

# Contract **TI**®

Tecnologia da Informação

# Configurações Simples mas Importantes

Leonardo Vieira - LeoMikrotik

Consultor Mikrotik

<http://www.mikrotik.com/consultants/latinamerica/brazil>

MTCNA - MTCWE - MTCRE - MTCINE - MTCTCE

## A Contract TI

Nosso foco é Contrato de TI “Outsourcing” para empresas de diversos segmentos inclusive ISP.

### Serviços:

- \* SCM Anatel c/ Eng.
- \* Cabeamento estruturado “c/ Certificação”
- \* Fibra Óptica
- \* Suporte Mikrotik, Wireless.
- \* Servidores Linux, Windows, Cache
- \* Contrato de Suporte - TI

Visite nosso site [contractti.com.br](http://contractti.com.br)

## Objetivo desta apresentação

Levar informações básicas e importantes a profissionais que estão dando os primeiros passos em Mikrotik RouterOS.

# Tópicos

- Cloud
- NTP
- DNS
- LOG
- Atualizações
- Gráfico
- IP Services
- Backup

## IP/CLOUD - Start RouterOS v6.14+

É um serviço de Dynamic DNS name para RouterBOARD

*Serial Number*

**469d04f7a6ce.sn.mynetname.net**

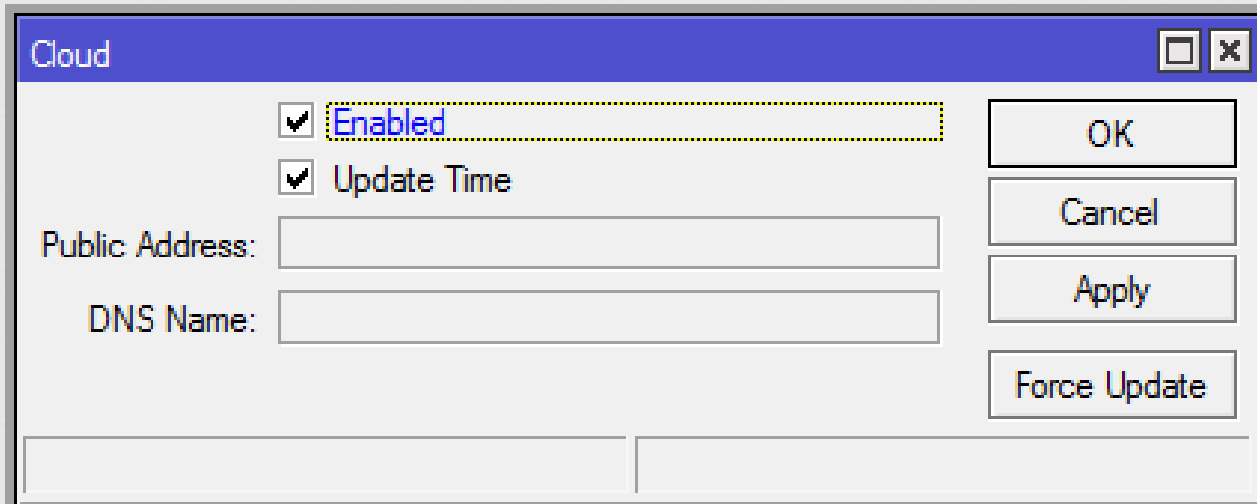
A cada 1 Min e verificado o IP externo e Atualizado c/ o nome.

Com este nome você poderá:

- \* Fechar VPN c/ base no nome.
- \* Acesso externo a RB ou redirecionamento de portas.
- \* Etc...

## IP/Cloud

Simple para configurar, basta marcar Enabled após aplicar o nome  
Aparecerá no campo DNS Name.



Cloud

Enabled

Update Time

Public Address:

DNS Name:

OK

Cancel

Apply

Force Update

# NTP - Network Time Protocol

É um protocolo para sincronização dos relógios dos Computadores roteadores, baseado em UDP.

**QUAL A IMPORTANCIA DA DATA E HORA CORRETA NA RB ?**

Regras de Firewall c/ hora programada  
Log com a data/hora correta  
Data/Hora correta do Backup  
Scripts com Scheduler programados



## NTP Server na sua Rede

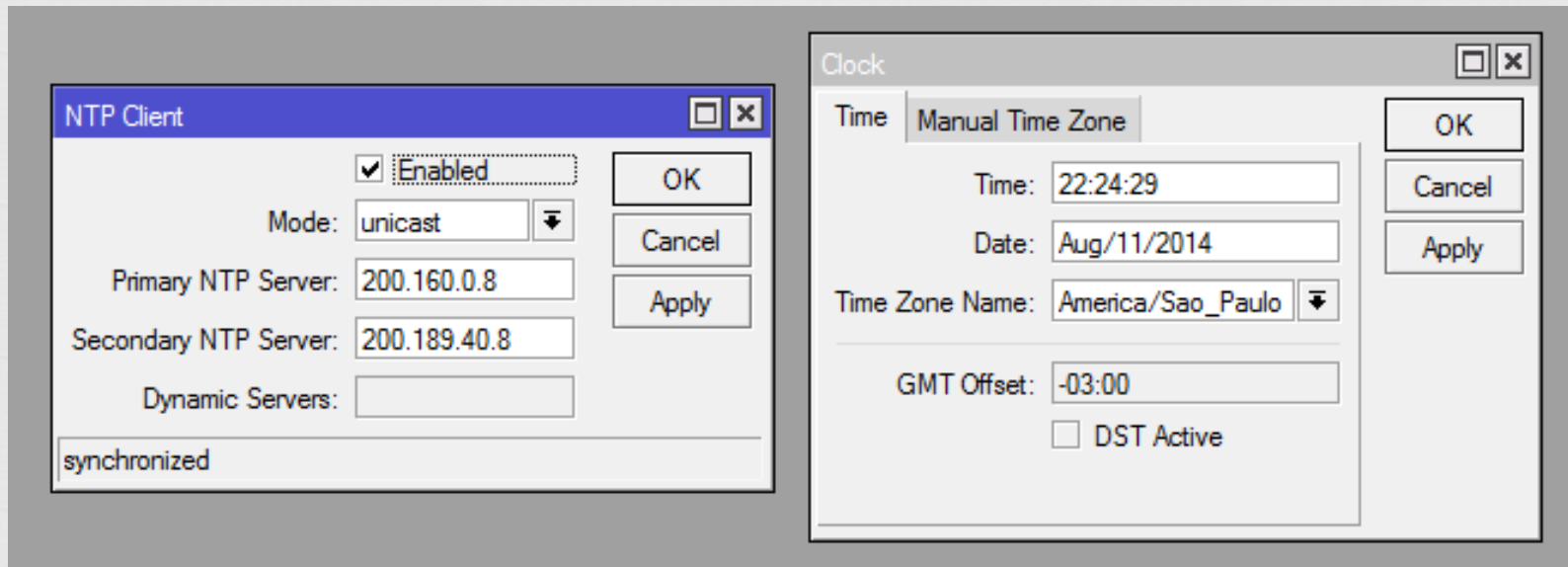


Se você não deseja que cada RB “equipamento” vá na internet atualizar Data e hora, você pode rodar o NTP Server em uma RB para que os demais equipamentos consulte dentro da sua rede.

**Firewall: Porta usada UDP 123**

<http://wiki.mikrotik.com/wiki/Manual:System/Time>

# Configuração NTP Client /System/ntp



Dica: No DHCP Server você pode repassar o IP do seu NTP Server

## DNS - Mikrotik - v4.6

O RouterOS faz um cache DNS, para agilizar a resposta para as consultas seguintes.

Cache Máximo do DNS 10240 KiB do Mikrotik ou seja 10 MB.

Devemos considerar a opção de interceptar as consultas DNS da rede e redirecionar para um servidor próprio.

*DNS Estático pode ser útil para você por exemplo dar nome a cada POP e ter facilidade no acesso ou testes.*

# LOG

## System/Logging

RouterOS é capaz de registrar vários eventos e podem ser gravados na memória, Disco, Remoto “Syslog”.

Eventos:

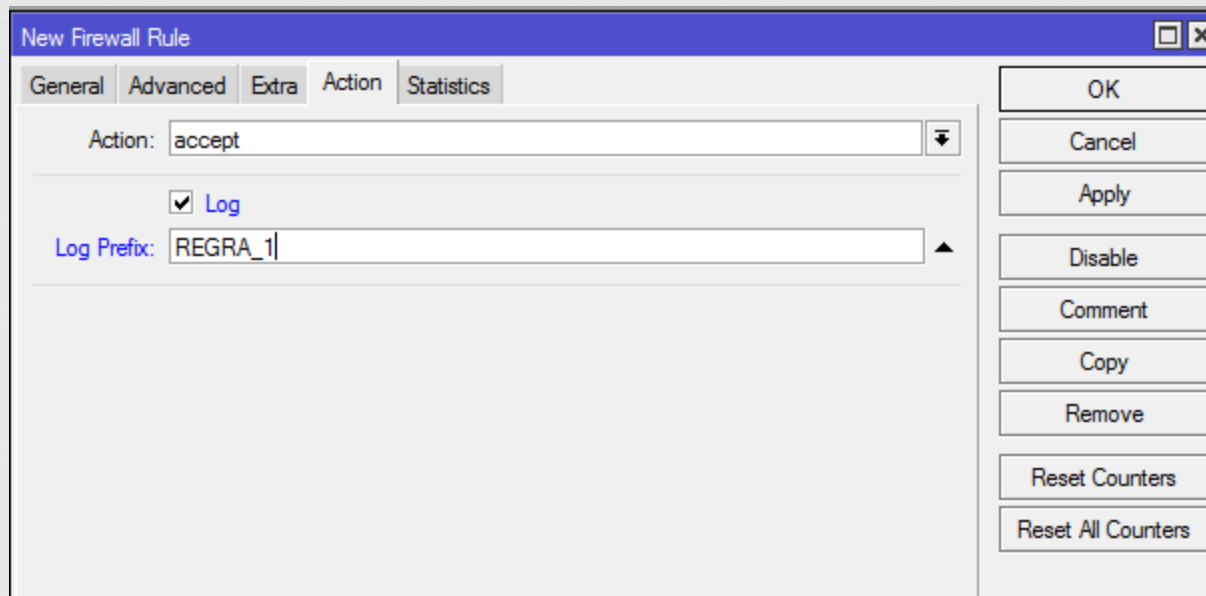
- \* Firewall
- \* Erros
- \* WebProxy
- \* entre outros.

Você pode gerar arquivos de LOG separados por assunto facilitando a leitura posterior.

Obs: Anatel exige que o provedor ISP guarde LOG por 1 Ano

## LOG / Firewall

Nas versões mais recentes na Guia Action você tem agora a Opção de “LOG” e Log Prefix tornando mais fácil você gerar LOG de regras no firewall.



The screenshot shows the 'Logging' application window with the 'Rules' tab selected. A table lists several logging rules, with 'LogPPoe' selected. A 'Log Action <LogPPoe>' dialog box is open, showing configuration for the selected rule.

Name	Type
LogFirewall	disk
LogPPoe	disk
LogWireless	disk
disk	disk
echo	echo
memory	memory
remote	remote

**Log Action <LogPPoe>**

Name: LogPPoe

Type: disk

File Name: PPoe

Lines Per File: 1000

File Count: 3

Stop on Full

The screenshot shows the 'Logging' application window with the 'Actions' tab selected. A 'New Log Rule' dialog box is open, showing configuration for a new rule.

**New Log Rule**

Topics:  firewall

Prefix: [Empty]

Action: LogFirewall

LogPPoe

LogWireless

disk

echo

memory

remote

enabled

# Atualizações (Updates)

## \* Changelog

[http://wiki.mikrotik.com/wiki/Manual:Upgrading\\_RouterOS](http://wiki.mikrotik.com/wiki/Manual:Upgrading_RouterOS)

### RouterOS

Please choose your instruction set:

*mipsbe* CRS series, RB4xx series, RB7xx series, RB9xx series, RB2011 series, SXT, OmniTik, Groove, METAL, SEXTANT

**v6.22**

2014-Nov-12



Upgrade package

Standard upgrade package. Can also be used for Netinstall.



All packages

Package with all features including less used ones.



Wireless CAPsMANv2

Wireless test package which includes the new CAPsMAN feature (Controlled AP system manager).



Netinstall

Utility for installation from network.



Torrent

Downloadable content with Bit-Torrent client.

Changelog

View changes in current version.



MD5

View MD5 hashes to confirm file validity.

**v5.26**



**v4.17**



15 $\Sigma$



## Firmware - Não esqueça!

[LeoMikrotik@MikroTik] System routerboard print

[LeoMikrotik@MikroTik] System routerboard upgrade

Routerboard

Routerboard

Model: 951Ui-2HnD

Serial Number: 4588025107C1

Current Firmware: 3.07

Upgrade Firmware: 3.18

OK

Upgrade

Settings

PoE Settings

USB Power Reset



## /System Package Instale o que realmente vai usar!

Name	Version	Build Time	Scheduled
advanced-tools	6.18	Aug/01/2014 10:47:47	
calea	6.18	Aug/01/2014 10:47:47	
dhcp	6.18	Aug/01/2014 10:47:47	
gps	6.18	Aug/01/2014 10:47:47	
hotspot	6.18	Aug/01/2014 10:47:47	
ipv6	6.18	Aug/01/2014 10:47:47	
lcd	6.18	Aug/01/2014 10:47:47	
mpls	6.18	Aug/01/2014 10:47:47	
multicast	6.18	Aug/01/2014 10:47:47	
ntp	6.18	Aug/01/2014 10:47:47	
openflow	6.18	Aug/01/2014 10:47:47	
ppp	6.18	Aug/01/2014 10:47:47	
routing	6.18	Aug/01/2014 10:47:47	
security	6.18	Aug/01/2014 10:47:47	
system	6.18	Aug/01/2014 10:47:47	
ups	6.18	Aug/01/2014 10:47:47	
user-manager	6.18	Aug/01/2014 10:47:47	
wireless	6.18	Aug/01/2014 10:47:47	

18 items

## Gráficos do RouterOS /tools Graphing

Temos alguns gráficos no RouterOS com informações sobre:

Uso de CPU

Uso de Memória

Uso de Disco

Trafego das Interfaces

QOS

**Para ativar de forma simples**

```
/tool graphing interface add interface=all
```

```
/tool graphing queue add simple-queue=all
```

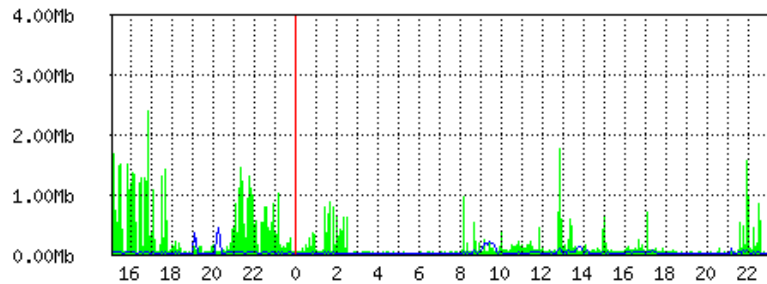
```
/tool graphing resource add allow-address=0.0.0.0/0
```

Em /IP Services você pode alterar a porta do serviço www

## Interface <ether1-LinkOK> Statistics

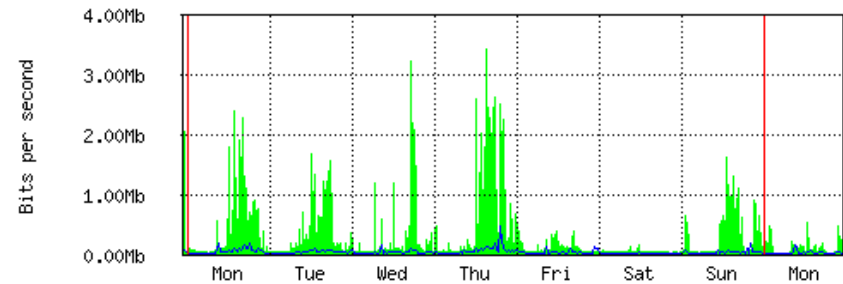
• Last update: Mon Nov 17 23:06:35 2014

"Daily" Graph (5 Minute Average)



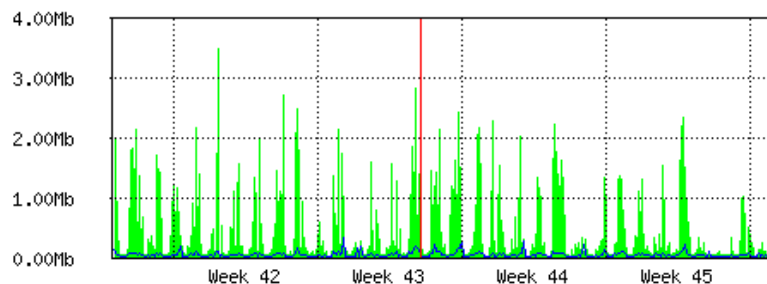
Max In: 2.39Mb; Average In: 210.06Kb; Current In: 12.82Kb;  
Max Out: 432.69Kb; Average Out: 18.86Kb; Current Out: 5.27Kb;

"Weekly" Graph (30 Minute Average)



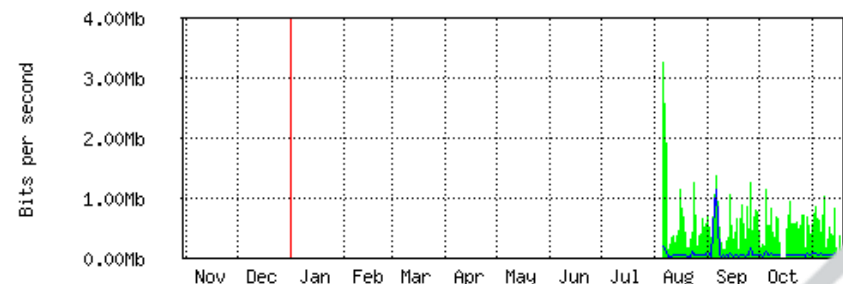
Max In: 3.43Mb; Average In: 337.48Kb; Current In: 239.62Kb;  
Max Out: 456.72Kb; Average Out: 24.92Kb; Current Out: 5.92Kb;

"Monthly" Graph (2 Hour Average)



Max In: 3.51Mb; Average In: 507.36Kb; Current In: 132.36Kb;  
Max Out: 317.28Kb; Average Out: 32.11Kb; Current Out: 13.47Kb;

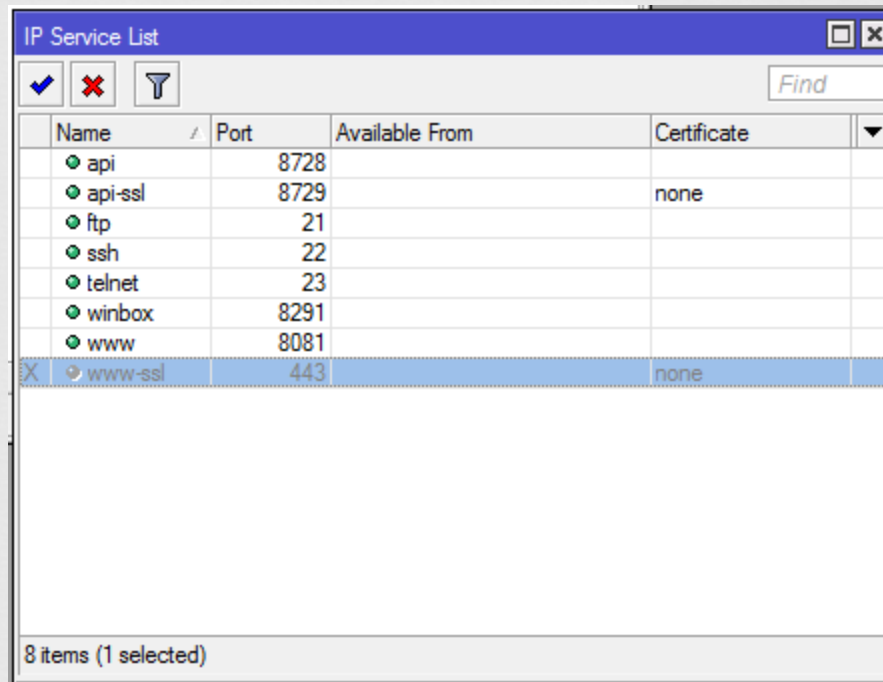
"Yearly" Graph (1 Day Average)



Max In: 3.28Mb; Average In: 558.49Kb; Current In: 118.25Kb;  
Max Out: 1.13Mb; Average Out: 52.00Kb; Current Out: 14.98Kb;

## IP / Services

Por padrão alguns serviços vem ativos no sistema; é importante desativar ou controlar como e quando estes vão ser utilizados.

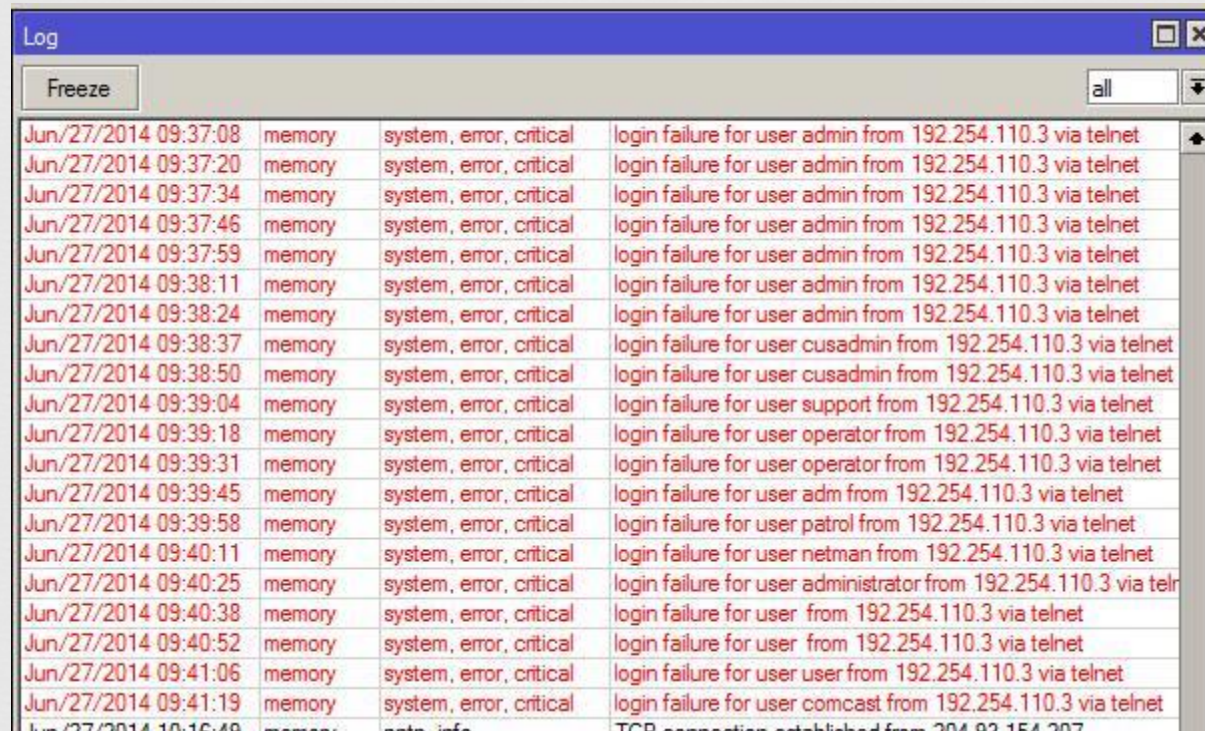


The screenshot shows a window titled "IP Service List" with a table of services. The table has columns for Name, Port, Available From, and Certificate. The 'www-ssl' service is selected, indicated by a blue highlight and a small 'X' icon in the first column. The status bar at the bottom indicates "8 items (1 selected)".

Name	Port	Available From	Certificate
api	8728		
api-ssl	8729		none
ftp	21		
ssh	22		
telnet	23		
winbox	8291		
www	8081		
X www-ssl	443		none

## SSH / Telnet

Vem ativo como default, recomendamos no mínimo alterar a porta ou usar a técnica de Firewall Knock Knock.



The screenshot shows a log window titled "Log" with a "Freeze" button and a dropdown menu set to "all". The log contains the following entries:

Timestamp	Source	Severity	Message
Jun/27/2014 09:37:08	memory	system, error, critical	login failure for user admin from 192.254.110.3 via telnet
Jun/27/2014 09:37:20	memory	system, error, critical	login failure for user admin from 192.254.110.3 via telnet
Jun/27/2014 09:37:34	memory	system, error, critical	login failure for user admin from 192.254.110.3 via telnet
Jun/27/2014 09:37:46	memory	system, error, critical	login failure for user admin from 192.254.110.3 via telnet
Jun/27/2014 09:37:59	memory	system, error, critical	login failure for user admin from 192.254.110.3 via telnet
Jun/27/2014 09:38:11	memory	system, error, critical	login failure for user admin from 192.254.110.3 via telnet
Jun/27/2014 09:38:24	memory	system, error, critical	login failure for user admin from 192.254.110.3 via telnet
Jun/27/2014 09:38:37	memory	system, error, critical	login failure for user cusadmin from 192.254.110.3 via telnet
Jun/27/2014 09:38:50	memory	system, error, critical	login failure for user cusadmin from 192.254.110.3 via telnet
Jun/27/2014 09:39:04	memory	system, error, critical	login failure for user support from 192.254.110.3 via telnet
Jun/27/2014 09:39:18	memory	system, error, critical	login failure for user operator from 192.254.110.3 via telnet
Jun/27/2014 09:39:31	memory	system, error, critical	login failure for user operator from 192.254.110.3 via telnet
Jun/27/2014 09:39:45	memory	system, error, critical	login failure for user adm from 192.254.110.3 via telnet
Jun/27/2014 09:39:58	memory	system, error, critical	login failure for user patrol from 192.254.110.3 via telnet
Jun/27/2014 09:40:11	memory	system, error, critical	login failure for user netman from 192.254.110.3 via telnet
Jun/27/2014 09:40:25	memory	system, error, critical	login failure for user administrator from 192.254.110.3 via telnet
Jun/27/2014 09:40:38	memory	system, error, critical	login failure for user from 192.254.110.3 via telnet
Jun/27/2014 09:40:52	memory	system, error, critical	login failure for user from 192.254.110.3 via telnet
Jun/27/2014 09:41:06	memory	system, error, critical	login failure for user user from 192.254.110.3 via telnet
Jun/27/2014 09:41:19	memory	system, error, critical	login failure for user comcast from 192.254.110.3 via telnet
Jun/27/2014 10:16:48	memory	sysinfo	TCP connection established from 204.92.154.207

## Port Knocking

É um método para abrir porta no firewall batendo em uma sequencia de portas aleatórias pré definidas por você.

```
add action=add-src-to-address-list address-list=passo1 address-list-timeout=10s chain=input
dst-port=\
    1234 in-interface=ether1-LinkOK protocol=tcp
add action=add-src-to-address-list address-list=passo2 address-list-timeout=10s chain=input
dst-port=\
    4321 in-interface=ether1-LinkOK protocol=tcp src-address-list=passo1
add action=add-src-to-address-list address-list=AcessoOK address-list-timeout=15m
chain=input \
    dst-port=2424 in-interface=ether1-LinkOK protocol=tcp src-address-list=passo2
add chain=input dst-port=8291 in-interface=ether1-LinkOK protocol=tcp src-address-
list=AcessoOK
```

Agora a ultima regra que falta criar e a DROP na porta 8291

[http://en.wikipedia.org/wiki/Port\\_knocking](http://en.wikipedia.org/wiki/Port_knocking)

## Backup

Quem não tem Backup dos seus equipamentos?

Estão armazenados fora dos equipamentos?

### **1º Forma**

/system backup save password=teste

### **2º Forma**

/export file=backup compact

Você pode agendar para ser realizado backup automático e até remover os antigos de forma automática.

## Backup por e-mail

```
:log info "backup esta iniciando"  
:global backupfile ([/system identity get name] . "-")  
/system backup save name=$backupfile  
:log info "backup pausing for 15s"  
:delay 15s  
:log info "backup enviando por email"  
/tool e-mail send to="provedor@seuemail.com.br" subject=([/system identity get  
name] . \  
" Backup Automatico") from=login@seuemail.com.br file=$backupfile  
server=8.8.8.8  
:log info "backup finalizado"
```



# Muito Obrigado

Leonardo Vieira

[leonardo@contractti.com.br](mailto:leonardo@contractti.com.br)



Whatsapp +55 31 9555-8380



LeoMikrotik



Facebook.com/Leonardo.Mikrotik

