



MUM

Mikrotik User's Meeting

Rio de Janeiro - 2009

Mikrotik e a Computação nas nuvens

Maila Networks



- Oferece serviços de Conectividade IP, Desenvolvimento e Integração de Sistemas.
- Consultoria `a Provedores de Acesso, Clientes Governamentais e Privados.

Jean R. Franco:

Formado como Administrador de Sistemas Unix pela Universidade da Califórnia-EUA.

Certificações: MCSE, CCNA, Apple Specialist, Network+, entre outras.

Experiências: 07 anos como Engenheiro de Telecomunicações pela AT&T (EUA),
04 anos como Engenheiro de Comunicação IP pela MITEL (Canadá),

Usuário Mikrotik desde 2000

Maila Networks

Problemas atuais

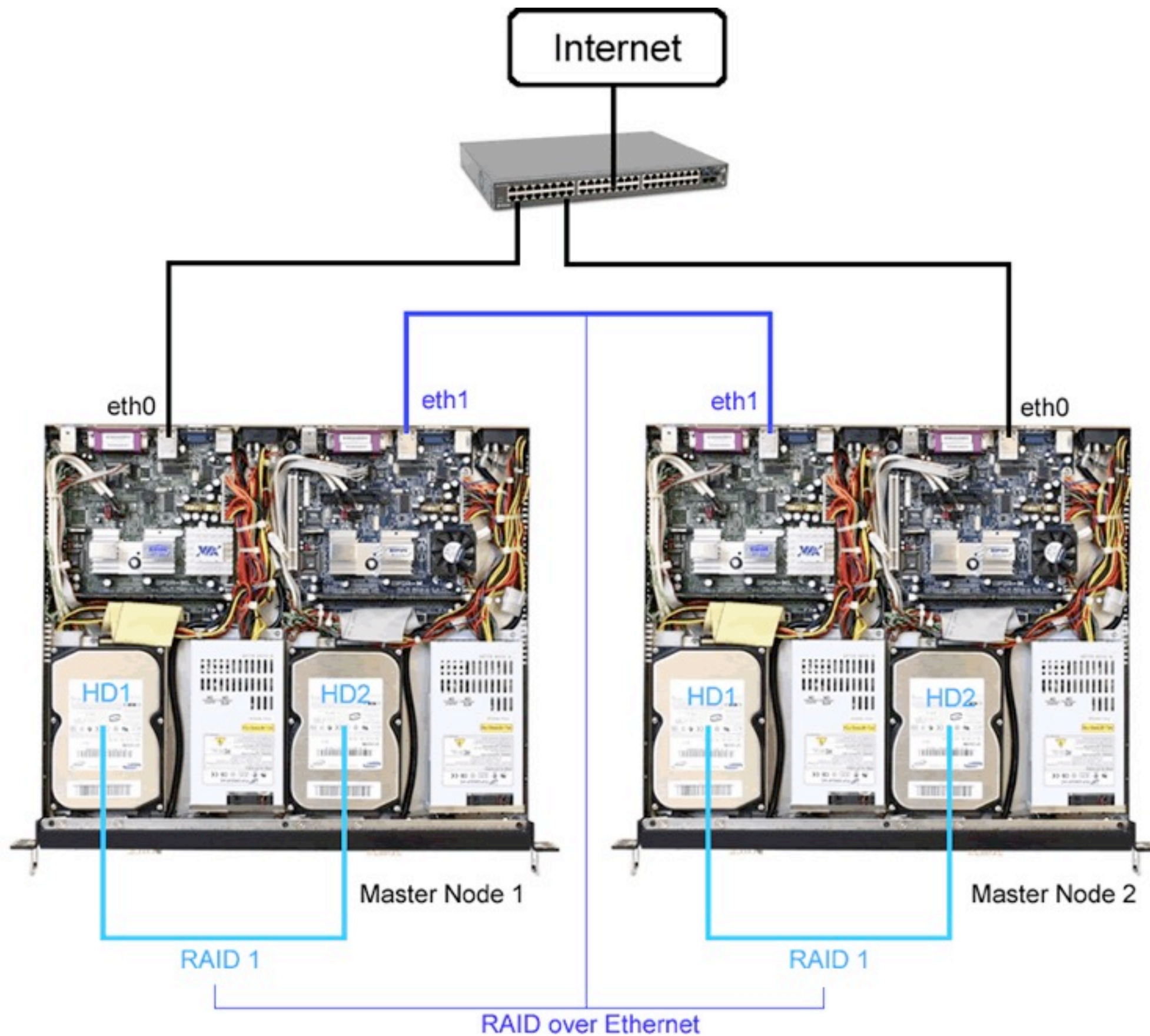
- Interrupção de serviços
- Apagão + ausência de UPS = falha de hardware
- Manutenção de sistemas
- Falha de hardware em geral
- Ausência de escalabilidade de sistemas

Maila Networks

Soluções

- High Availability (Alta Disponibilidade)
- VRRP
- CARP
- Cloud Computing com clusters

Maila Networks



Maila Networks

COMPUTAÇÃO NAS NUUVENS

O conceito de Cloud está associado a Software as a Service (SAAS), Plataform as a Service (PAAS) e Infrastructure as a Service (IAAS).

Exemplos de destaque desta tecnologia: Google Docs, EyeOS, Xcerion AB, novos módulos do OpenOffice, WebEx, Facebook, etc.

Quais os benefícios da computação nas nuvens e como podemos utilizar o Mikrotik com esta tecnologia?



Vantagens

- Economia de espaço e investimento;
- Contribui com o meio ambiente;
- Possibilita a redundância de sistemas;
- Possibilidade de expansão em segundos;
- Gerenciamento centralizado e seguro;
- Controle de acesso, QoS, VPN, etc. (graças ao Mikrotik)

Maila Networks

ESCOLHENDO A PLATAFORMA

Mikrotik Built-in Package	Citrix Xen	Xen Cloud
Custo incluso na licença	U\$5k	Free
Sem PCIBACK	Sem PCIBACK	Com PCIBACK
Hardware limitado a 2GB de RAM	Módulo de administração Windows	Administração por linha de comando

Maila Networks

Quem utiliza?



Maila Networks

Montando o datacenter

Hardware:

Mínimo de 2 x Servidores de 64bits X86 (para a clusterização de hardware)

Storage iSCSI de 1Gbps

Switch gerenciável

Servidores:

Para virtualização de Windows® é necessário que o processador seja Intel VT™ ou AMD-V™

O máximo de memória possível.

Opcionais:

Placas de comunicação PCI (Digium, cartões adaptadores, placas seriais)
(Necessita PCIBACK)

Sistemas:

Xen Cloud Platform – Plataforma preferida devido ao suporte

Mikrotik RouterOS 4.X – Sistema roteador multi-tarefa

Plataforma preferida para os serviços essenciais de rede.

Maila Networks

CENÁRIO:

Hardware
redundante



Storage para os Sistemas Operacionais

Instalação rápida:

1. Instale o Xen Cloud Platform em ambos os servidores, todos os equipamentos devem possuir IPs fixos.
2. Prepare o iSCSI, habilitando 'multiples initiators'
3. Escolha um dos servidores para ser o 'Pool master'
4. Adicione o(s) servidor(es) extras ao Pool Master
5. Configure o iSCSI IQN (iSCSI Qualified Name) para cada um dos servidores
6. Crie um SR (Storage Repository) e adicione a ambos os hosts, Pool Master e Pool Slave.

Maila Networks

EXEMPLO DE CONFIG POR LINHA DE COMANDO

Adicione os hosts ao pool:

```
xe pool-join master-address=<host1> master-username=<root> \ master-  
password=<password>
```

Configure o nome do iSCSI:

```
xe-set-iscsi-ign <iscsi_ign>
```

Para criar um SR

```
xe sr-create name-label=<nome_do_SR>  
\ content-type=user device-config-target=<Endereço IP ou hostname do iSCSI>  
\ device-config-targetIQN=<iscsi_target_ign, especificado acima>  
\ device-config-localIQN=<iscsi_local_ign, nome local do ign>  
\ type=lvmoiscsi shared=true device-config-LUNid=<lun_id>
```

O LUN ID pode ser separado por vírgula, uma vez que é compartilhado.

Para descobrir o UUID do Storage, execute o seguinte comando:

```
xe pool-list
```

Configure o SR como o default pool:

```
xe pool-param-set name-label=<"Novo_Pool"> uuid=<pool_uuid>  
xe pool-param-set uuid=<pool_uuid> default-SR=<iscsi_shared_sr_uuid>
```

Uma vez que o Storage foi configurado, todos os hosts virtuais serão automaticamente adicionados usando ele como default.

LIMITAÇÕES

Storages	Tamanho máximo
EXT3	2TB
LVM	2TB
Netapp	2TB
EqualLogic (\$\$\$)	15TB

Maila Networks

...MAIS ALGUNS LIMITES:

Limite do número de máquinas virtuais	32
Limite de clusters	16
1 ponto de falha	

Maila Networks

SEGURANÇA E CONTROLE NA NUVEM:

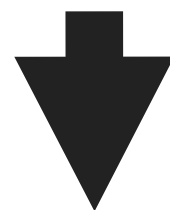
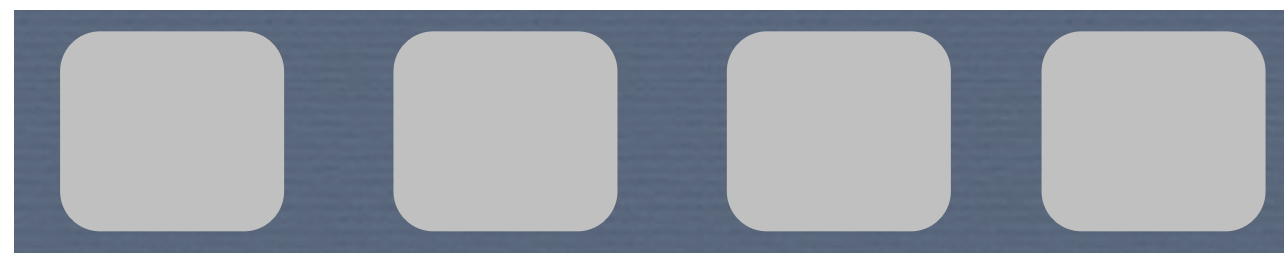
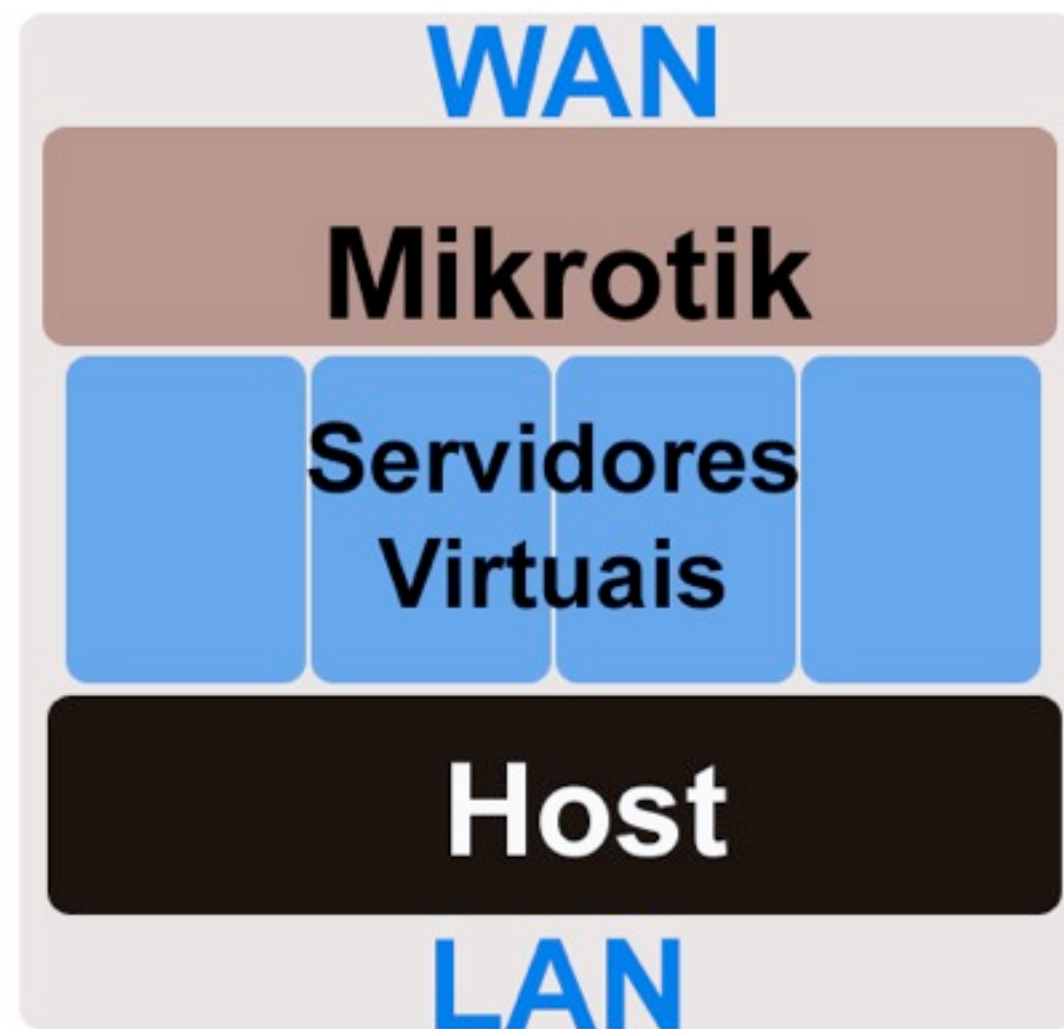


Apesar de todas as funcionalidades e vantagens que o sistema pode nos trazer, a parte de segurança foi esquecida ou é mínima. Entra em jogo o Mikrotik RouterOS como a plataforma de controle de acesso e QoS.

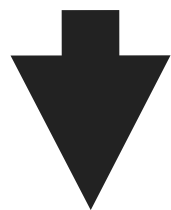
O Mikrotik se posiciona como gateway de toda a rede exercendo as seguintes funções:

1. Gerenciador de conexões: Permite gerenciar quem pode acessar quais serviços em qual máquina virtual;
2. Gerenciador de banda: Gerencia a banda de cada serviço ou host através de Simple Queues;
3. Gerencia a banda de clientes através de PCQ e Queue Tree;
4. Layer7 Firewall: Detecção de protocolos e posterior bloqueio/liberação;
5. IDS: Script de detecção de Port Scanners;
6. NAT: Mascaramento e redirecionamento de portas com controle de acesso;
7. Webproxy e DNS Cache: Aceleração do acesso a Internet;
8. Gerenciador de VLANs: Garantia de segurança e controle de acesso interno;
9. VPNs: OpenVPN, PPTP, L2PT e IPSEC para comunicação remota;
10. Servidor DHCP: Facilita a administração da rede com a configuração automática.

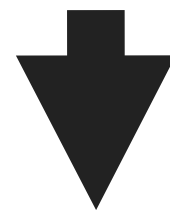
Maila Networks



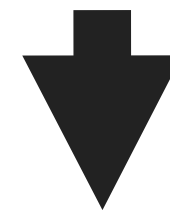
WAN



LAN



Backup



Gerenciamento

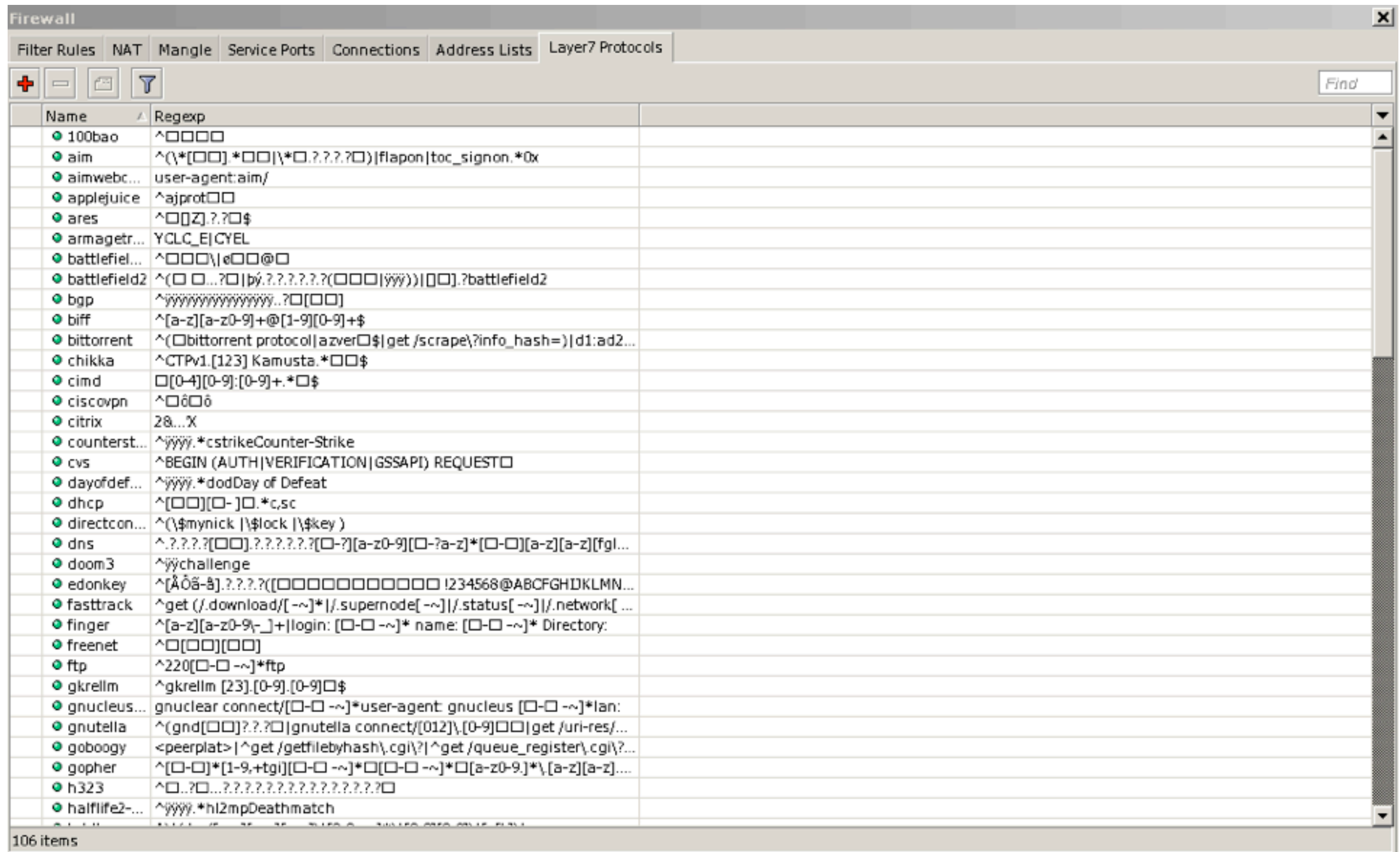
Maila Networks

Exemplo de um RouterOS rodando virtualmente na nuvem:

Firewall												
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols												
<div><div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div>Reset Counters</div><div>Reset All Counters</div></div><div>Find all</div></div>												
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Int...	Out. In...	Bytes	Packets	
0	jump	prerouting			6 (tcp)					14.4 MiB	281 010	
1	jump	prerouting			17 (...)					69.5 MiB	810 453	
2	jump	prerouting								130.9 MiB	1 123 903	
;;; QoS para o Proxy												
3	mar...	postrouting			6 (tcp)	8080				575.2 KiB	545	
4	mar...	postrouting			6 (tcp)	8080				31.9 KiB	126	
5	mar...	postrouting								0 B	0	
;;; Rede Maila												
6	mar...	forward	172.16.0.0/...							5.0 GB	11 575 721	
7	mar...	forward								11.3 GB	17 330 1...	
;;; FTP												
8	mar...	tcp-servic...			6 (tcp)	1024-655...	20-21			726 B	12	
;;; FTP-packet												
9	mar...	prerouting								0 B	0	
;;; SSH												
10	mar...	tcp-servic...			6 (tcp)	513-65535	22			3348 B	58	
;;; ssh - packet												
11	mar...	prerouting								0 B	0	
;;; TELNET												
12	mar...	tcp-servic...			6 (tcp)	1024-655...	23			601.2 KiB	10 273	
;;; telnet-packet												
13	mar...	prerouting								0 B	0	
;;; SMTP												
14	mar...	tcp-servic...			6 (tcp)	1024-655...	25			160 B	3	
;;; smtp - packet												
15	mar...	prerouting								0 B	0	
;;; DNS												
16	mar...	tcp-servic...			6 (tcp)	53	53			0 B	0	
17	mar...	tcp-servic...			6 (tcp)	1024-655...	53			1920 B	45	
;;; dns-packet												
18	mar...	prerouting								2365 B	35	
;;; HTTP												
19	mar...	tcp-servic...			6 (tcp)	1024-655...	80			4041.8 KiB	70 782	
20	mar...	tcp-servic...			6 (tcp)	1024-655...	8080			5.1 KiB	96	
;;; http-packet												
21	mar...	prerouting								0 B	0	
81 items												

Maila Networks

Detecção de protocolo utilizando Layer7



Maila Networks

Configuração de VLANs:

Interface List				
Interface	Ethernet	EoIP Tunnel	IP Tunnel	VLAN
<div><div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div><div></div></div></div></div>				
Name	Type	MTU		
test	VLAN	1500		
Interface administrativa				
R test vlan-admin	VLAN	1500		
Deia				
R test vlan-andreia	VLAN	1500		
Cameras IP				
R test vlan-cameras	VLAN	1500		
Escritorio				
R test vlan-escritorio	VLAN	1500		
Depto. Financeiro				
R test vlan-financeiro	VLAN	1500		
Home				
R test vlan-home	VLAN	1500		
Hotspot				
R test vlan-hotspot	VLAN	1500		
Informatica				
R test vlan-informat...	VLAN	1500		
Depto. Juridico				
R test vlan-juridico	VLAN	1500		
Lab2				
R test vlan-lab2	VLAN	1500		
Lab01				
R test vlan-laborato...	VLAN	1500		
Video Tivo				
R test vlan-video	VLAN	1500		
15 items out of 25				

Address List				
Address	Network	Broadcast	Interface	
hotspot network				
X test 10.5.50.1/24	10.5.50.0	10.5.50.255	hotspot	
X test 10.10.10.100/24	10.10.10.0	10.10.10.255	LAN	
Rede Maila				
test 172.16.0.200/24	172.16.0.0	172.16.0.255	LAN	
Rede Maila				
X test 172.16.0.220/24	172.16.0.0	172.16.0.255	LAN	
test 172.16.1.1/24	172.16.1.0	172.16.1.255	vlan-admin	
test 172.16.2.1/24	172.16.2.0	172.16.2.255	vlan-andreia	
test 172.16.3.1/24	172.16.3.0	172.16.3.255	vlan-cameras	
test 172.16.4.1/24	172.16.4.0	172.16.4.255	vlan-escritorio	
test 172.16.5.1/24	172.16.5.0	172.16.5.255	vlan-financeiro	
test 172.16.6.1/24	172.16.6.0	172.16.6.255	vlan-home	
test 172.16.7.1/24	172.16.7.0	172.16.7.255	vlan-hotspot	
test 172.16.8.1/24	172.16.8.0	172.16.8.255	vlan-informati...	
test 172.16.9.1/24	172.16.9.0	172.16.9.255	vlan-juridico	
test 172.16.10.1/24	172.16.10.0	172.16.10.255	vlan-lab2	
test 172.16.11.1/24	172.16.11.0	172.16.11.255	vlan-laboratorio	
test 172.16.12.1/24	172.16.12.0	172.16.12.255	vlan-video	
test 172.16.13.1/24	172.16.13.0	172.16.13.255	vlan-visitantes	
test 172.16.14.1/24	172.16.14.0	172.16.14.255	vlan-voip	
VPN				
X test 172.16.100.22...	172.16.100.0	172.16.100.255	LAN	
X test 103.168.1.1/24	103.168.1.0	103.168.1.255	LAN	
22 items (1 selected)				

Maila Networks

Connection's Tracking

Firewall									
<div>Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols</div>									
<div> <div> <div></div> <div></div> <div>Tracking</div> </div> <div>Find</div> </div>									
	Src. Address	Dst. Address	Proto...	Connecti...	Connecti...	P2P	Timeout	TCP State	
	172.16.253.1:47222	192.54.112.30:53	17 (...)				00:00:00		
U	172.16.253.1:47352	80.190.151.40:80	6 (tcp)			bit-t...	04:55:12	establis...	
A	172.16.253.1:47505	74.125.67.133:80	6 (tcp)		outro_tr...		00:03:43	establis...	
A	172.16.253.1:47783	65.54.49.123:80	6 (tcp)		outro_tr...		00:00:02	time wait	
A	172.16.253.1:48376	188.126.64.3:80	6 (tcp)		outro_tr...		11:59:29	establis...	
U	172.16.253.1:48532	188.126.64.3:80	6 (tcp)			bit-t...	01:28:01	establis...	
A	172.16.253.1:48610	65.54.50.197:80	6 (tcp)		outro_tr...		00:00:01	time wait	
A	172.16.253.1:48618	188.126.64.2:80	6 (tcp)		outro_tr...		11:59:39	establis...	
	172.16.253.1:48772	192.33.14.30:53	17 (...)				00:00:04		
A	172.16.253.1:48953	188.126.64.2:80	6 (tcp)		outro_tr...	bit-t...	00:00:46	time wait	
A	172.16.253.1:49221	200.98.211.5:80	6 (tcp)		outro_tr...		09:03:45	establis...	
U	172.16.253.1:49223	200.98.211.5:80	6 (tcp)				09:04:30	establis...	
A	172.16.253.1:49226	87.233.179.135:3310	6 (tcp)		outro_tr...		00:35:37	establis...	
A	172.16.253.1:49243	189.71.96.236:5051	6 (tcp)		outro_tr...		08:39:32	establis...	
A	172.16.253.1:49279	187.26.42.241:4161	6 (tcp)		outro_tr...		11:46:20	establis...	
A	172.16.253.1:49453	64.233.163.87:80	6 (tcp)		outro_tr...		11:57:12	establis...	
A	172.16.253.1:49507	188.126.64.4:6969	6 (tcp)		outro_tr...		00:37:37	establis...	
A	172.16.253.1:49567	200.215.181.197:80	6 (tcp)		outro_tr...		11:34:06	establis...	
A	172.16.253.1:49622	65.54.85.197:80	6 (tcp)		outro_tr...		00:03:52	establis...	
A	172.16.253.1:49744	65.54.50.46:80	6 (tcp)		outro_tr...		11:59:48	establis...	
A	172.16.253.1:49747	200.160.145.2:80	6 (tcp)		outro_tr...		00:00:00	time wait	
A	172.16.253.1:49766	65.54.49.180:80	6 (tcp)		outro_tr...		00:00:03	time wait	
A	172.16.253.1:49802	65.54.50.93:80	6 (tcp)		outro_tr...		11:59:44	establis...	
U	172.16.253.1:49887	94.108.194.161:49500	6 (tcp)				09:55:38	establis...	
A	172.16.253.1:49900	87.233.179.135:3310	6 (tcp)		outro_tr...		00:40:28	establis...	
U	172.16.253.1:49987	212.117.176.218:1337	6 (tcp)			bit-t...	05:19:13	establis...	
A	172.16.253.1:50061	64.208.152.3:5222	6 (tcp)		outro_tr...		11:20:34	establis...	
	172.16.253.1:50121	192.33.14.30:53	17 (...)				00:00:00		
A	172.16.253.1:50177	200.98.210.3:80	6 (tcp)		outro_tr...		00:00:04	time wait	
A	172.16.253.1:50201	201.10.1.2:53	17 (...)				00:00:09		
A	172.16.253.1:50324	189.118.163.247:5051	6 (tcp)		outro_tr...		05:41:56	establis...	
U	172.16.253.1:50461	61.140.78.91:6969	6 (tcp)			bit-t...	09:59:33	establis...	
A	172.16.253.1:50560	217.77.155.11:80	6 (tcp)		outro_tr...		03:53:36	establis...	
A	172.16.253.1:50574	208.73.210.125:80	6 (tcp)		outro_tr...		10:17:05	establis...	
	172.16.253.1:50580	208.73.210.125:80	6 (tcp)		outro_tr...		10:17:05	establis...	
<div>1141 items out of 1133</div> <div>Max Entries: 524288</div>									

Todo o tráfego neste caso é originado do 172.16.253.1 que gerencia o acesso dos usuários.

Maila Networks

Interface List

Interface	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Errors
R	LAN	Ethernet		2.5 Mbps	421.8 kbps	309	266	0	89	0
R	WAN	Ethernet		418.1 kbps	2.5 Mbps	261	308	0	23 756	0

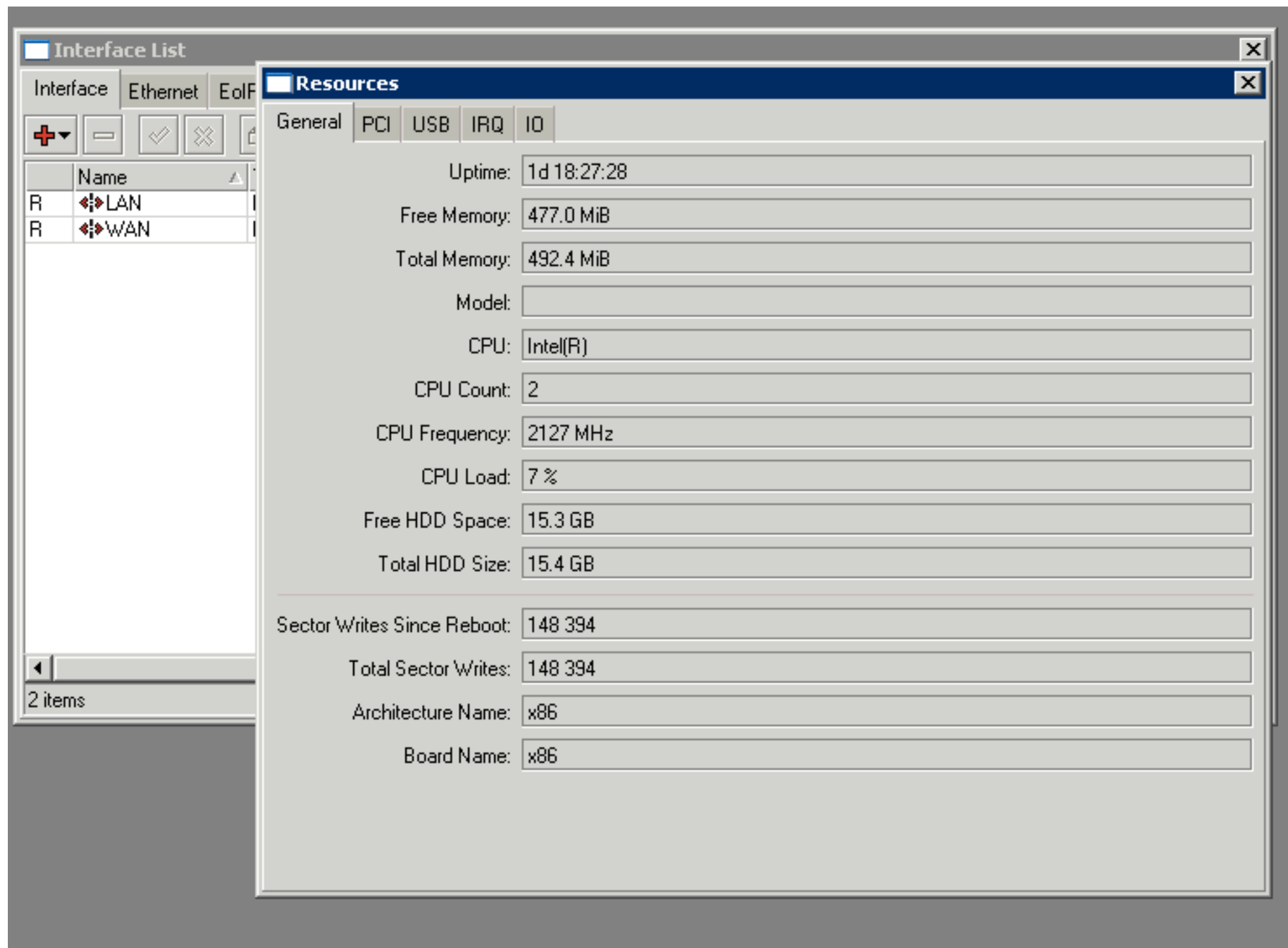
Resources

Device	Vendor	Name
00:00.0	Intel Corporation	440FX - 82441FX PMC [...]
00:01.0	Intel Corporation	82371SB PIIX3 ISA [Nat...]
00:01.1	Intel Corporation	82371SB PIIX3 IDE [Na...]
00:01.2	Intel Corporation	82371SB PIIX3 USB [N...]
00:01.3	Intel Corporation	82371AB/EB/MB PIIX4 ...
00:02.0	Cirrus Logic	GD 5446 (rev: 0)
00:03.0	XenSource, Inc.	Xen Platform Device (re...]
00:04.0	Realtek Semiconductor ...	RTL-8139/8139C/8139...
00:05.0	Realtek Semiconductor ...	RTL-8139/8139C/8139...

2 items

Detecção de hardware pelo sistema virtual

Maila Networks



System resources

Maila Networks

Xen:

<http://www.xen.org>

Xen-BR:

<http://www.xen-br.org>

Mikrotik:

<http://www.mikrotik.com>

Maila Networks

Jean R. Franco
jfranco@maila.com.br
Maila Networks
51.4063-6335
MSN: franco@maila.com.br



Maila Networks