

DANIEL LENHARO DE SOUZA

SENDO SYSADMIN COM SOFTWARE LIVRE



\$whoami

> Daniel Lenharo de Souza

- > Técnico de Redes na CELEPAR
- > Mestrando em Redes e Sistemas Distribuídos

- > Ativista de Software Livre
- > Usuário Debian
- > Membro da Comunidade Debian
- > Membro da Comunidade Curitiba Livre
- > Associado da Associação de Software Livre – ASL org

Programa

- * O que é ser SYSADMIN?
- * O que é Software Livre?
- * Estrutura Básica de rede
- * Serviços de Rede

O que é ser SYSADMIN?

O que é ser SYSADMIN?

É ir além do Sistema Operacional, precisa pensar sua infraestrutura, precisa se preocupar com a velocidade na entrega de aplicações, precisa se preocupar como ajudar Desenvolvedores e o negócio a ganhar eficiência operacional, reduzir custos e maximizar os ganhos.

SYSADMIN

Curiosidade

Se você não tem curiosidade para saber como as coisas funcionam, terá dificuldade para evoluir na carreira de sysadmin e provavelmente em muitas outras carreiras.

Quem é curioso tende a ser mais fuçador e a não se contentar com a frase “é assim mesmo” ou “sempre foi assim”. Ele quer descobrir o porquê das coisas e não sossega enquanto não descobre uma solução para aquele problema.

SYSADMIN

Persistência

Quem é curioso também tem mais persistência e não confunde persistência com teimosia. Existe uma linha muito tênue que separa estas 2 características. Teimosia é quando você continua fazendo as mesmas coisas para tentar chegar a um resultado e, persistência é quando você tenta coisas diferentes para chegar a um resultado.

SYSADMIN

Iniciativa

Profissional que não tem iniciativa e que não chama para si a responsabilidade, não é visto como um bom SYSADMIN.

Perceba que se você não for curioso e não for persistente, provavelmente não terá iniciativa.

SYSADMIN

Faça parte da solução

Não sente em cima do problema e fique dando voltas em torno dele. Isso faz com que o profissional faça parte do problema e não da solução.

foco na solução e não no problema.

2% das pessoas fazem parte do problema

8% fazem parte da solução

90% restantes fazem parte da paisagem.

Fazer parte da paisagem é ser inerte e seguir a boiada, o conhecido “maria vai com as outras”.

SYSADMIN

Se capacitar

Todo sysadmin precisa estar em constante aprendizado e sempre se capacitando para aprender algo novo.

SYSADMIN

Treino

Não adianta aprender novas habilidades e não colocá-las em prática.

Você precisa colocar tudo que aprende em prática e isso chama-se treino. O ex-jogador de basquete Oscar Schmidt disse em uma matéria na revista Superinteressante que o seu sucesso deve-se a muito treino. Quando mais você treina, melhor você se torna naquilo.

SYSADMIN

Paixão (brilho nos olhos)

Essa é a característica mais importante de qualquer profissional. Ele precisa ter paixão pelo que faz.

O que é Software Livre

O que é Software Livre

Free software is software that gives you the user the freedom to share, study and modify it. We call this free software because the user is free.

<http://www.fsf.org/about/what-is-free-software>

O que é Software Livre

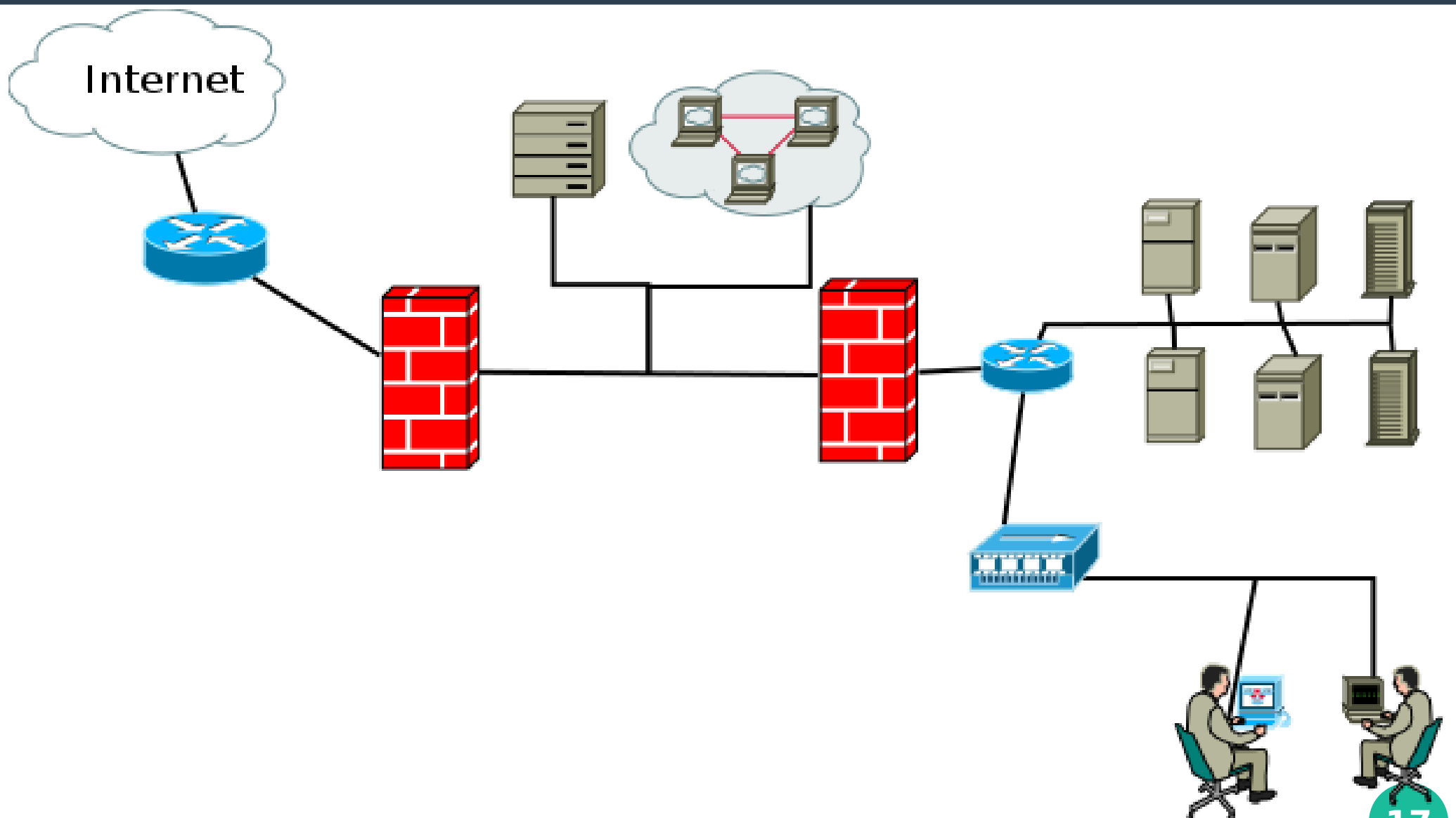
Um programa é Software Livre se os usuários têm as quatro liberdades essenciais:

0. A liberdade de executar o programa como quiser, para qualquer fim
1. A liberdade de estudar como o programa funciona, e alterá-lo para que ele faz sua computação como você deseja.
2. A liberdade de redistribuir cópias de modo que você possa ajudar ao seu próximo.
3. A liberdade de distribuir cópias de suas versões modificadas para os outros. Ao fazer isso você pode dar toda a comunidade a oportunidade de se beneficiar de suas alterações.

<http://www.gnu.org/philosophy/free-sw.html>

Estrutura Básica de rede

Estrutura Básica de rede

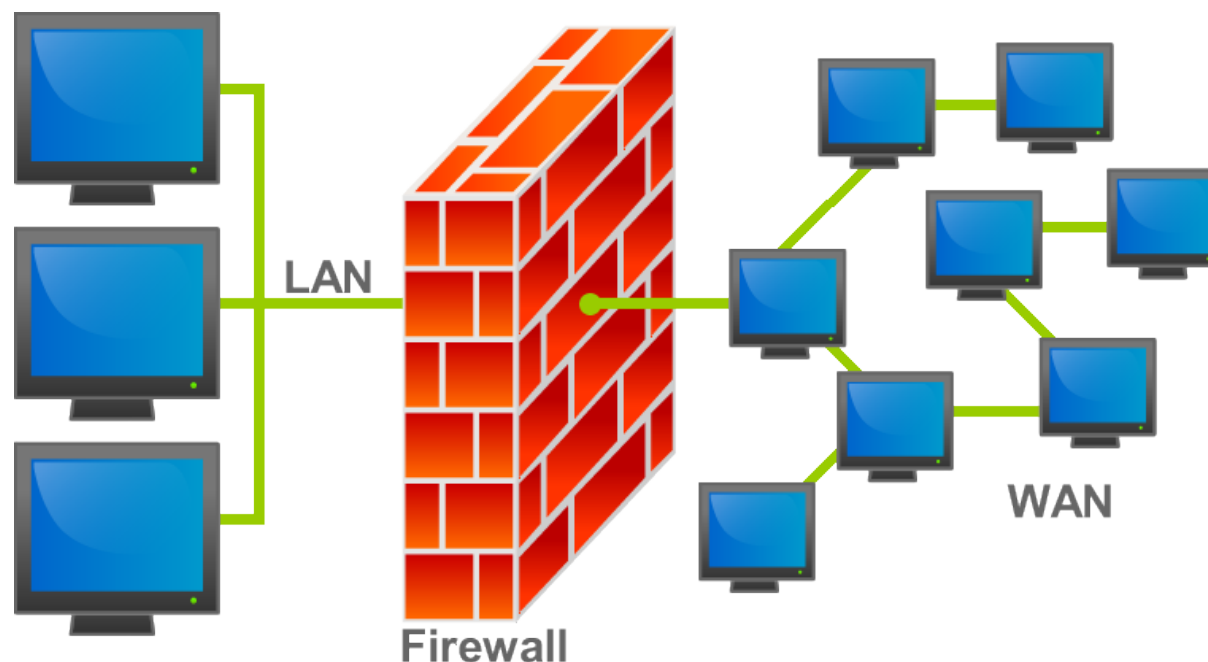


Serviços de Rede

Serviços de Rede - FIREWALL

* Firewall

Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede



Serviços de Rede - FIREWALL

Opções:

- Iptables
- IPFire
- Endian
- PFSense

Serviços de Rede - FIREWALL

Opções:

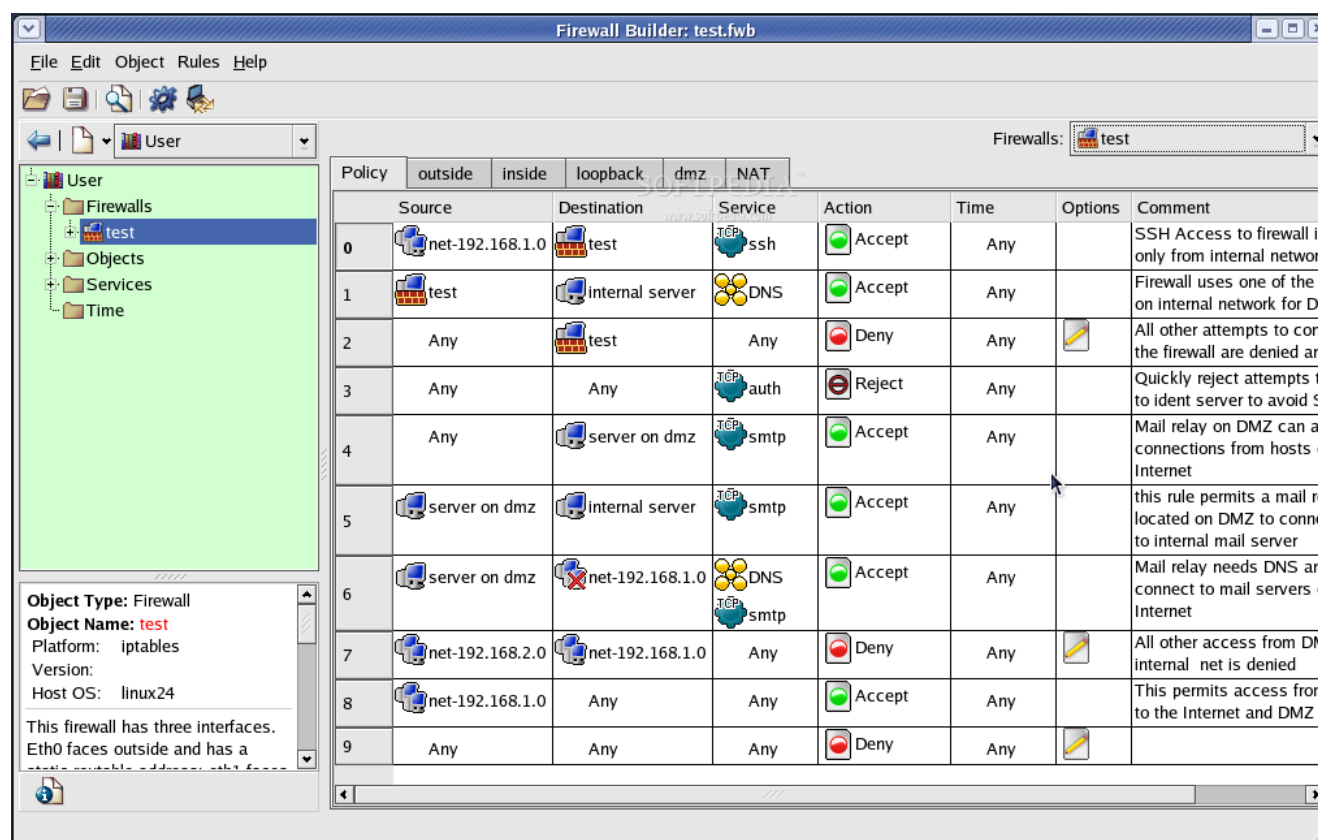
- **Iptables**
- IPFire
- Endian
- PFSense

O iptables é um firewall em nível de pacotes e funciona baseado no endereço/porta de origem/destino do pacote, prioridade, etc. Ele funciona através da comparação de regras para saber se um pacote tem ou não permissão para passar. Em firewalls mais restritivos, o pacote é bloqueado e registrado para que o administrador do sistema tenha conhecimento sobre o que está acontecendo em seu sistema.

Serviços de Rede - FIREWALL

Opções:

- Iptables + Fwbuilder
- IPFire
- Endian
- PFSense



Serviços de Rede - FIREWALL

Opções:

- Iptables + Fwbuilder

- **IPFire**

- Endian

- PFSense

IPfire é uma distribuição GNU/Linux, desenhada especificamente para prover as funções de FIREWALL e roteamento em rede local.

Interface Web de gerenciamento para facilitar a configuração.

Servidor Proxy.

Sistema de detección de intrusos en una red o equipo.

VPN a través de IPsec y OpenVPN.

Servidor DHCP.

Caché de nombres de dominio.

Servidor horario.

Wake-on-Lan.

Servidor DDNS.

QoS.

Completo Log de todos los sucesos que ocurren en el sistema.

Serviços de Rede - FIREWALL

The screenshot displays the IPFire web interface in a Mozilla Firefox browser window. The browser's address bar shows the URL `https://ipfire.cosc.tu:444/cgi-bin/connections.cgi`. The interface features a navigation menu with tabs for 'system', 'status', 'network', 'services', 'firewall', 'ipfire', and 'logs'. The 'status' tab is currently selected.

The main content area is titled 'iptables connection tracking' and includes a legend for network zones: LAN (green), INTERNET (red), DMZ (orange), Wireless (blue), IPFire (black), VPN (purple), and OpenVPN (teal). Below the legend, there are dropdown menus for 'Protocol:' (set to 'All') and 'Connection Status:' (set to 'All'), along with an 'Update' button.

The connection tracking table shows the following data:

Source IP: Port	Dest. IP: Port	Protocol:	Connection Status	Expires (Secs)
172.16.1.3 50889	192.168.1.2 444 (SNPP)	tcp	ESTABLISHED	119:59:59
172.16.1.100 49158	23.3.109.11 80 (HTTP)	tcp	ESTABLISHED	119:59:39
172.16.1.100 49160	192.168.1.68 80 (HTTP)	tcp	TIME_WAIT	0:01:42
172.16.1.100 49159	192.168.1.68 80 (HTTP)	tcp	TIME_WAIT	0:01:41
172.16.1.100 49157	64.4.18.90 80 (HTTP)	tcp	TIME_WAIT	0:00:33
172.16.1.100 62357	192.168.1.60 53 (DOMAIN)	udp		0:00:11
172.16.1.100 56453	192.168.1.60 53 (DOMAIN)	udp		0:00:09
192.168.1.2	192.168.1.1	icmp		0:00:02

On the right side of the interface, there is a 'sidemenu' with links to various system components: System, Memory, Services, Media, Network (external), Network (internal), Network (other), Hardware Graphs, Connections, and Net-Traffic.

Serviços de Rede - FIREWALL

Opções:

- Iptables
- IPFire
- **Endian**
- PFSense

The screenshot displays the Endian Firewall Community web interface. The top navigation bar includes 'System', 'Status', 'Network', 'Services', 'Firewall', 'Proxy', 'VPN', and 'Logs'. The main content area is divided into several sections:

- Dashboard:** Overview for 'efw-1256732343.localdomain' showing Appliance (Community), Version (2.3.0), and Uptime (7m).
- Hardware information:** Resource usage for CPU 1 (6%), Memory (6% / 1010 MB), Swap (0% / 512 MB), Main disk (4% / 13 GB), Data disk (5% / 42 GB), /var/efw (6% / 99 MB), and /var/log (1% / 20 GB).
- Services (Live log):** HTTP Proxy, SMTP Proxy, POP3 Proxy, and Intrusion Detection are all shown as OFF.
- Network Interfaces:** Table showing br0 and eth0, both Up, with In and Out traffic rates.
- Incoming traffic in KB/s (max. 6 interfaces):** Line graph showing traffic for br0.
- Outgoing traffic in KB/s (max. 6 interfaces):** Line graph showing traffic for br0.
- Uplinks:** Table with columns Name, IP Address, Status, Active, and Managed.

Status: Idle Uptime: 12:26:41 up 7 min, 0 users, load average: 0.13, 0.32, 0.22

Serviços de Rede - FIREWALL

Opções:

- Iptables
- IPFire
- **Endian**
- PFSense

Current rules:

Add a new rule:

Log accepted outgoing connections

Save

Proto	Source	Destination	Policy: log	Remark	Action				
TCP	GREEN	ALL : 80(HTTP)	✓	allow HTTP	↑	↓	☑	✎	🗑
TCP	GREEN	ALL : 443(HTTPS)	✓	allow HTTPS	↑	↓	☑	✎	🗑
TCP	GREEN	ALL : 21(FTP)	✓	allow FTP	↑	↓	☑	✎	🗑
TCP	GREEN	ALL : 25(SMTP)	✓	allow SMTP	↑	↓	☑	✎	🗑
TCP	GREEN	ALL : 110(POP3)	✓	allow POP	↑	↓	☑	✎	🗑
TCP	GREEN	ALL : 143(IMAP)	✓	allow IMAP	↑	↓	☑	✎	🗑
TCP	GREEN	ALL : 53(DOMAIN)	✓	allow DNS	↑	↓	☑	✎	🗑
UDP	GREEN	ALL : 53(DOMAIN)	✓	allow DNS	↑	↓	☑	✎	🗑
TCP	BLUE	ALL : 53(DOMAIN)	✓	allow DNS	↑	↓	☑	✎	🗑
UDP	BLUE	ALL : 53(DOMAIN)	✓	allow DNS	↑	↓	☑	✎	🗑
TCP	ORANGE	ALL : 53(DOMAIN)	✓	allow DNS	↑	↓	☑	✎	🗑
UDP	ORANGE	ALL : 53(DOMAIN)	✓	allow DNS	↑	↓	☑	✎	🗑

Legend: Enabled (click to disable) Disabled (click to enable) ✎ Edit 🗑 Remove

Serviços de Rede - FIREWALL

Opções:

- Iptables
- IPFire
- Endian
- PFSense

System Interfaces Firewall Services VPN Status Diagnostics Gold Help pfSense

Firewall: NAT: Outbound

Port Forward 1:1 Outbound NPt

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
<input type="checkbox"/> WAN	127.0.0.0/8	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP - localhost to WAN
<input type="checkbox"/> BLACKVPNINTERFACE	127.0.0.0/8	*	*	500	BLACKVPNINTERFACE address	*	YES	Auto created rule for ISAKMP - localhost to WAN
<input type="checkbox"/> WAN	127.0.0.0/8	*	*	*	WAN address	*	NO	Auto created rule - localhost to WAN
<input type="checkbox"/> BLACKVPNINTERFACE	127.0.0.0/8	*	*	*	BLACKVPNINTERFACE address	*	NO	Auto created rule - localhost to WAN

Serviços de Rede - DNS

* DNS

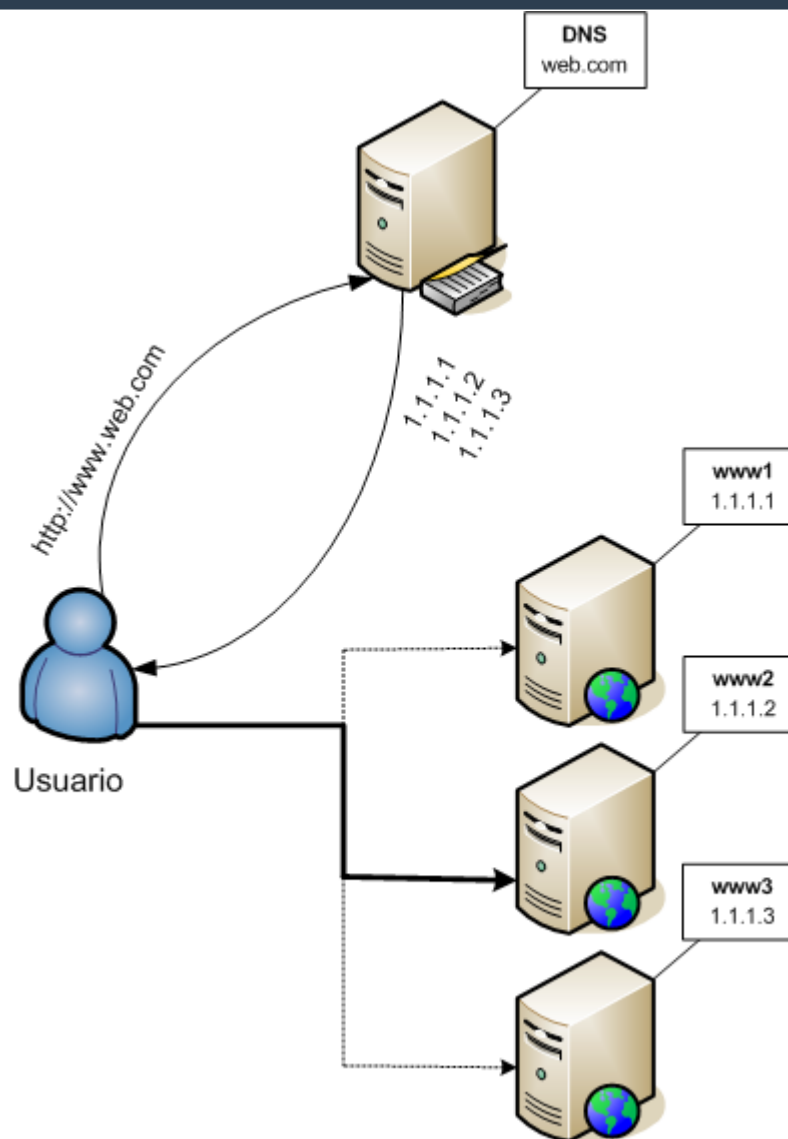
Sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada. Ele baseia-se em nomes hierárquicos e permite a inscrição de vários dados digitados além do nome do host e seu IP

Serviços de Rede - DNS

* DNS

- BIND

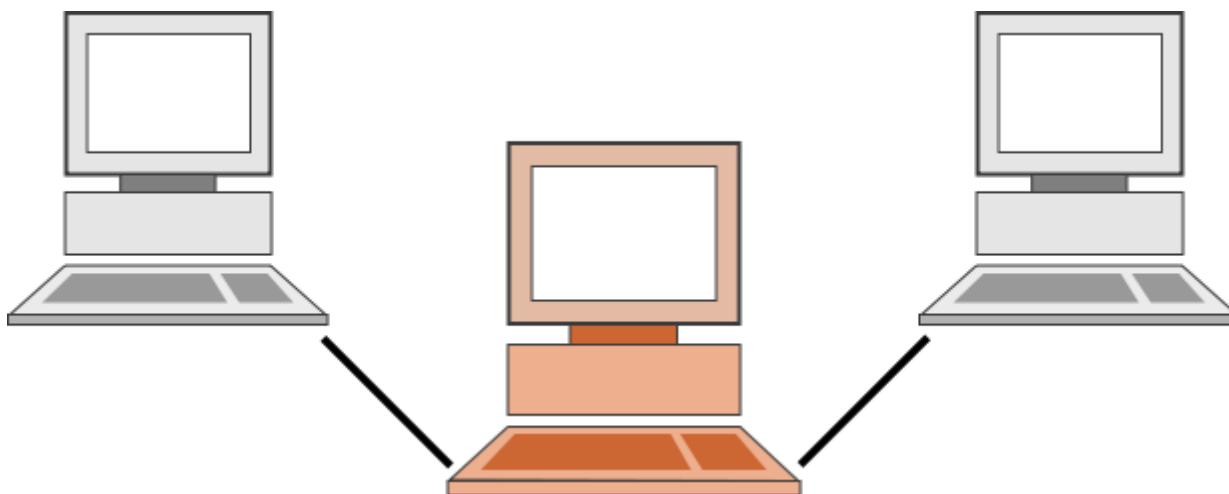
- PowerDNS



Serviços de Rede - PROXY

* Proxy

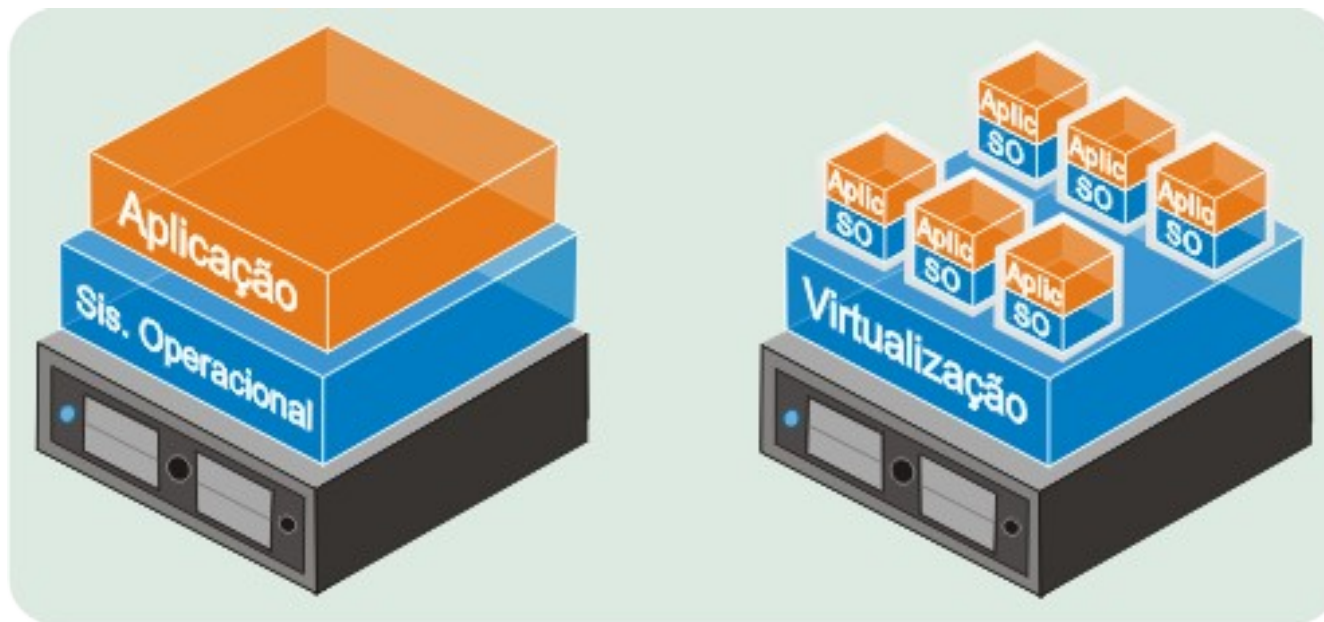
Proxy é um serviço de rede que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.



VIRTUALIZAÇÃO

* VIRTUALIZAÇÃO

Virtualização, basicamente, é a técnica de separar aplicação e sistema operacional dos componentes físicos.



Arquitetura Tradicional x Virtualização

VIRTUALIZAÇÃO

* VIRTUALIZAÇÃO

- KVM
- Xen
- OpenVZ

BACKUP

* Backup

Backup é a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

BACKUP

* Backup

- **Bacula**

- **Amanda**

- BackupNinja

- **Backuppc**

-UrBackup

Banco de Dados

- * BANCO DE DADOS

- * MySql

- * PostgreSQL

- * MongoDB

- * Mariadb

Email

* E-mail

Um serviço que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação.

- Zimbra

- Expresso

ARQUIVOS

* Servidor de Arquivos

Servidor de arquivos é um computador conectado a uma rede que tem o objetivo principal de proporcionar um local para o armazenamento compartilhado de arquivos de computadores (como documentos, arquivos de som, fotografias, filmes, imagens, bases de dados, etc) que podem ser acessados pelo trabalho que estão ligados à rede de computadores.

ARQUIVOS

* Servidor de Arquivos



ARQUIVOS

* Servidor de Arquivos

A screenshot of the FreeNAS web interface. The top navigation bar includes System, Network, Storage, Sharing, Services, Plugins, Jails, Reporting, Account, Help, Log Out, and Alert. The left sidebar shows a tree view with categories like Account, System (with sub-items like Cron Jobs, Init/Shutdown Scripts, NTP Servers, Rsync Tasks, S.M.A.R.T. Tests, Settings, Sysctls, Tunables), Network, Storage, and Periodic Snapshot Tasks. The main content area displays "System Information" with a table of system details.

Hostname	freenas.freenas.tld	Edit
Build	FreeNAS-9.2.1.5-RELEASE-x64 (80c1d35)	
Platform	AMD A6-5400K APU with Radeon(tm) HD Graphics	
Memory	7614MB	
System Time	Mon May 26 13:31:13 PDT 2014	
Uptime	1:31PM up 37 secs, 0 users	
Load Average	1.82, 0.58, 0.22	

ARQUIVOS

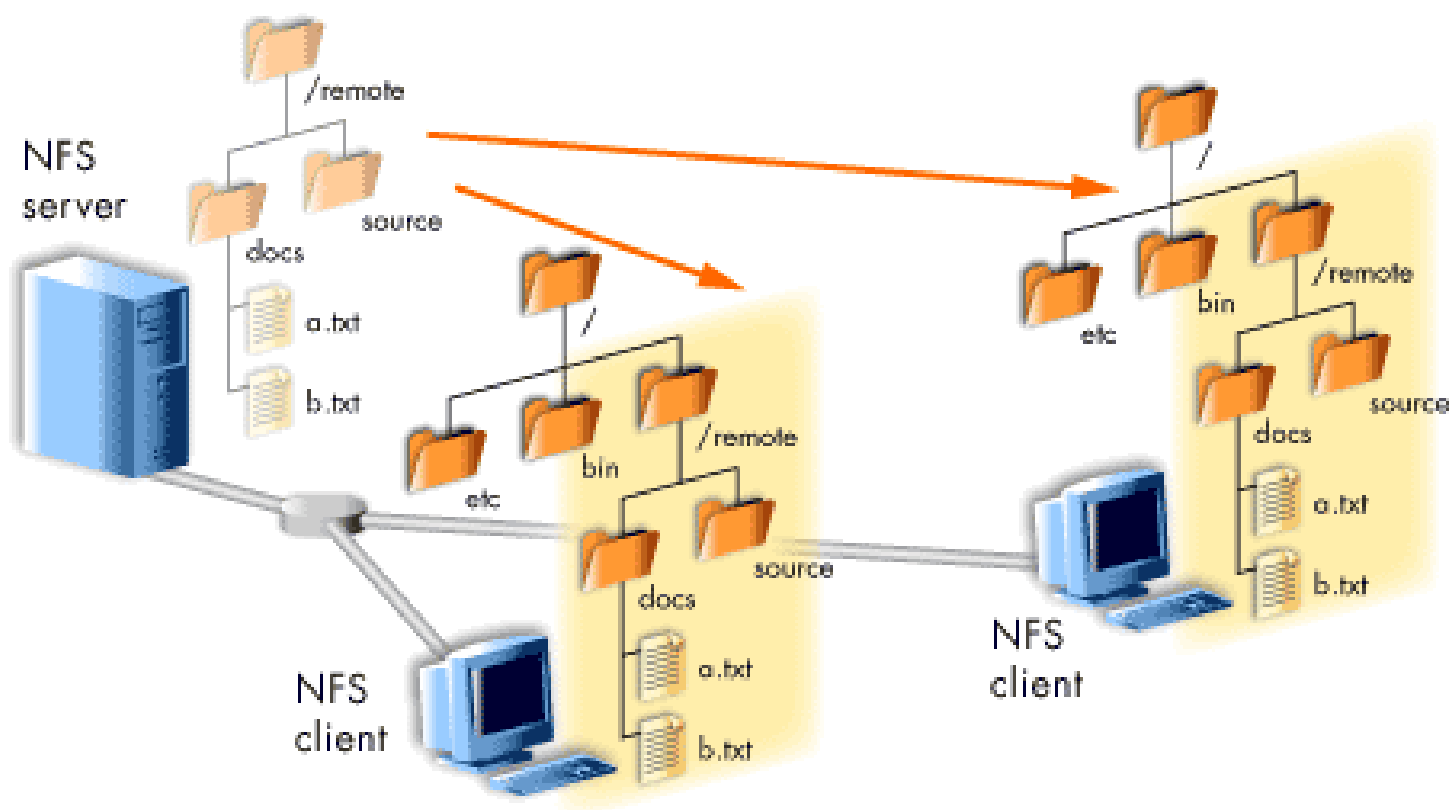
* Servidor de Arquivos

samba



FreeNAS™

NFS
NETWORK FILE SYSTEM



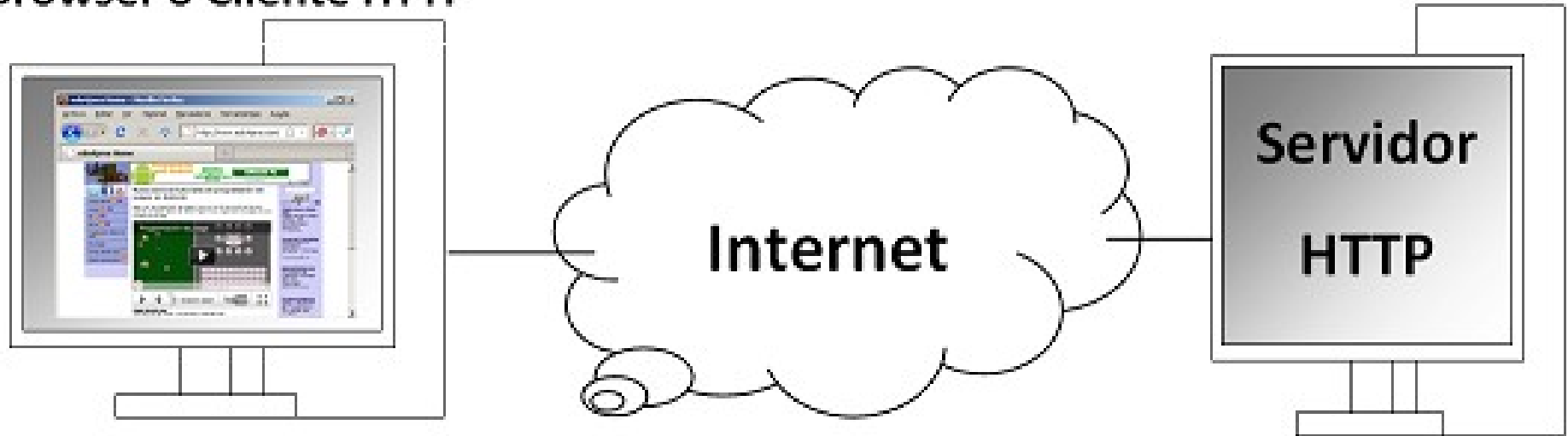
The NFS server exports the /remote filesystem to two NFS clients.

HTTP

* Servidor HTTP

É um programa de computador responsável por aceitar pedidos HTTP de clientes, geralmente os navegadores, e servi-los com respostas HTTP.

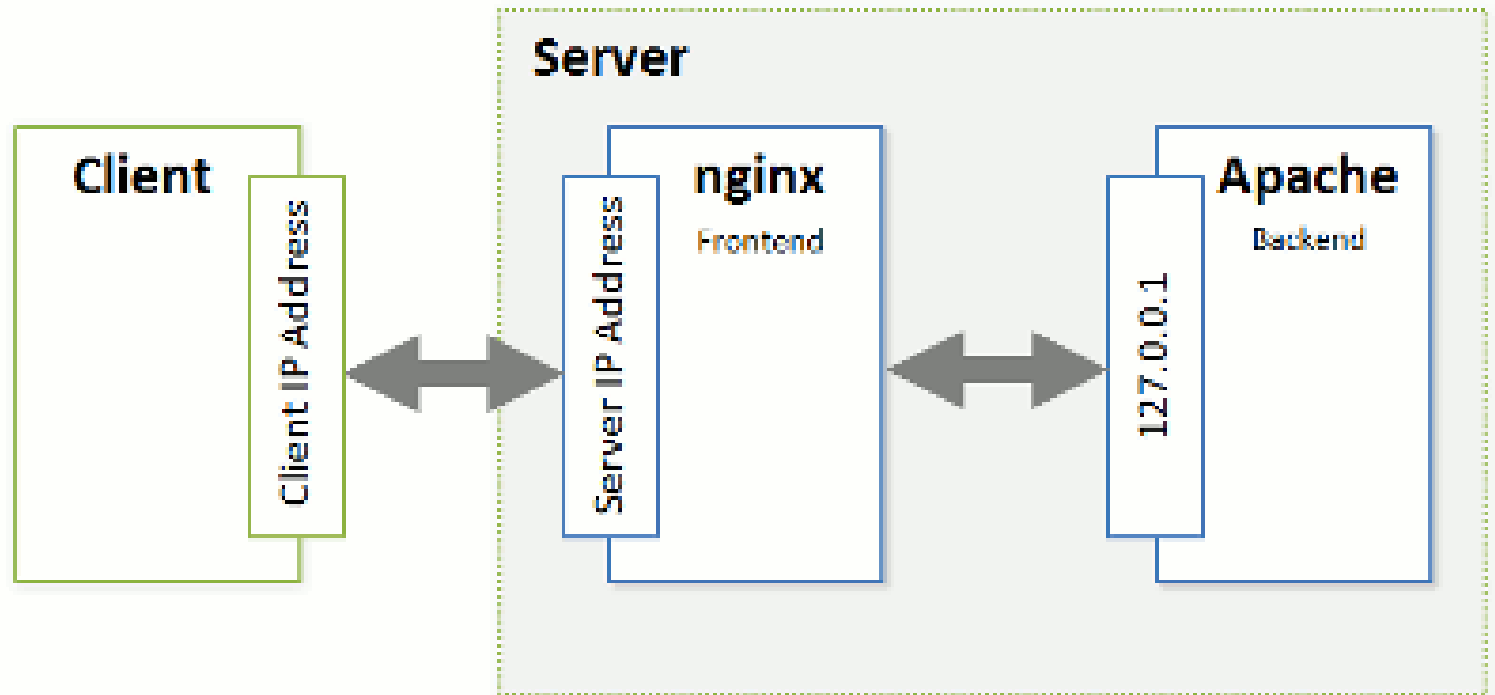
Browser o Cliente HTTP



HTTP

* Servidor HTTP

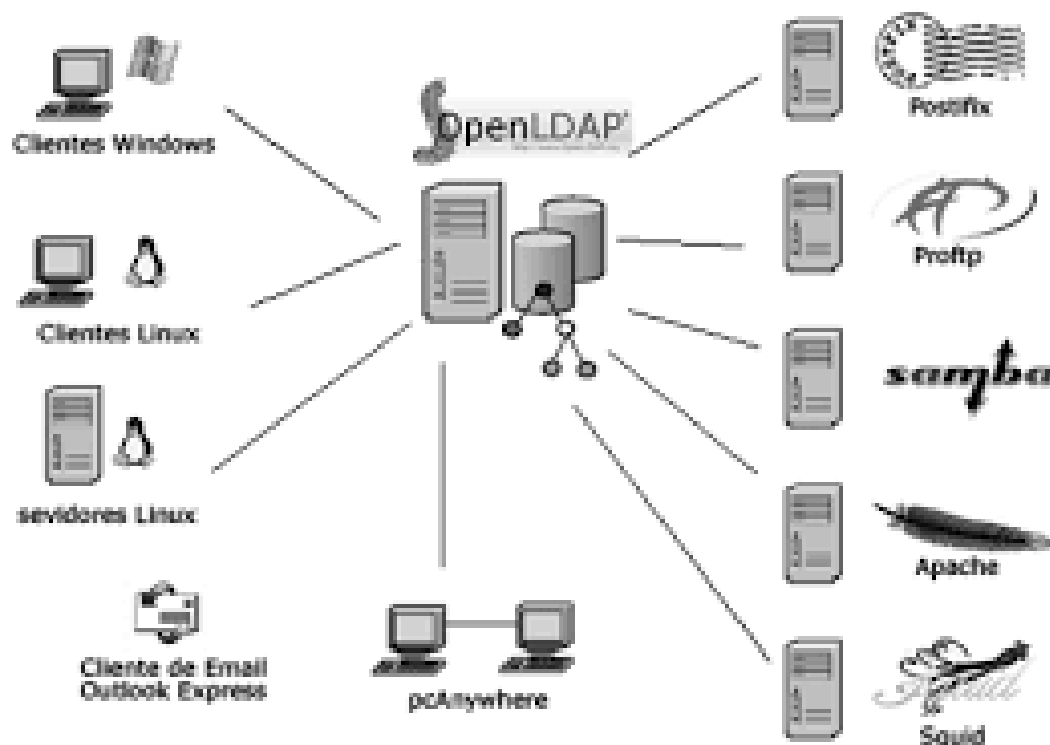
- Apache
- NGINX
- lighttpd



AUTENTICAÇÃO

* Servidor de Autenticação

Serviço de rede responsável por controlar e gerenciar as credenciais de acesso, de forma centralizada e segura.



AUTENTICAÇÃO

* Servidor de Autenticação

- LDAP
- Kerberos
- Samba
- Samba 4

CLONAGEM

- * Clonagem de disco
 - Clonezilla
 - FOG

VoIP

* VoIP

VoIP é o roteamento de conversação humana usando a Internet ou qualquer outra rede de computadores baseada no Protocolo de Internet, tornando a transmissão de voz mais um dos serviços suportados pela rede de dados.

- Asterix
(elastix)

MONITORAMENTO

* Monitoramento

Poder acompanhar o que acontece em sua rede é fundamental, por isso é importante a utilização de Sistemas de monitoramento.

MONITORAMENTO

* Monitoramento

- Nagios
- Zabbix
- Cacti
- NeDi
- Observium

DEPLOY

* Automatização de processos

- PUPPET

- CHEF

- ANSIBLE

QUAL O PROBLEMA?

OBRIGADO

daniel@lenharo.eti.br

