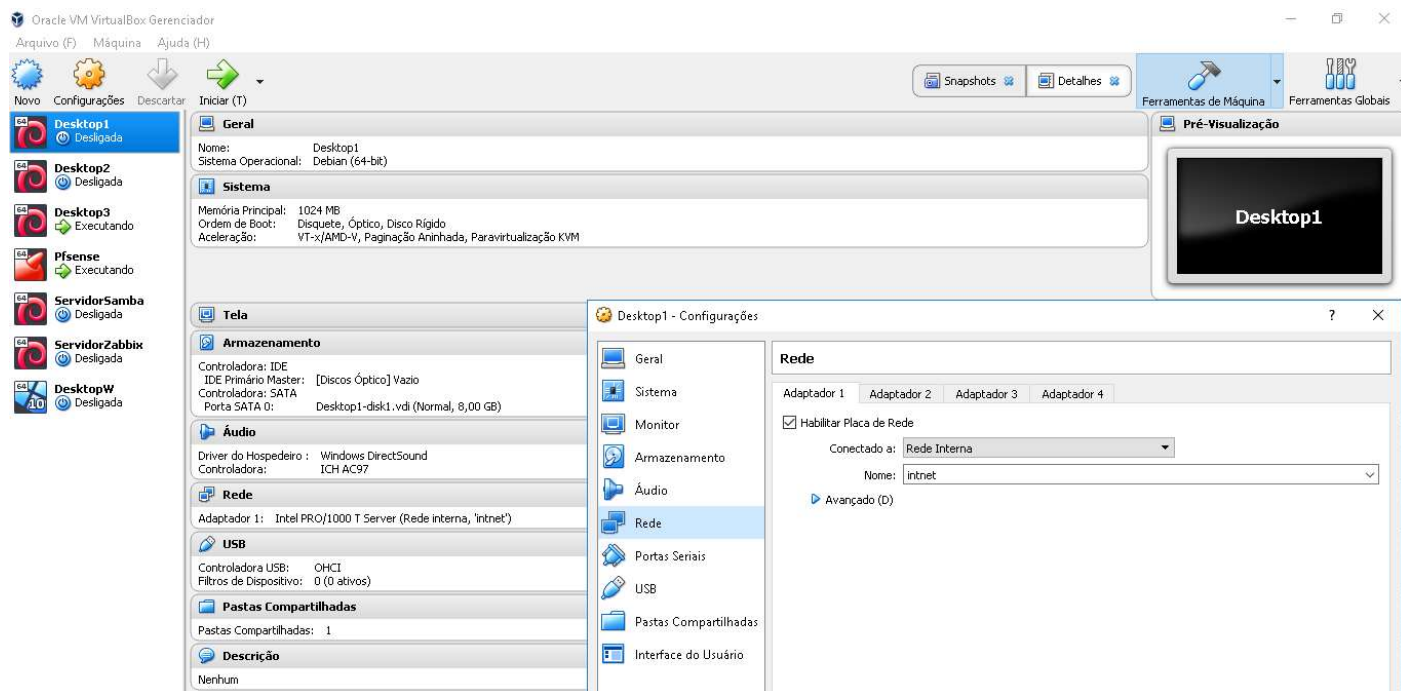


Tela suíte LibreOffice

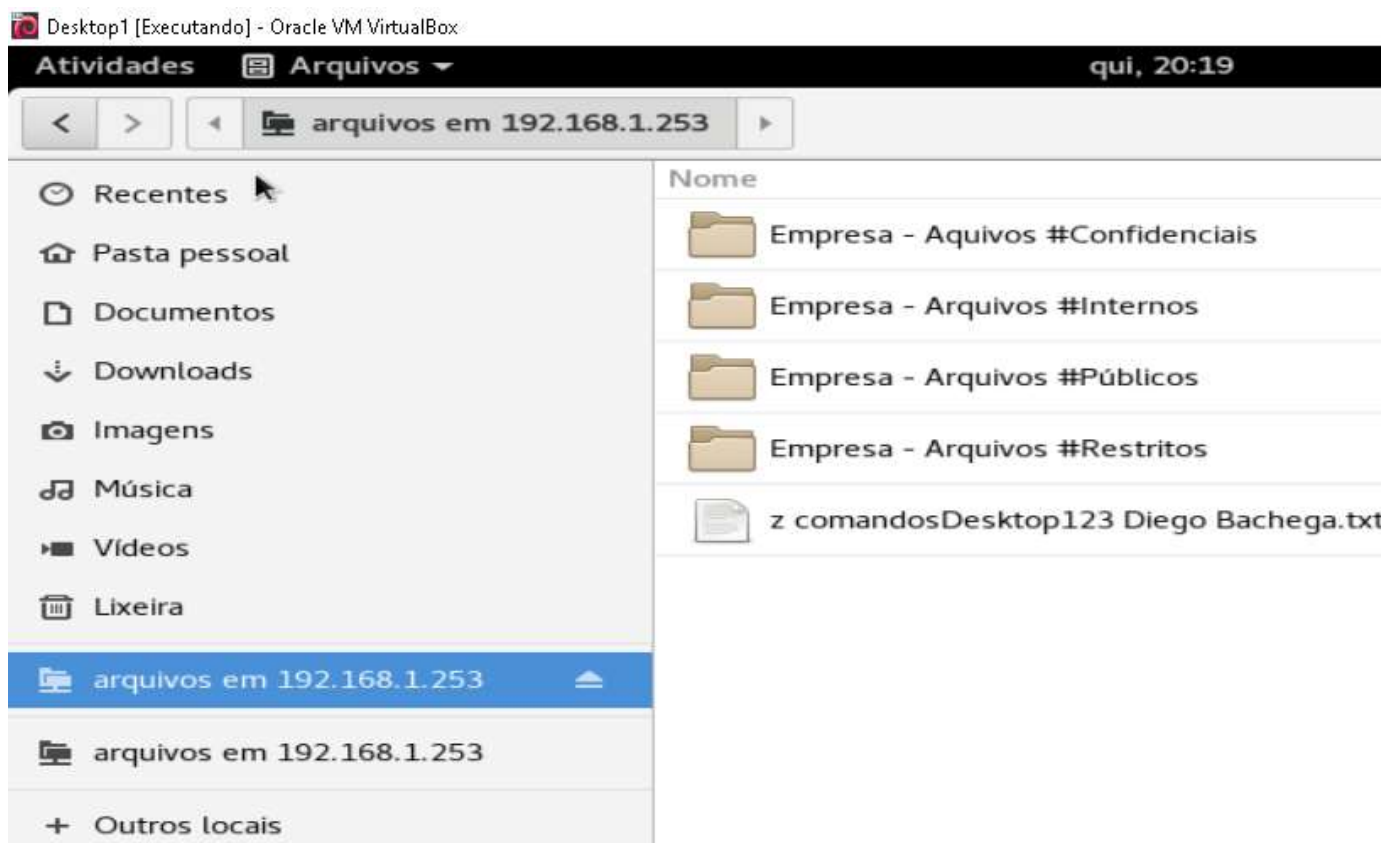
Além desse pacote, algumas configurações e aplicações OpenSource podem facilitar o dia a dia da empresa. E buscando trazer um pouco desta realidade para o projeto foram feitas configurações de melhoria como a atualização dos repositórios (sources.list) e adicionalmente foram instalados os seguintes programas:



Desktop1 - Principal

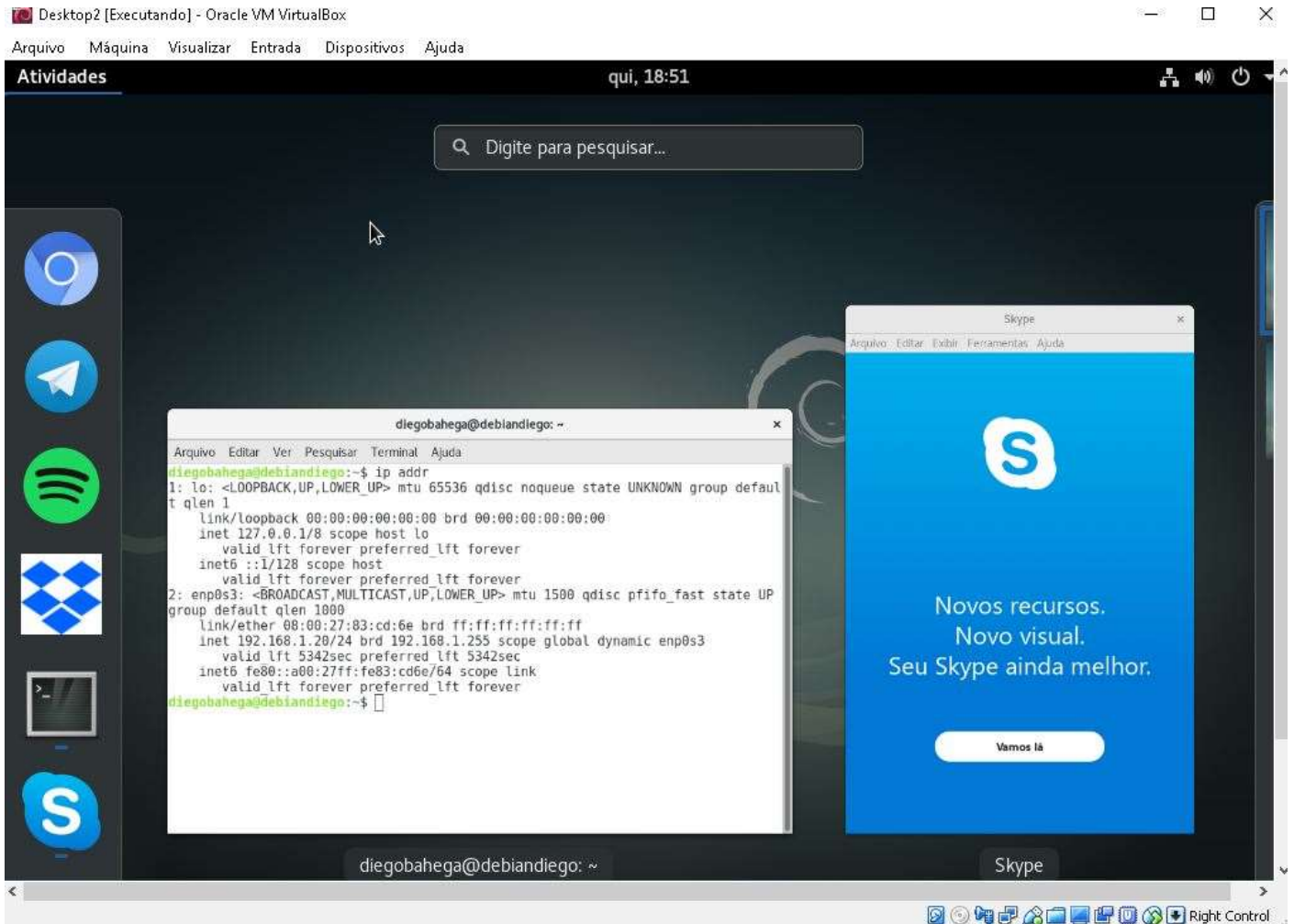


Desktop1 - Console VB

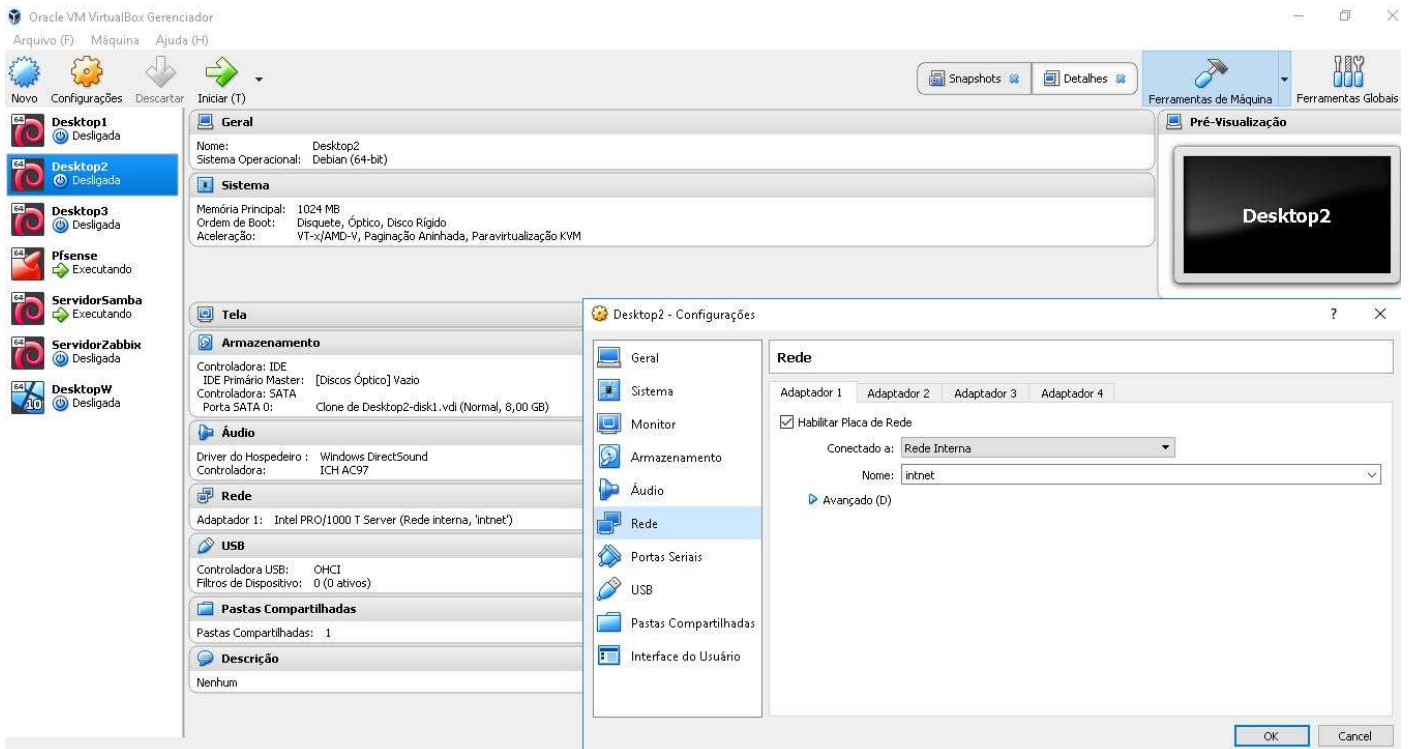


Desktop1 - Compartilhamento de Arquivos

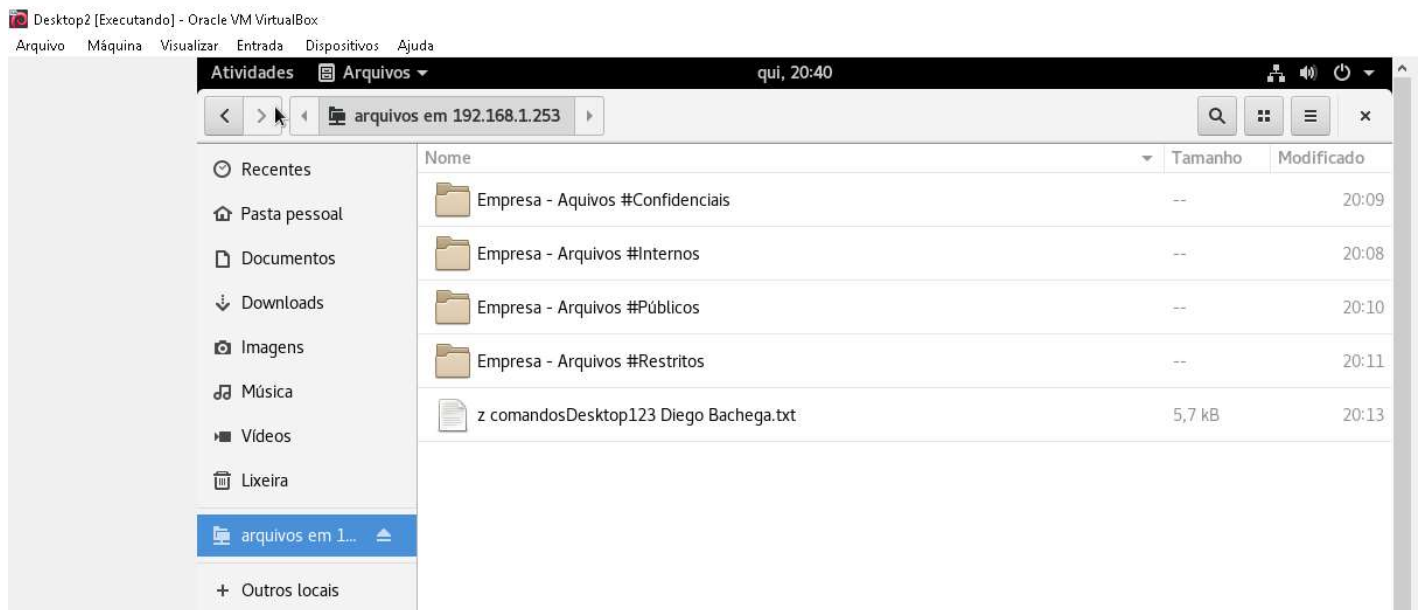




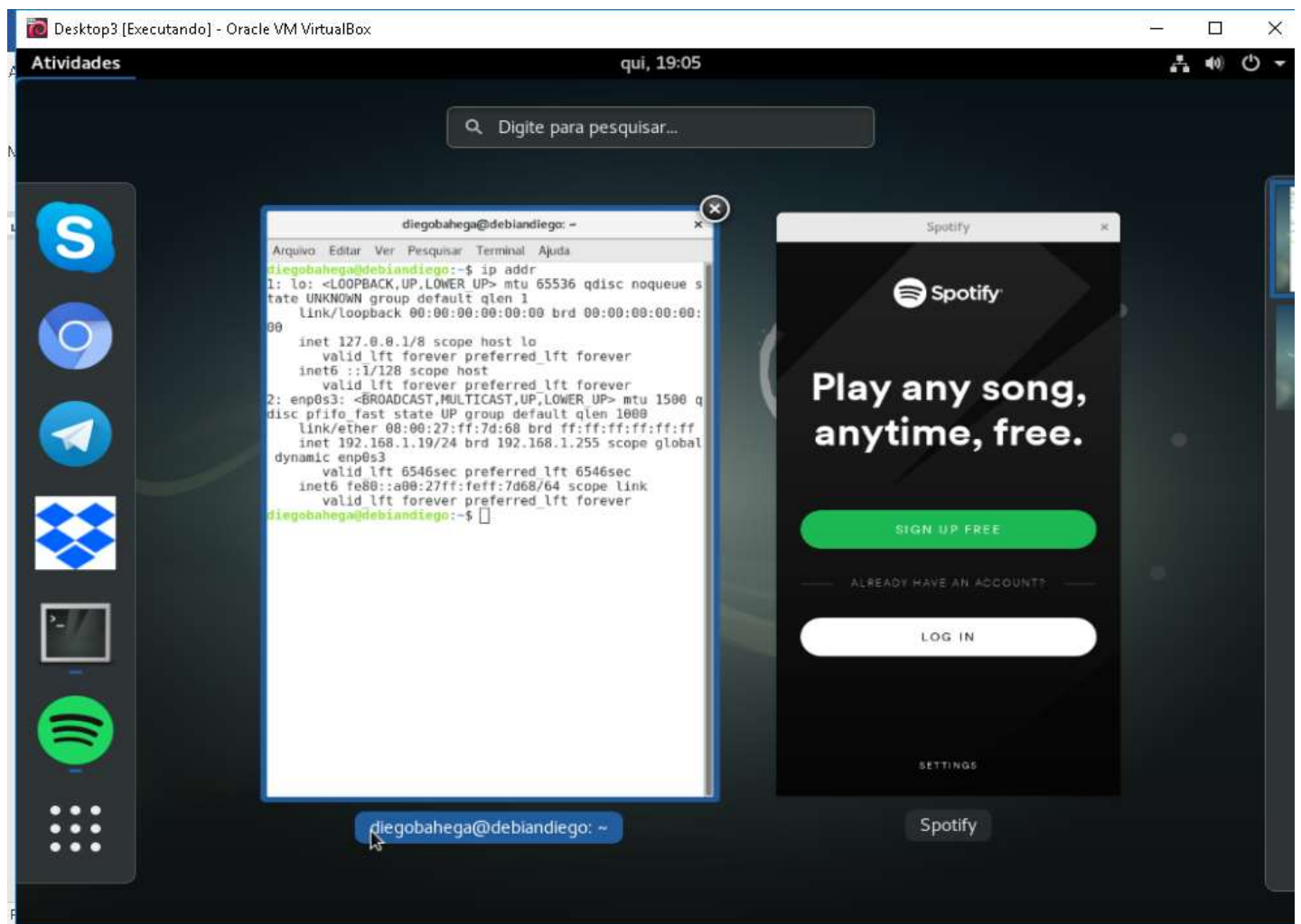
Desktop 2 – Principal



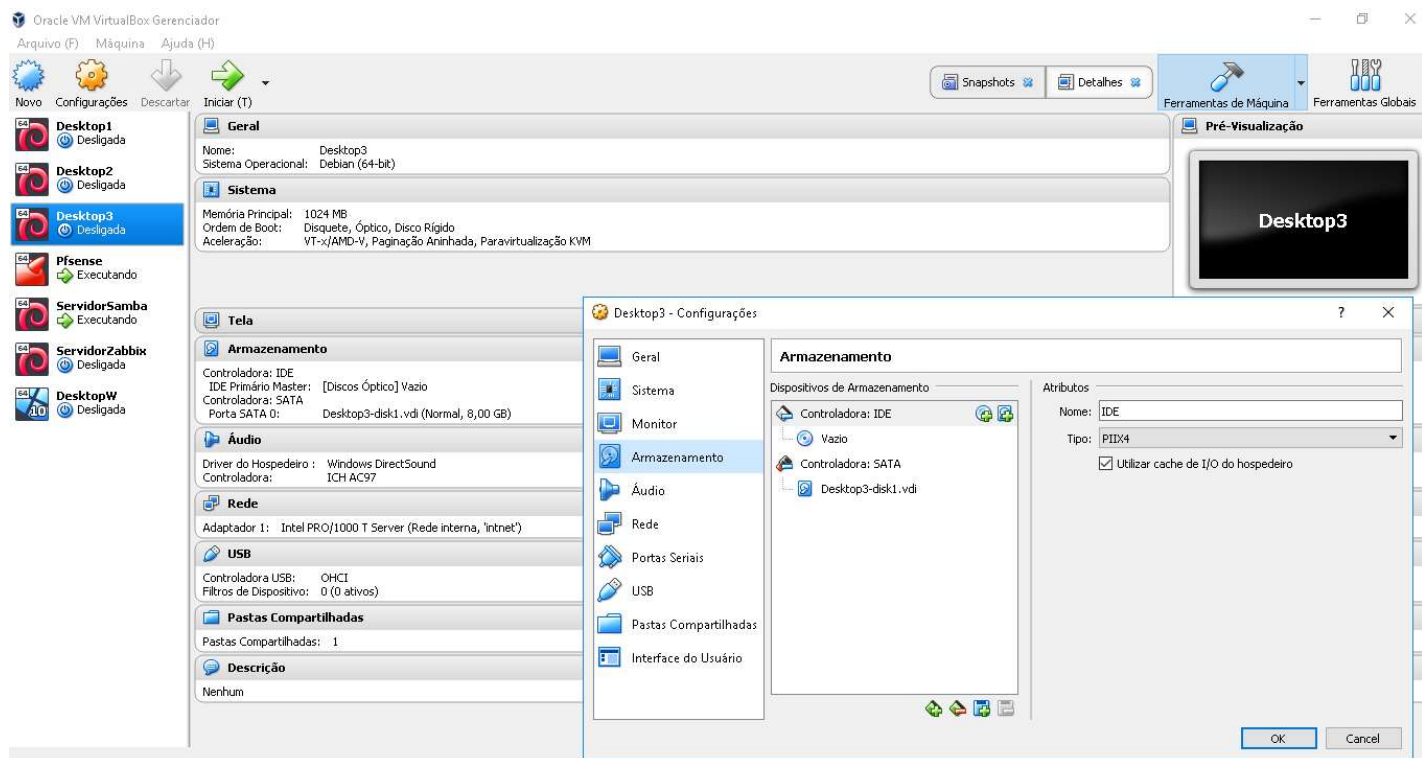
Desktop 2 - Console VB



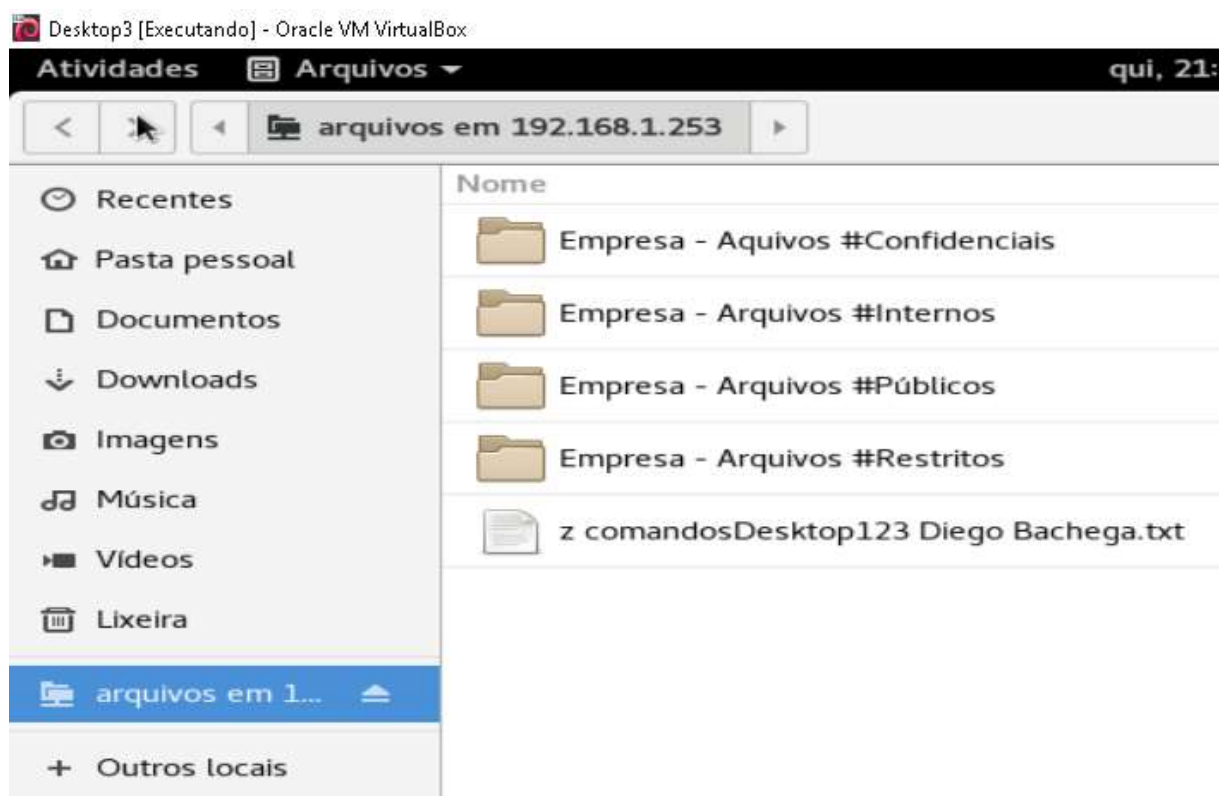
Desktop 2 - Compartilhamento de Arquivos



Desktop 3 - Principal



Desktop 3 - Console VB



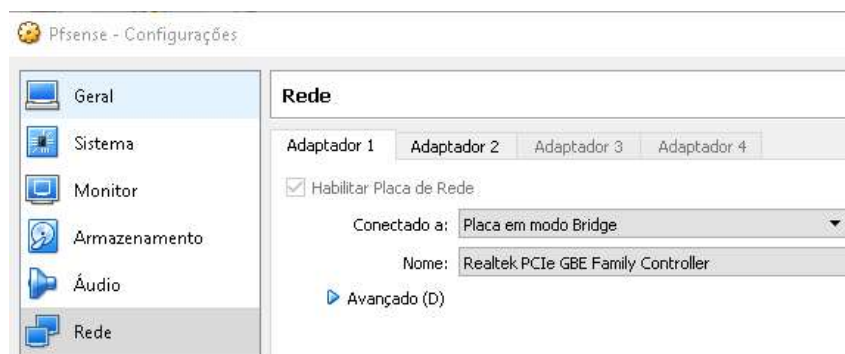
Desktop 3 - Compartilhamento de Arquivos

#### IV. Firewall – Linha de Defesa

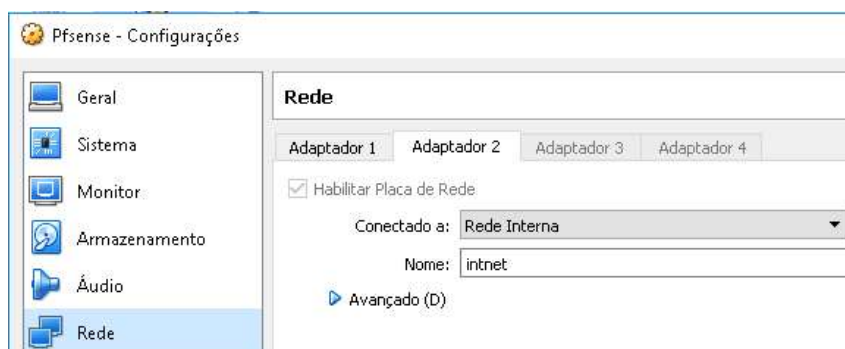
Foi escolhido o Firewall Pfsense (Versão Free 2.4.4 64bits) por ser um software livre, baseado em FreeBSD, adaptado tanto para o seu uso como roteador como firewall. De maneira resumida, ele é um appliance com muitos recursos prontos para serem instalados e já vem embarcado nele uma série de opções como o controle avançado de banda, VPN, autenticação Radius, balanceamento de link dentre outras.

##### Passo a Passo par a Instalação do Firewall

- ✓ Download do arquivo com a arquitetura AMD64 (64-bit).
- ✓ Software 7-zip, para descompactar a iso;
- ✓ Para instalação do Appliance, foi criada uma máquina virtual com nome Pfsense2 configurado para FreeBSD;
- ✓ Nas configurações de Rede, o Adaptador 1 ficou configurado em modo bridge e o 2 ficou como rede interna;



Adaptador 1

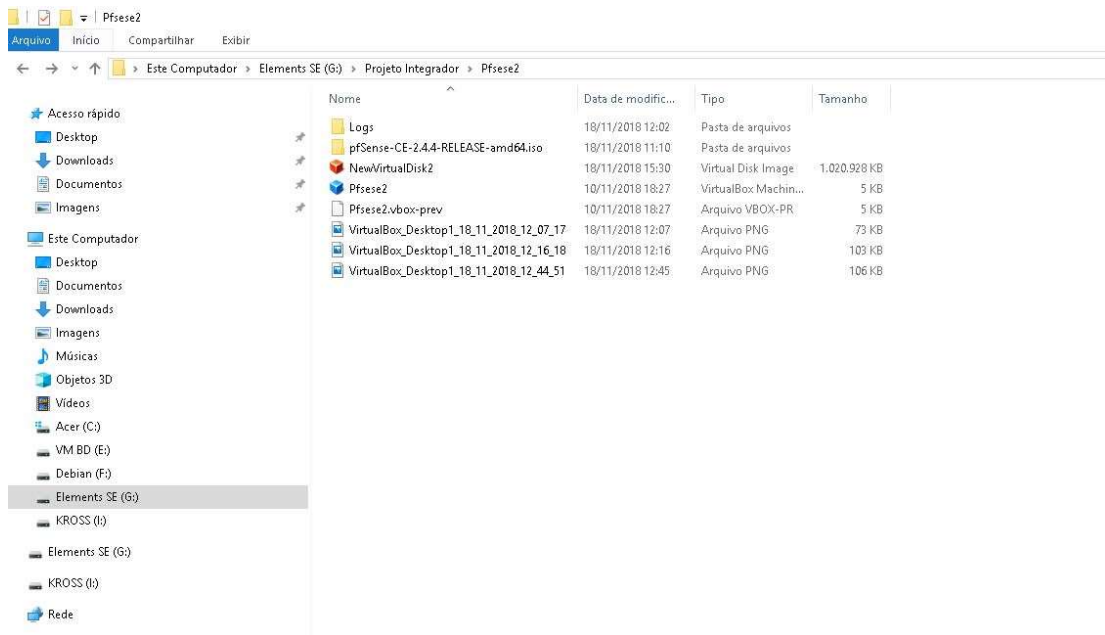


Adaptador 2

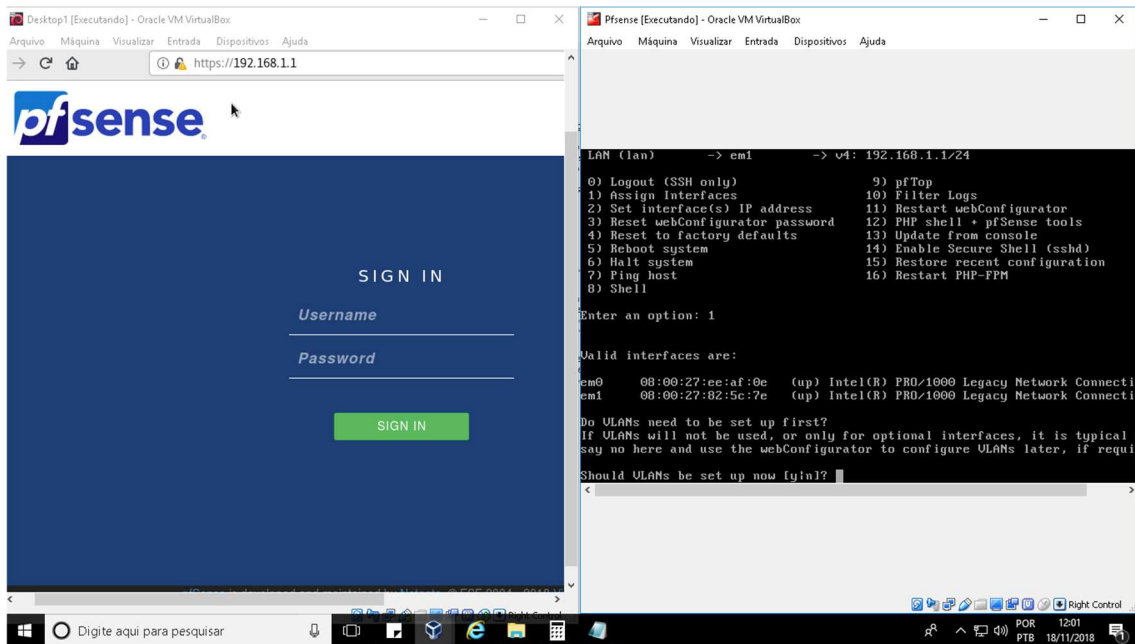
- ✓ Por fim, as máquinas Servidor1 e Servidor2, Desktop1, Desktop2 e Desktop3 foram conectadas à rede interna com toda a conexão passando pelo Firewall.

**Observação:** A instalação do PfSense só foi concluída depois de muito pesquisar, testar e errar até acertar.



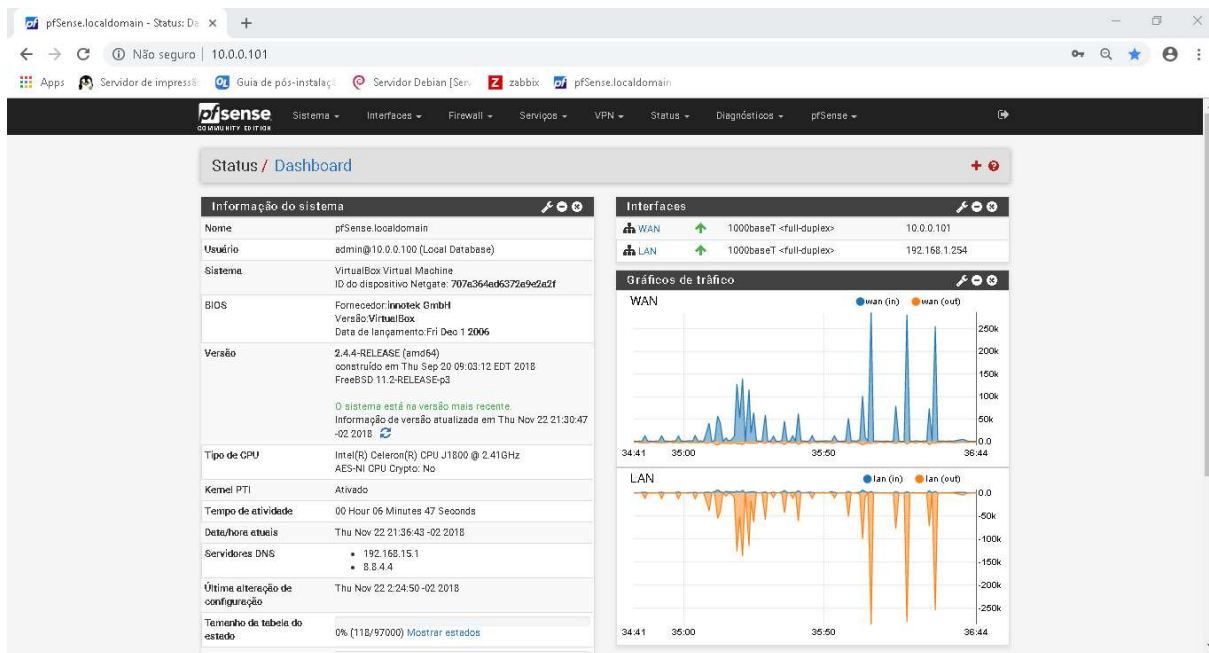


Tela PfSense Pastas

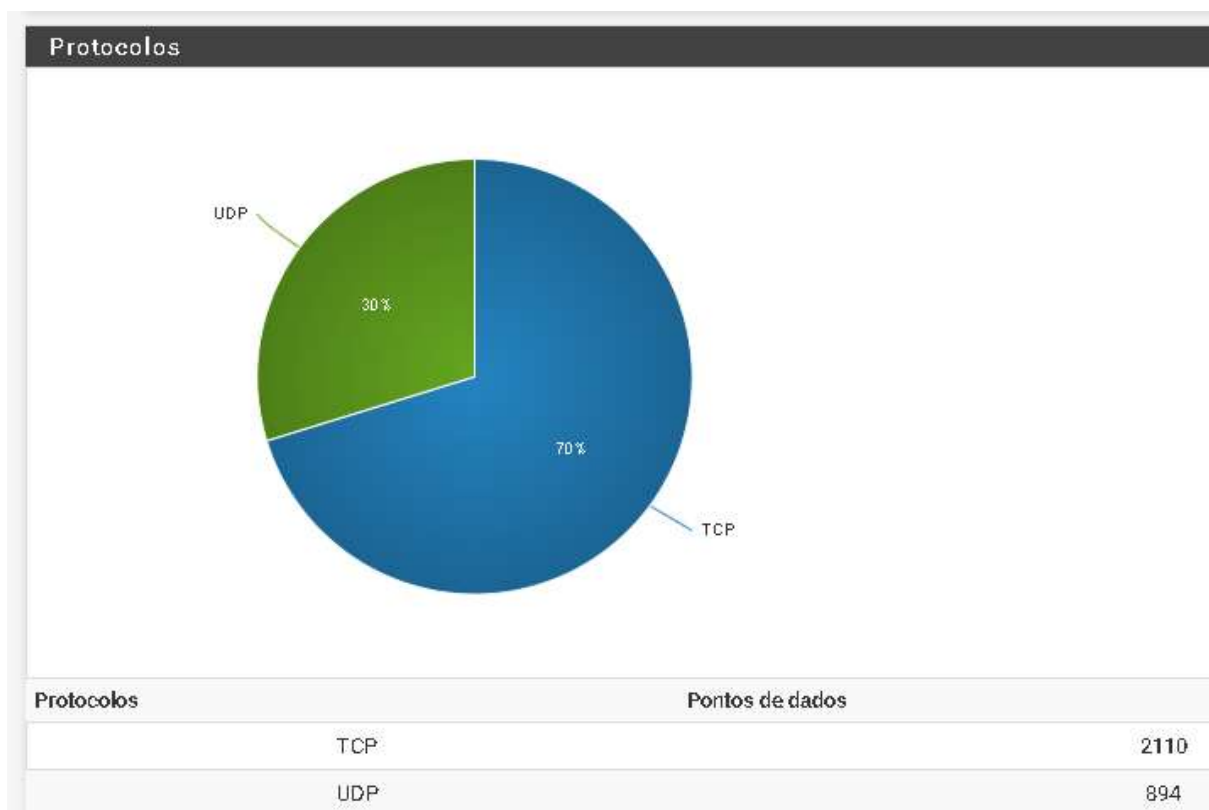


Tela Pfsense Login

Pela Máquina Real (IP 192.168.1.254) redirecionado para 10.0.0.101  
Acessando pelas Máquinas Virtuais (Desktop 1, 2 ou 3 - Rede Interna) IP 10.0.0.101

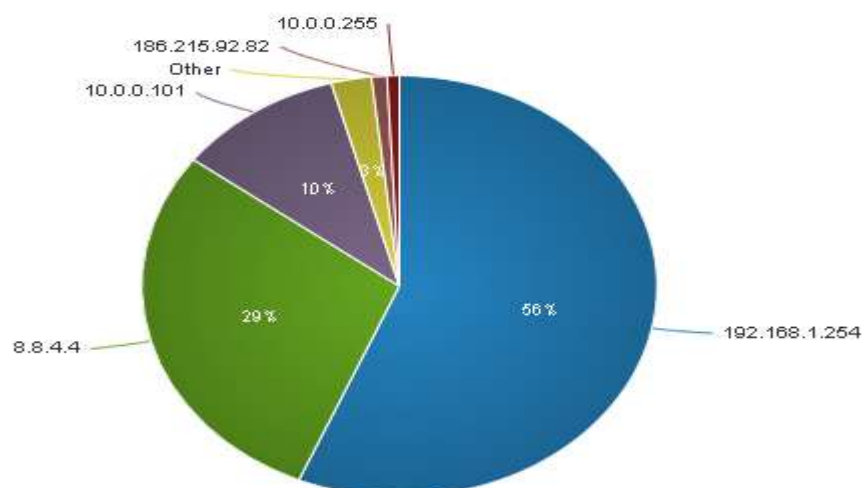


Tela PfSense1 Inicial



Percentual de Protocolos UDP e TCP

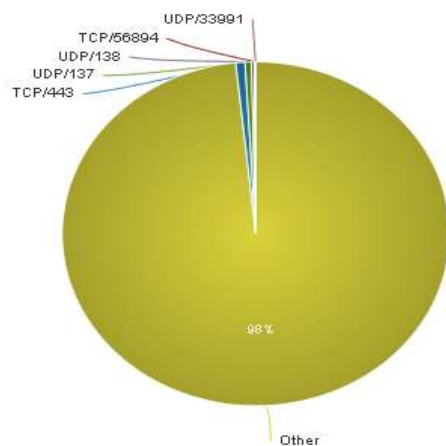
## IPs de Destino



IPs de Destino	Pontos de dados
192.168.1.254	1694
8.8.4.4	867
10.0.0.101	315
186.215.92.82	29
10.0.0.255	23

## IPs Destino

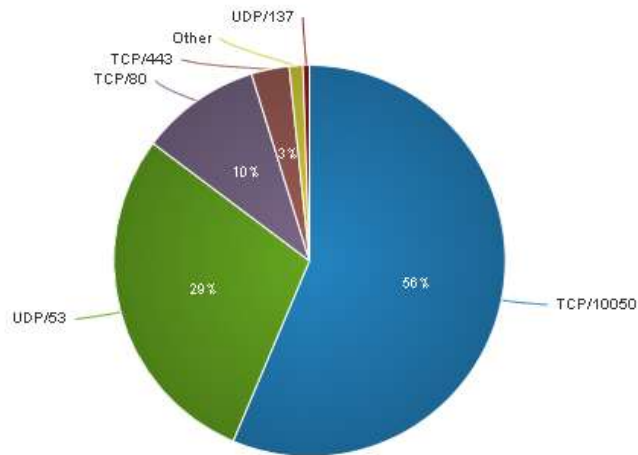
### Portas de Origem



Portas de Origem	Pontos de dados
TCP/443: https	23
UDP/137: netbios-ns	16
UDP/138: netbios-dgm	7
UDP/33991	2
TCP/56894	2
Other	2954

## IPs Origem

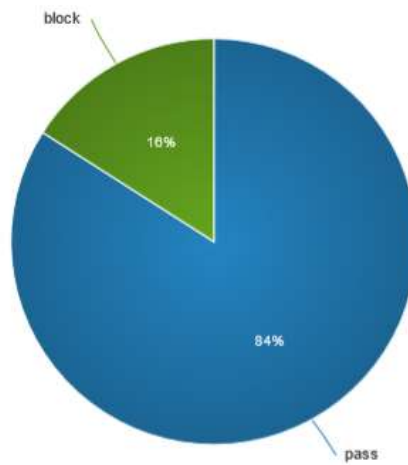
## Portas de Destino



Portas de Destino	Pontos de dados
TCP/10050	1694
UDP/53: domain	867
TCP/80: http	299
TCP/443: https	94
UDP/137: netbios-ns	16
Other	34

Portas Destino

## Ações



Ações	Pontos de dados
pass	2552
block	485

Ações BloqueadosxPermitidos

## Diagnósticos / Atividades do Sistema

### Atividade da CPU

last pid: 43534; load averages: 0.29, 0.51, 0.59 up 0+00:48:43 22:18:39  
121 processes: 3 running, 104 sleeping, 14 waiting

Mem: 58M Active, 63M Inact, 81M Hired, 16M Buf, 759M Free

Swap:

PID	USERNAME	PRI	NICE	SIZE	RES	STATE	TIME	%CPU	COMMAND
11	root	155	ki31	0K	16K	RUN	43:46	100.00%	[idle]
0	root	-16	-	0K	240K	swpin	0:31	0.00%	[kernel{swapper}]
0	root	-92	-	0K	240K	-	0:19	0.00%	[kernel{em0 taskq}]
316	root	52	0	91720K	36724K	accept	0:10	0.00%	php-fpm: pool nginx (php-fpm){php-fpm}
73647	root	24	0	91464K	36416K	pipe rd	0:10	0.00%	php-fpm: pool nginx (php-fpm){php-fpm}
0	root	-92	-	0K	240K	-	0:10	0.00%	[kernel{em0 taskq}]
315	root	52	0	89284K	34604K	accept	0:09	0.00%	php-fpm: pool nginx (php-fpm)
12	root	-60	-	0K	224K	WAIT	0:06	0.00%	[intr{swi4: clock (0)}]
33817	root	20	0	13352K	8124K	kqread	0:06	0.00%	nginx: worker process (nginx)
79406	root	20	0	6400K	2556K	select	0:04	0.00%	/usr/sbin/syslogd -s -c -c -l /var/dhcpd/va
26873	root	52	0	91464K	36184K	accept	0:03	0.00%	php-fpm: pool nginx (php-fpm){php-fpm}
7	root	-16	-	0K	16K	-	0:02	0.00%	[rand_harvestq]
16562	zabbix	20	0	10956K	7344K	select	0:01	0.00%	zabbix_agentd: listener #3 [waiting for con
23033	root	20	0	6000K	2324K	nanslp	0:01	0.00%	[dpinger{dpinger}]
68781	root	52	20	6068K	2596K	wait	0:01	0.00%	/bin/sh /var/db/rrd/updaterrd.sh
10672	root	20	0	6600K	2360K	bpf	0:01	0.00%	/usr/local/sbin/filterlog -i pflog0 -p /var
6	root	-16	-	0K	16K	prtm	0:01	0.00%	[pf_purge]
4	root	-16	-	0K	32K	-	0:01	0.00%	[cam{done00}]

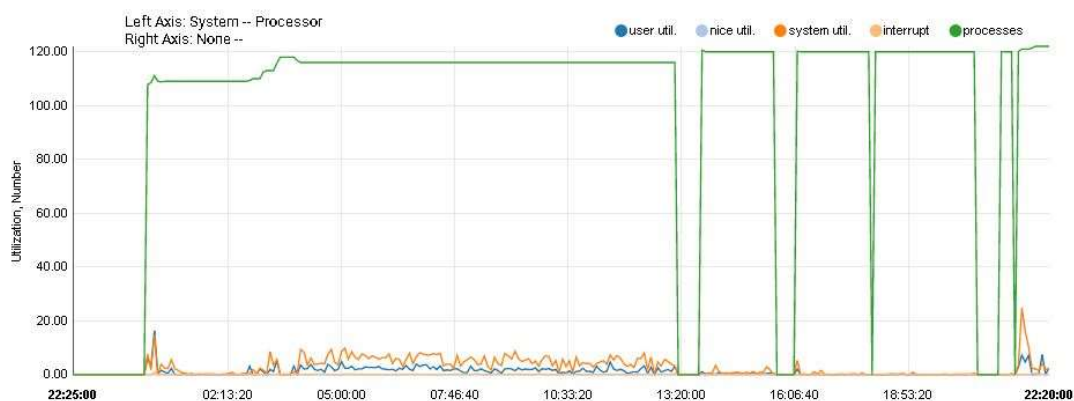
### Diagnóstico

## Status / Monitoring



Padrão

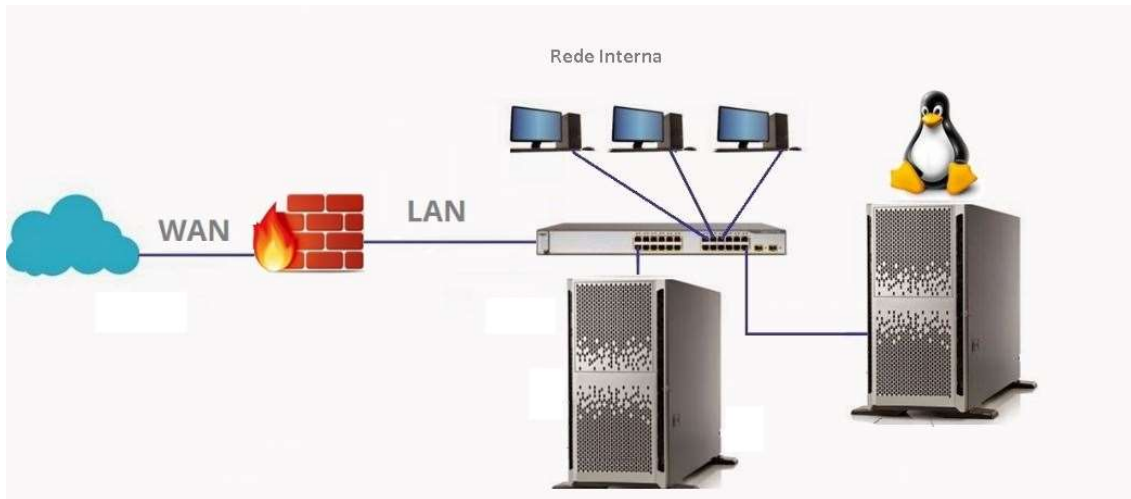
### Interactive Graph



### Monitoramento Processador

## V. Servidores

Este projeto ilustra, a instalação dois servidores Debian 9 Stretch, voltados para uma empresa fictícia. Somados, os dois servidores possuem a capacidade de compartilhamento, proteção do sistema de segurança e monitorização do sistema.



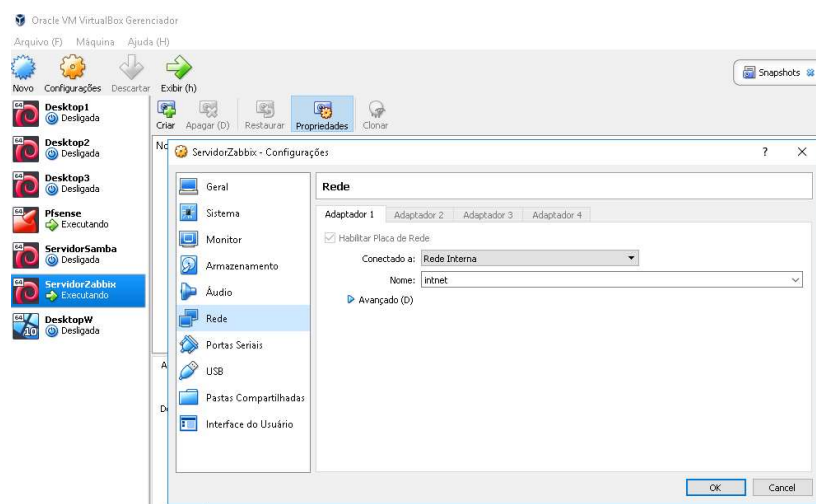
Arquitetura de rede do projeto

(proposta para uma empresa fictícia 1 Firewall, 2 Servidores (Arquivos e Zabbix) e 3 Desktops.

## VI. Servidor MySQL + Apache

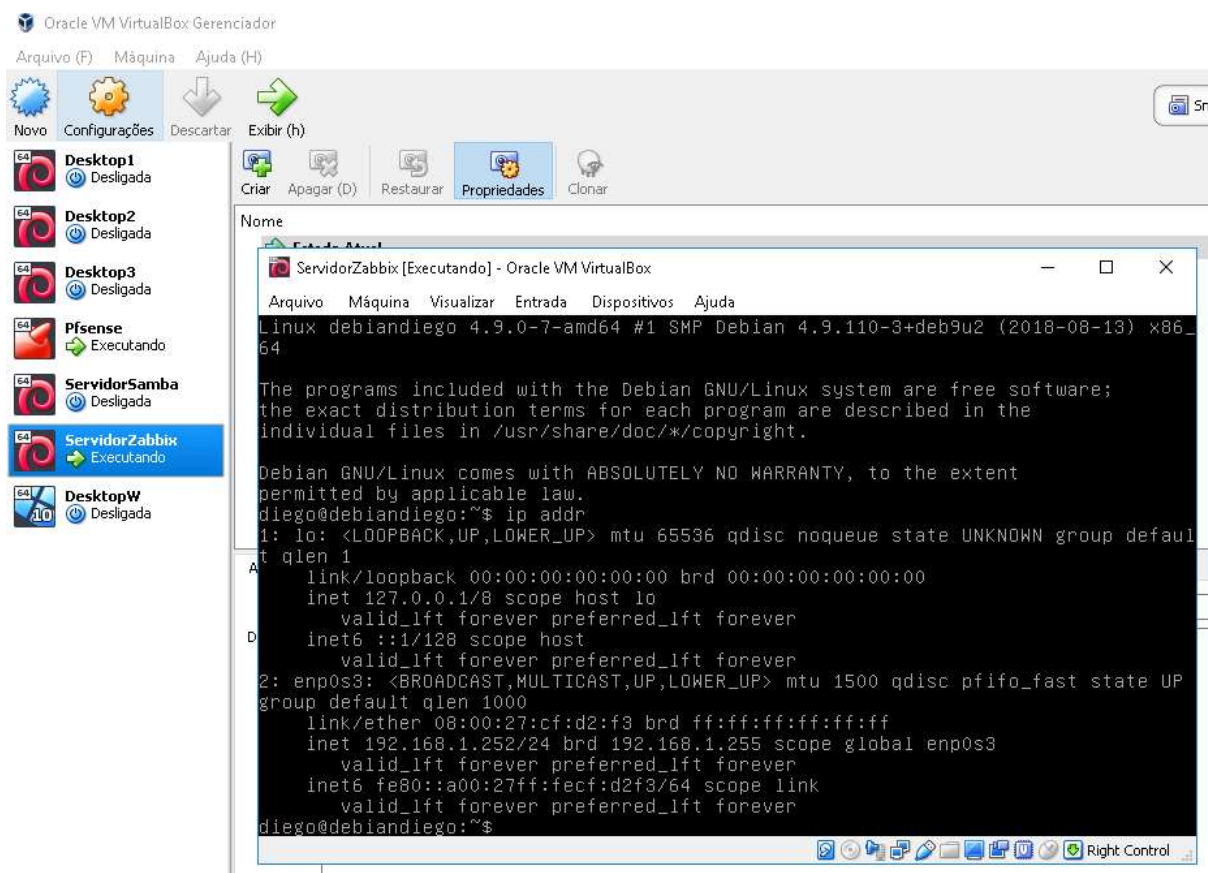
Este Servidor foi projeto para o Zabbix, que é uma solução Open Source, e que pode ser utilizada para monitorar toda a infraestrutura de rede e aplicações. Neste projeto seu objetivo será detectar anormalidades no Firewall, disparando alertas em telas, armazenando os dados em banco de dados MySQL para que possam ser gerados gráficos e painéis de acompanhamento e que mostrem informações de comportamento do Firewall Pfsense.

BD Name: zabbix\_db User Name: zabbix\_usr



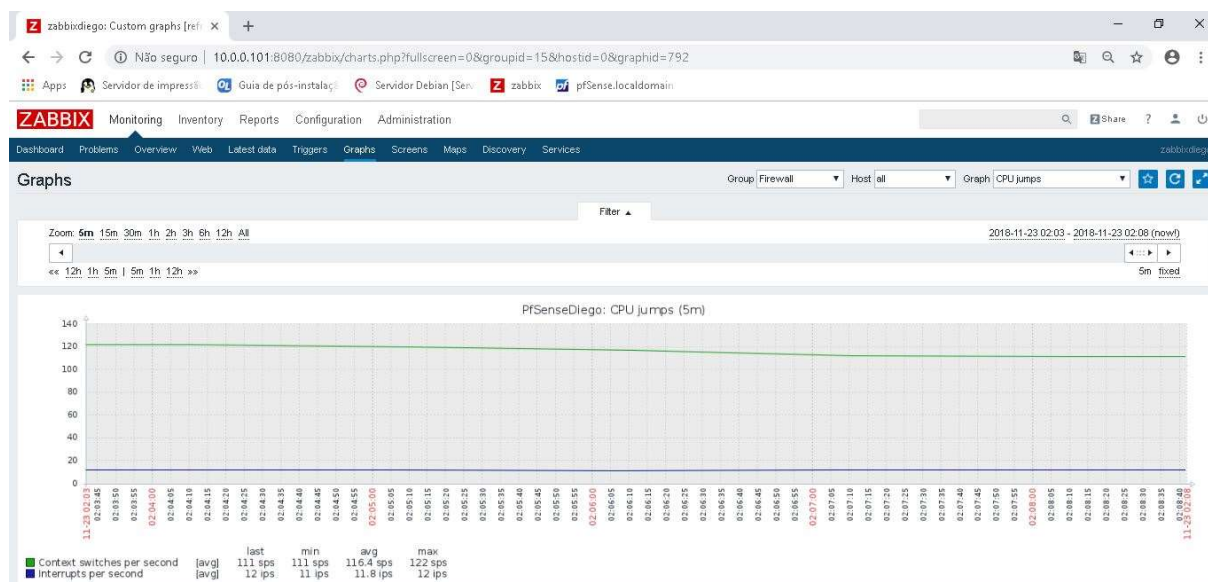
Rede do Servidor



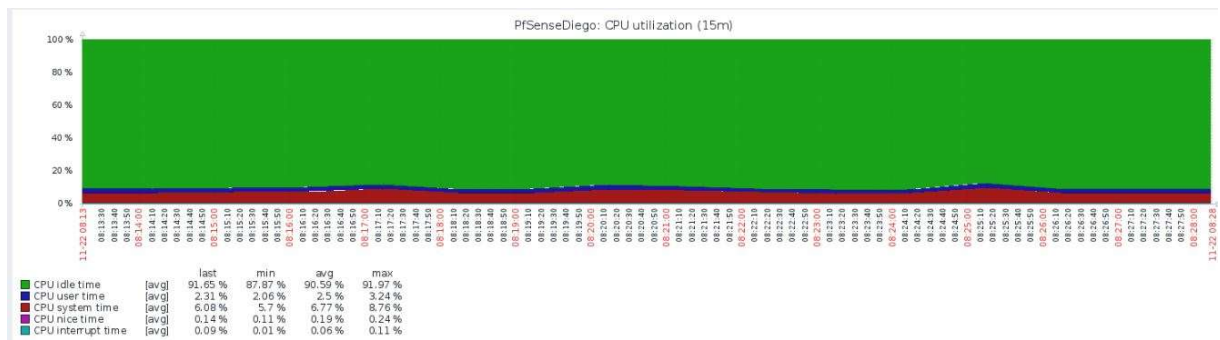


IP 192.168.15.252

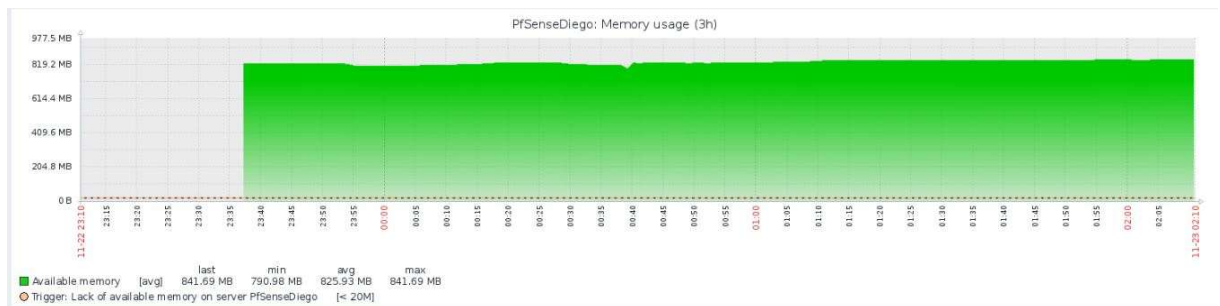
Observação: Pela Máquina Real (IP 192.168.1.252) redirecionado para pfsense:8080zabbix



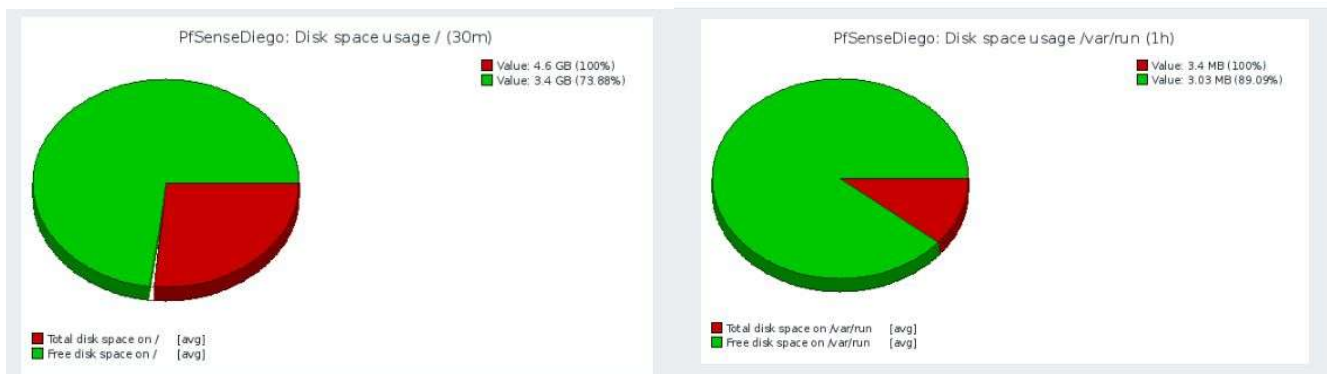
Pfsense CPU Jump



Utilização de CPU Pfsense

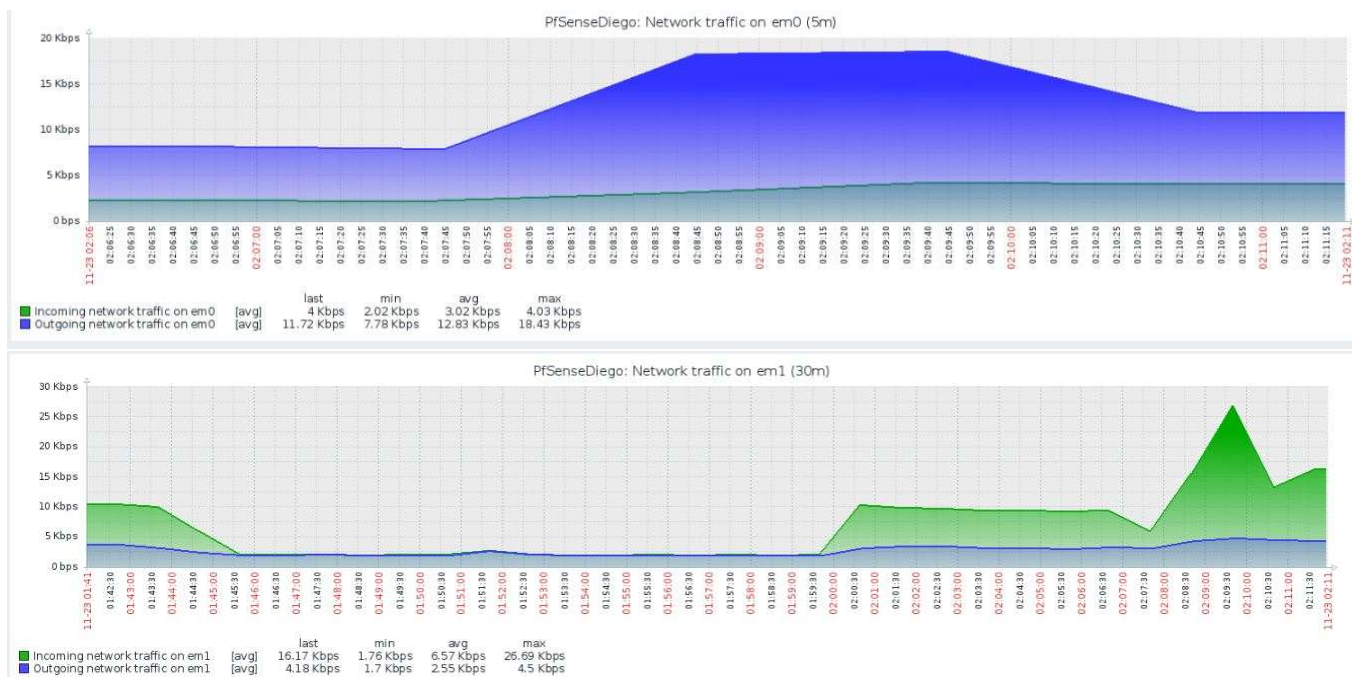


Uso de memória - Pfsense



Uso de Disco do Pfsense





Network PfSense

## VII. Servidor FTP

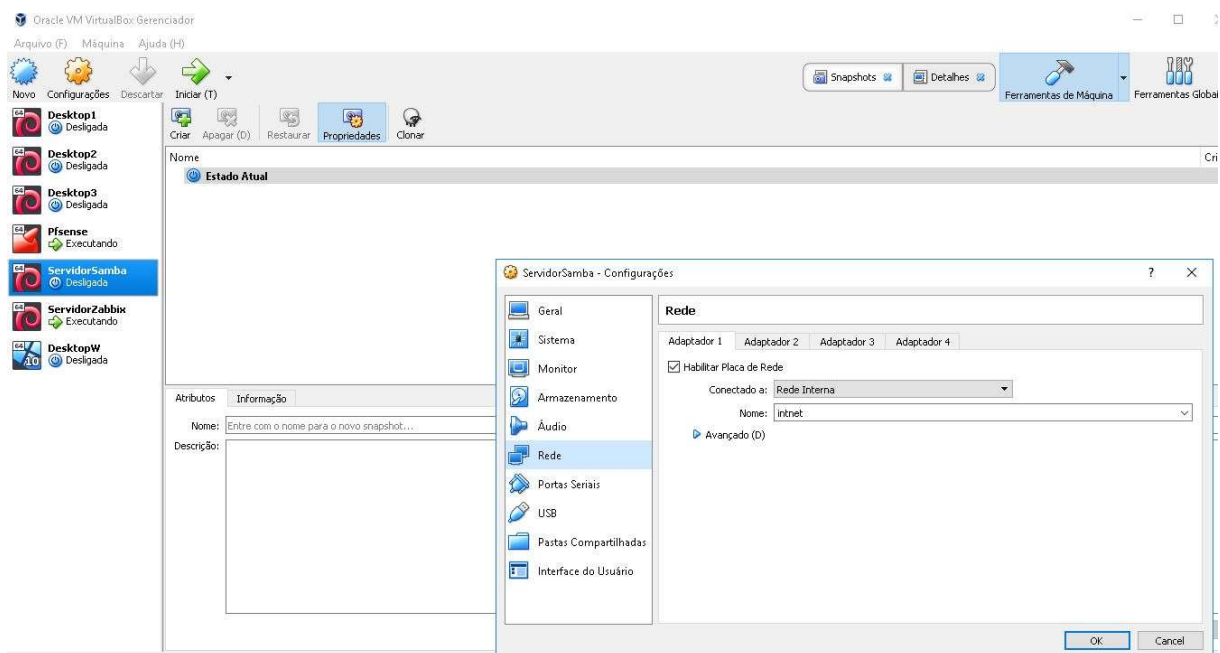
Foi criado um servidor de arquivos com o Samba, que utiliza o protocolo SMB (Server Message Block). Este protocolo é utilizado para o compartilhamento de arquivos na rede. A transferência de dados em redes de computadores envolve a transferência dos arquivos, em uma rede empresarial, serve para o acesso aos sistemas de arquivos internos, podendo ser utilizado também por equipamentos como relógios de ponto eletrônico, impressoras ou scanners de rede.

```
Linux debiandiego 4.9.0-7-amd64 #1 SMP Debian 4.9.110-3+deb9u2 (2018-08-13) x86_64

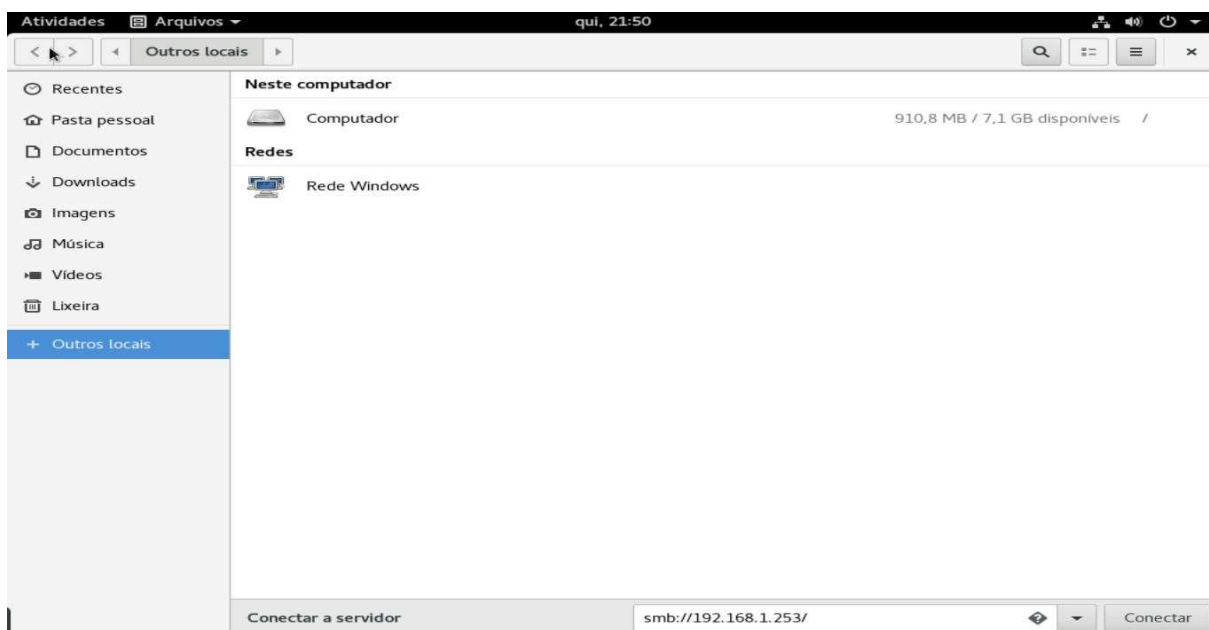
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
diego@debiandiego:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    group default qlen 1000
    link/ether 08:00:27:7f:6e:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.253/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe7f:6eb6/64 scope link
        valid_lft forever preferred_lft forever
diego@debiandiego:~$
```

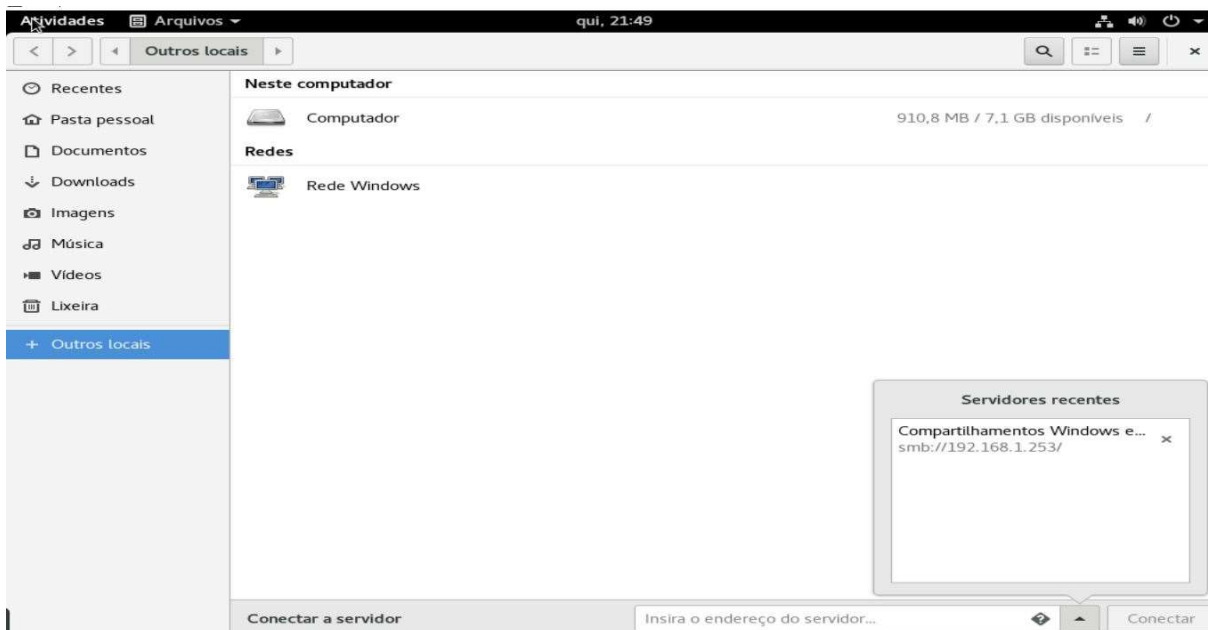
Acesso ao Servidor - IP 192.168.1.253



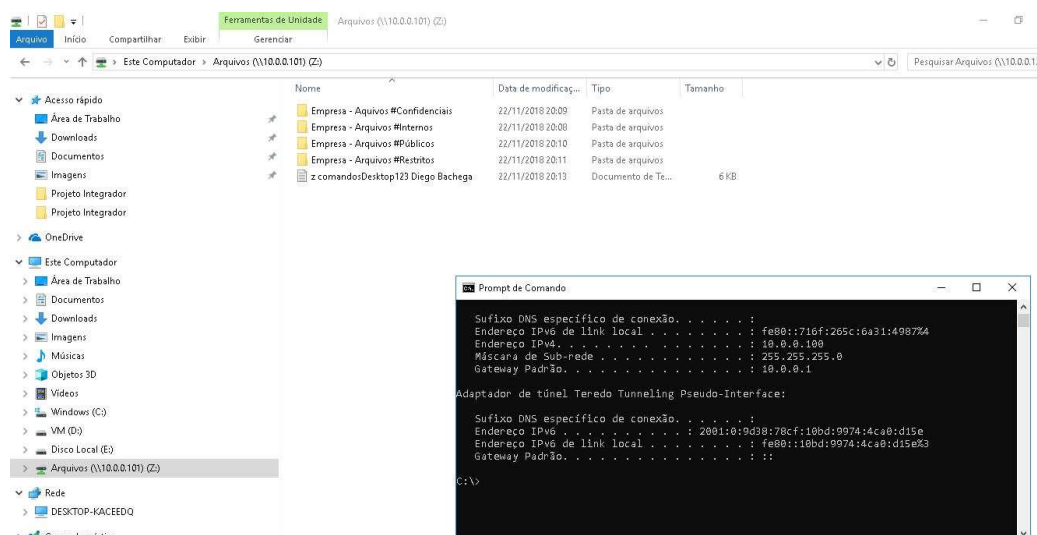
Configuração de Rede: Interna



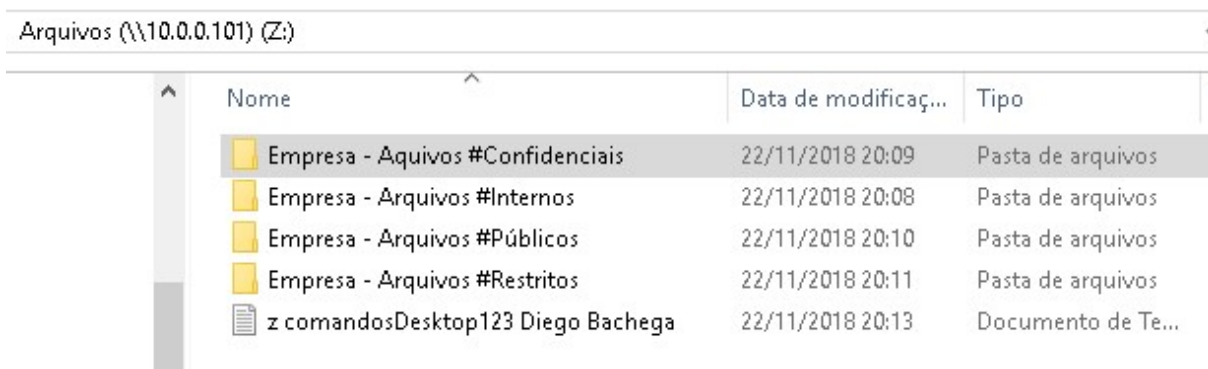
Acessando o Compartilhamento de Arquivos SMB://192.168.1.253/



Acessando o Compartilhamento após reiniciar a máquina.



Acesso ao Servidor através da maquina real ( fora do VirtualBox)



Compartilhamento criado para a empresa fictícia

## 6 Registros de Logs

Todos os registros foram anexados no <https://github.com/diegobachega/Projeto-Integrador-Implementacao-de-Seguranca>. Para a análise da evolução, a maioria dos logs antigos foram inseridos no Github após a conclusão do projeto. Isso ocorreu porque os sistemas foram refeitos várias vezes e a maioria desses logs apresentam as configurações que não deram certo.

## 7 Conclusão

Inicialmente, foi feito um estudo para apresentação do pré-projeto, com definição de cronograma básico com as etapas que seriam seguidas e uma definição da arquitetura a ser apresentada. Esta entrega foi feita através do GitHub em 21/09/18.

A construção do projeto foi a segunda fase, feita sob a supervisão do professor através dos reportes de versionamento via GitHub. Os reportes de versionamentos foram feitos em 21/09, 22/10, 24/10, 07/11, 18/11 e 19/11. O aplicativo GitHub desktop estava apresentando erros de upload devido ao tamanho limitado de arquivos. Por isso, optou-se por fazer o upload dos arquivos direto no site.

Durante o desenvolvimento do projeto, ocorreram diversos problemas que foram resolvidos caso a caso. Um exemplo foi o aplicativo pré-instalado BlueStacks que derrubou o Virtual Box, corrompendo o programa de tal forma que só foi possível reinstalá-lo depois de formatar o computador Acer. Outra dificuldade foi encontrar a configuração correta de rede, desde o roteador da operadora, que bloqueia e derruba automaticamente redes virtuais, até os servidores e as estações de trabalho devidamente instalados na rede interna com o firewall na borda, com a rede passando por ele.

A metodologia utilizada foi unificada com pesquisas em arquivos de outras matérias IESB concluídas durante este curso de segurança, fóruns, sites e videoaulas. O sistema operacional era diferente do padrão utilizado e não se possuía domínio sobre as tecnologias necessárias para construção do projeto. Neste contexto, houve diversos obstáculos que foram superados com investimentos em novos hardwares, tempo e estudo, como por exemplo, a baixa capacidade de processamento do computador Acer que desencadeou em lentidão na rede, deixando a construção onerosa, reduzindo a velocidade de evolução até chegar a parar devido a corrupção de arquivos no HD. A reconstrução só foi possível com a aquisição de outro dispositivo, para evitar passar muito tempo sem progressos.

O projeto foi concluído com sucesso em 22/11/2018, e ficou composto por dois servidores, um para compartilhamento de arquivos e outro para monitoramento do firewall com a solução Zabbix, ambos com Debian sem interface gráfica. As 3 estações de trabalho foram testadas uma a uma, devido a falta de recursos de

processamento para ligá-las ao mesmo tempo. O appliance virtual firewall PfSense funcionou corretamente durante o período de testes, conforme relatórios postados.

A idéia é que este projeto será reaproveitado para uso pessoal. Os dois servidores virtuais ficarão em uma arquitetura nova, voltado para o uso caseiro, redesenhada de tal forma que será possível ser acessada pelo celular.

## **8 Referências Bibliográficas**

### Sites

- [www.blogopcaolinux.com.br/2017/06/Guia-de-instalacao-do-Debian-9-Stretch.html](http://www.blogopcaolinux.com.br/2017/06/Guia-de-instalacao-do-Debian-9-Stretch.html);
- [www.haulaead.thinkific.com/courses/take/curso-gratis-servidor-linux](http://www.haulaead.thinkific.com/courses/take/curso-gratis-servidor-linux);
- <https://www.pfsense.org/download>;
- <https://www.debian.org>
- <https://www.blogopcaolinux.com.br>
- <https://www.vivaolinux.com.br>
- <http://www.minhaconexao.com.br>
- <https://sempreupdate.com.br/instalandozabbix-server-4-0-no-debian-9-strech>