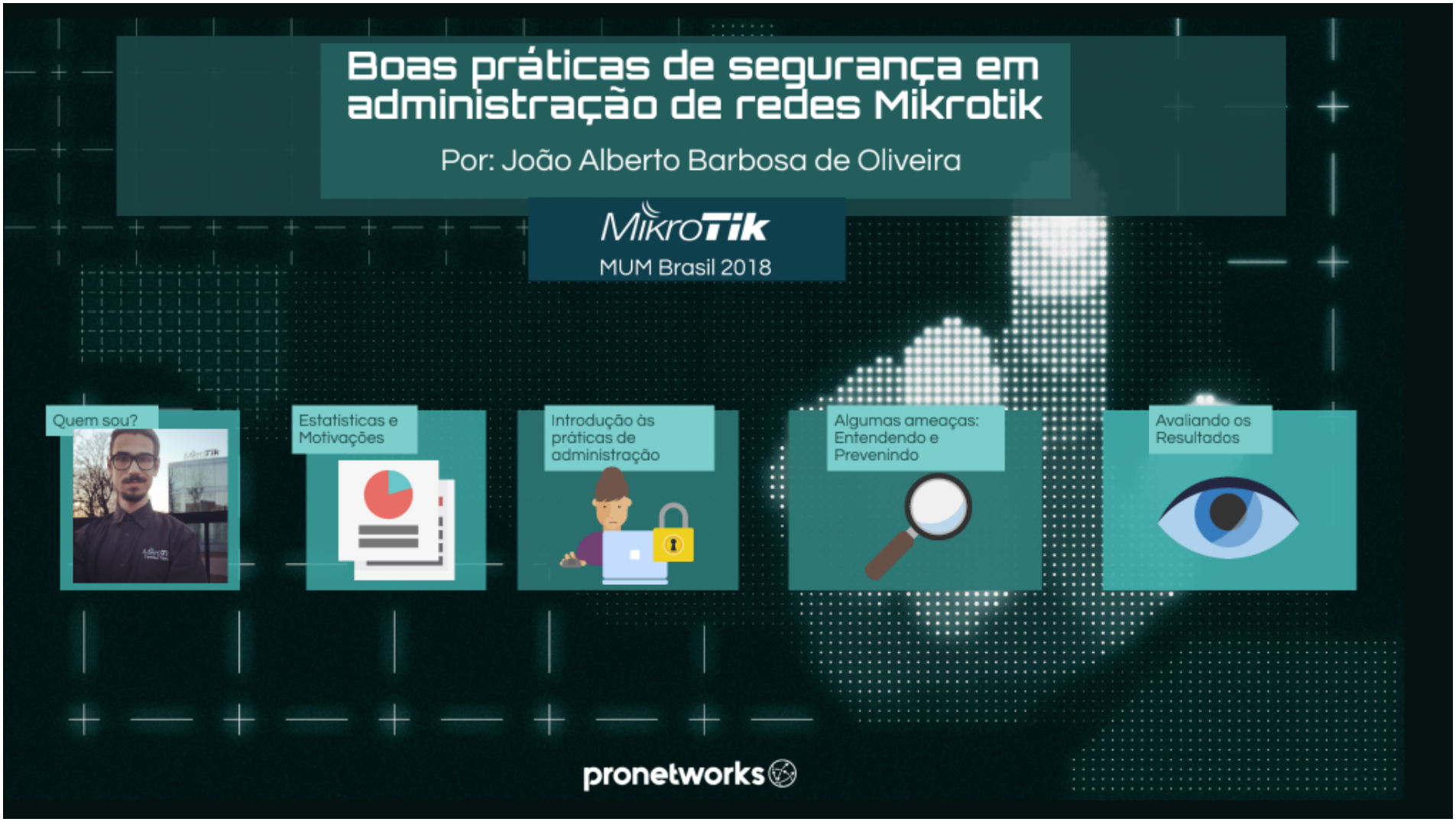

Boas práticas de segurança em administração de redes Mikrotik
Por: João Alberto Barbosa de Oliveira
MikroTik
MUM Brasil 2018
Quem sou?
Estatísticas e Motivações
Introdução às práticas de administração
Algumas ameaças: Entendendo e Prevenindo
Avaliando os Resultados
pronetworks

# #whoami

João Alberto
Barbosa de Oliveira

- Pós Graduado em gestão e segurança em redes de computadores – UEG 2016
- Gerente de Redes - Radar WISP
- Fundador e Trainer Oficial - Pro Networks
- Artigo: "Boas Práticas em roteamento de borda para sistemas autônomos provedores de acesso à internet em processo de dual stack"
- Certificações Mikrotik: MTCNA, MTCTCE, MTCIPv6E, MTCRE, MTCINE e TRAINER

Radar Internet

Pro Networks

Objetivos

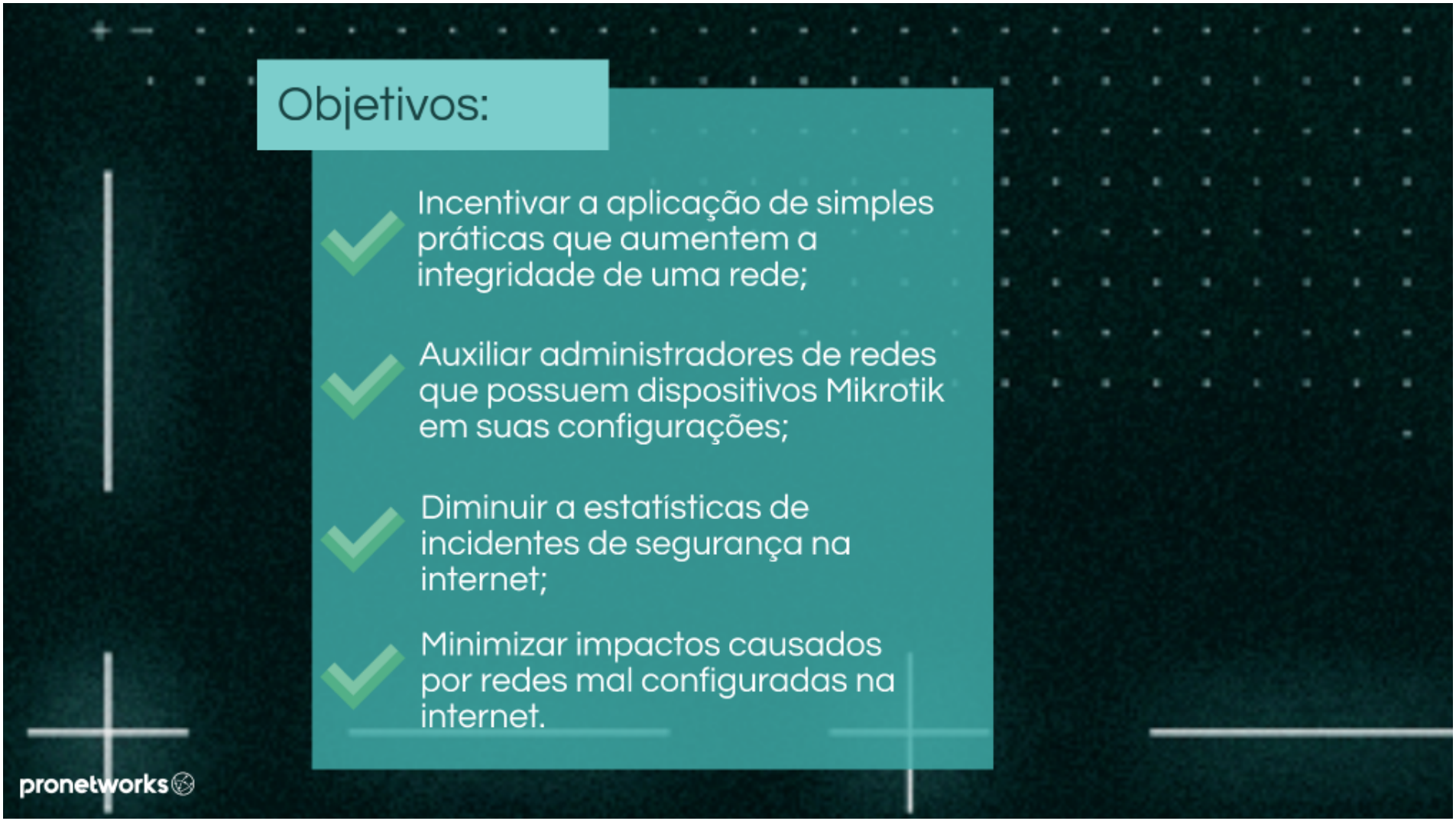
Cronograma

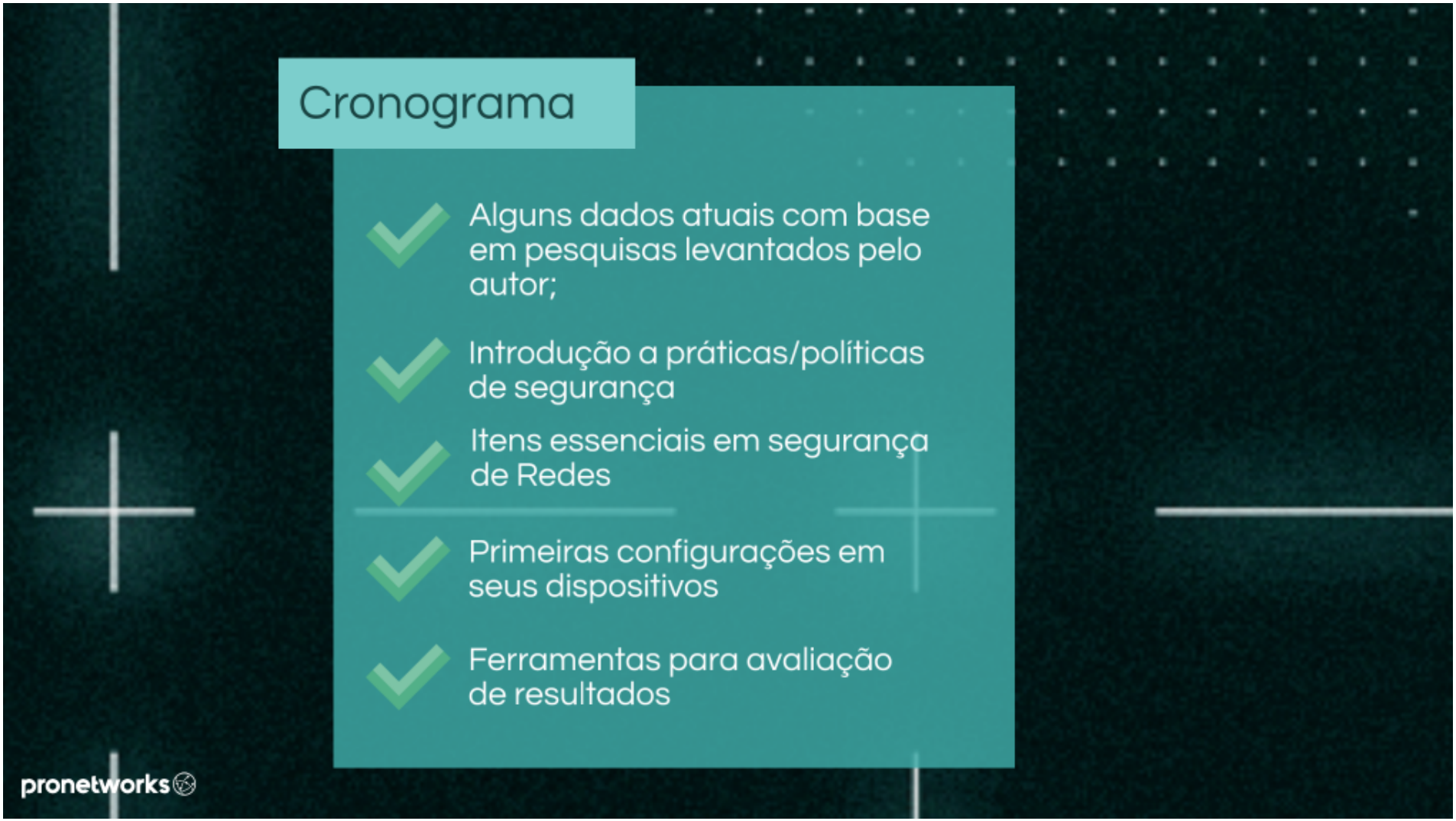
pronetworks

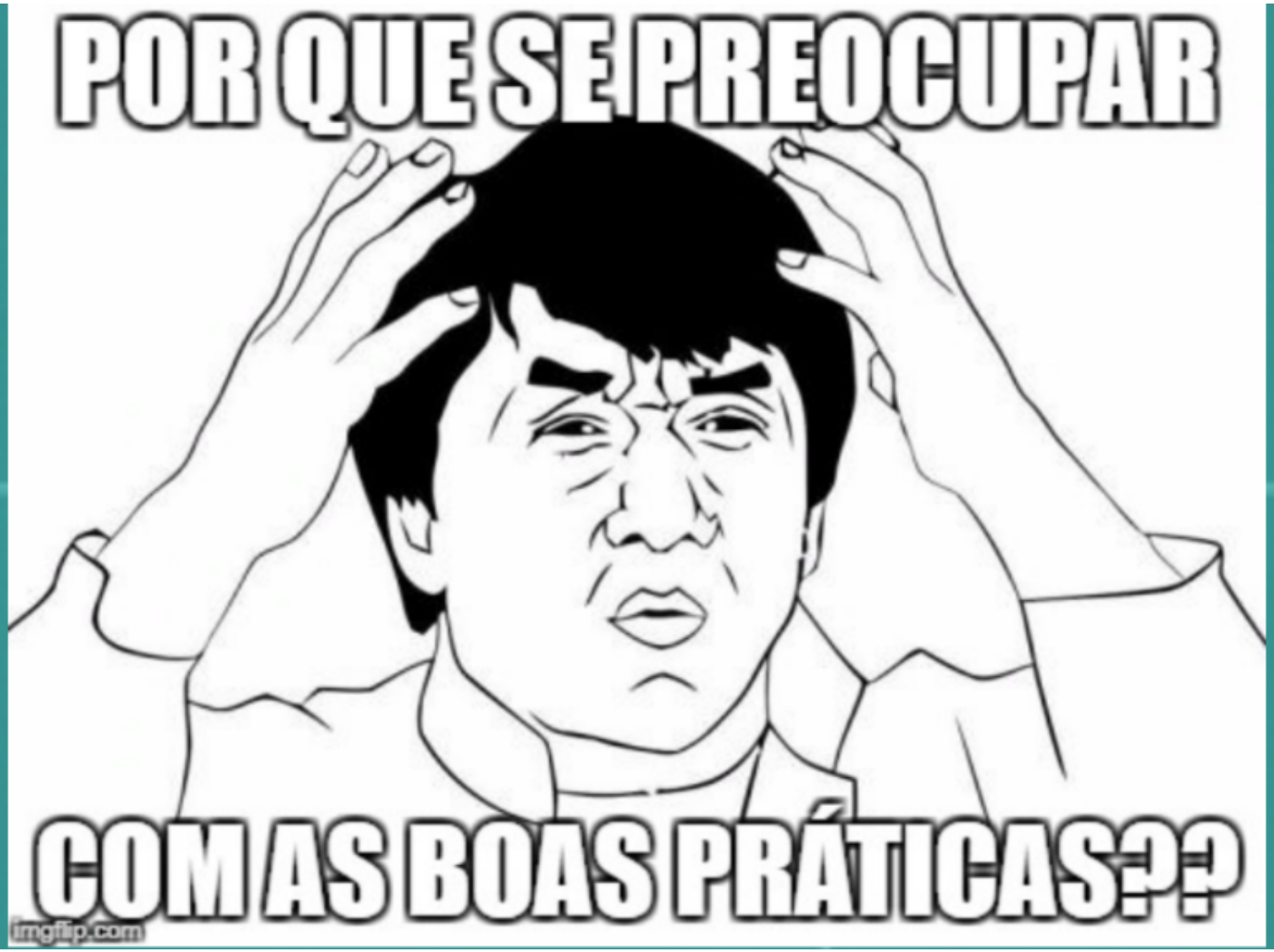
# Radar Internet

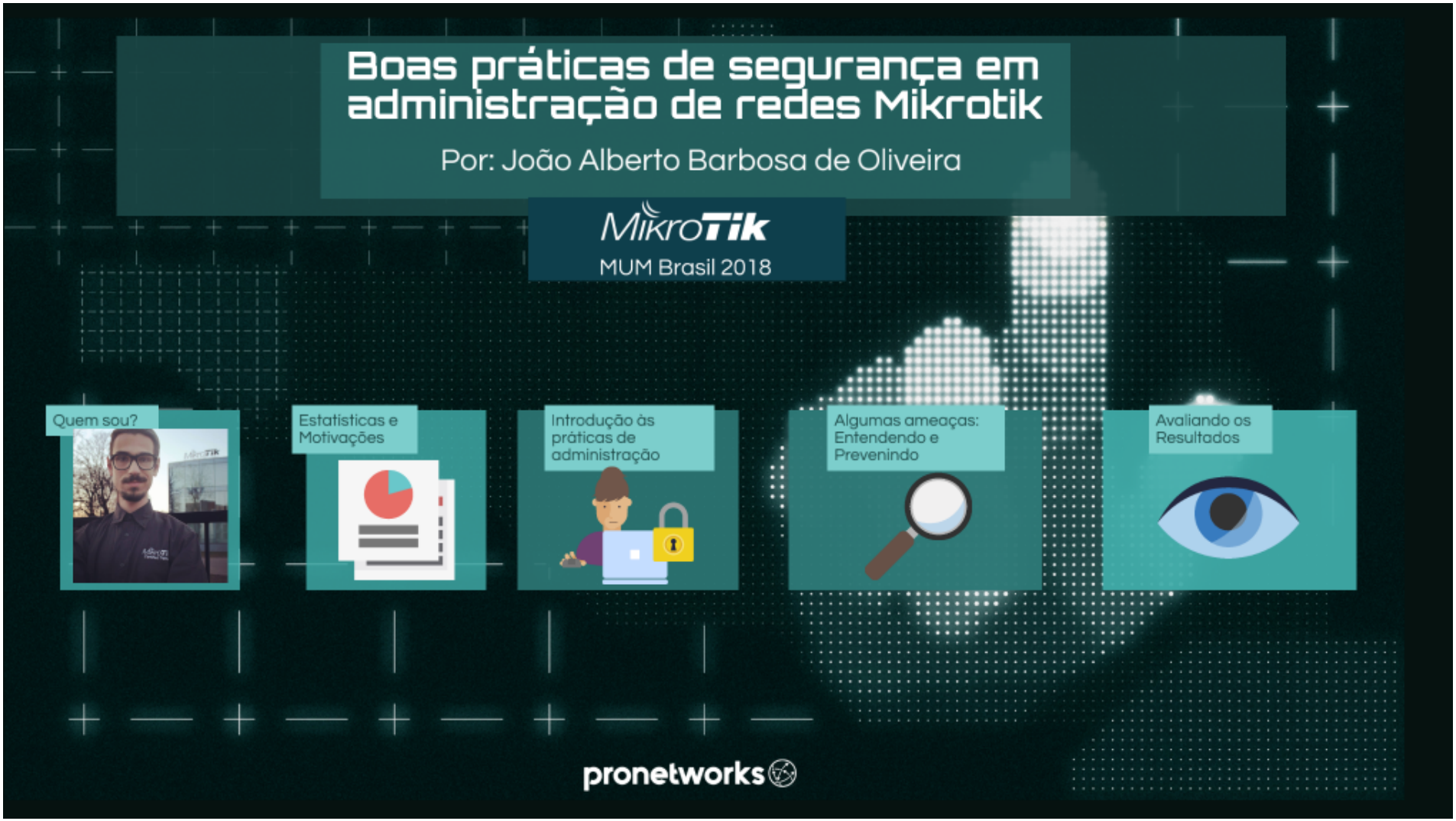
Pro Networks

pronetworks


Objetivos:
Incentivar a aplicação de simples práticas que aumentem a integridade de uma rede;
Auxiliar administradores de redes que possuem dispositivos Mikrotik em suas configurações;
Diminuir a estatísticas de incidentes de segurança na internet;
Minimizar impactos causados por redes mal configuradas na internet.
pronetworks


Cronograma
Alguns dados atuais com base em pesquisas levantados pelo autor;
Introdução a práticas/políticas de segurança
Itens essenciais em segurança de Redes
Primeiras configurações em seus dispositivos
Ferramentas para avaliação de resultados
pronetworks


POR QUE SE PREOCUPAR
COM AS BOAS PRÁTICAS??
imgflip.com


Boas práticas de segurança em administração de redes Mikrotik
Por: João Alberto Barbosa de Oliveira
MikroTik
MUM Brasil 2018
Quem sou?
Estatísticas e Motivações
Introdução às práticas de administração
Algumas ameaças: Entendendo e Prevenindo
Avaliando os Resultados
pronetworks

# Estatísticas/Motivações

- Mostrar alguns dados estimados, com base no Shodan;
- Dados levantam dispositivos com endereçamento público;
- Alguns resultados provam a necessidade de atenção principalmente para o Brasil;
- Minimizar problemas de dispositivos Mikrotik mal configurados na internet



pronetworks

# Roteadores Mikrotik Mundo (4,325,406)

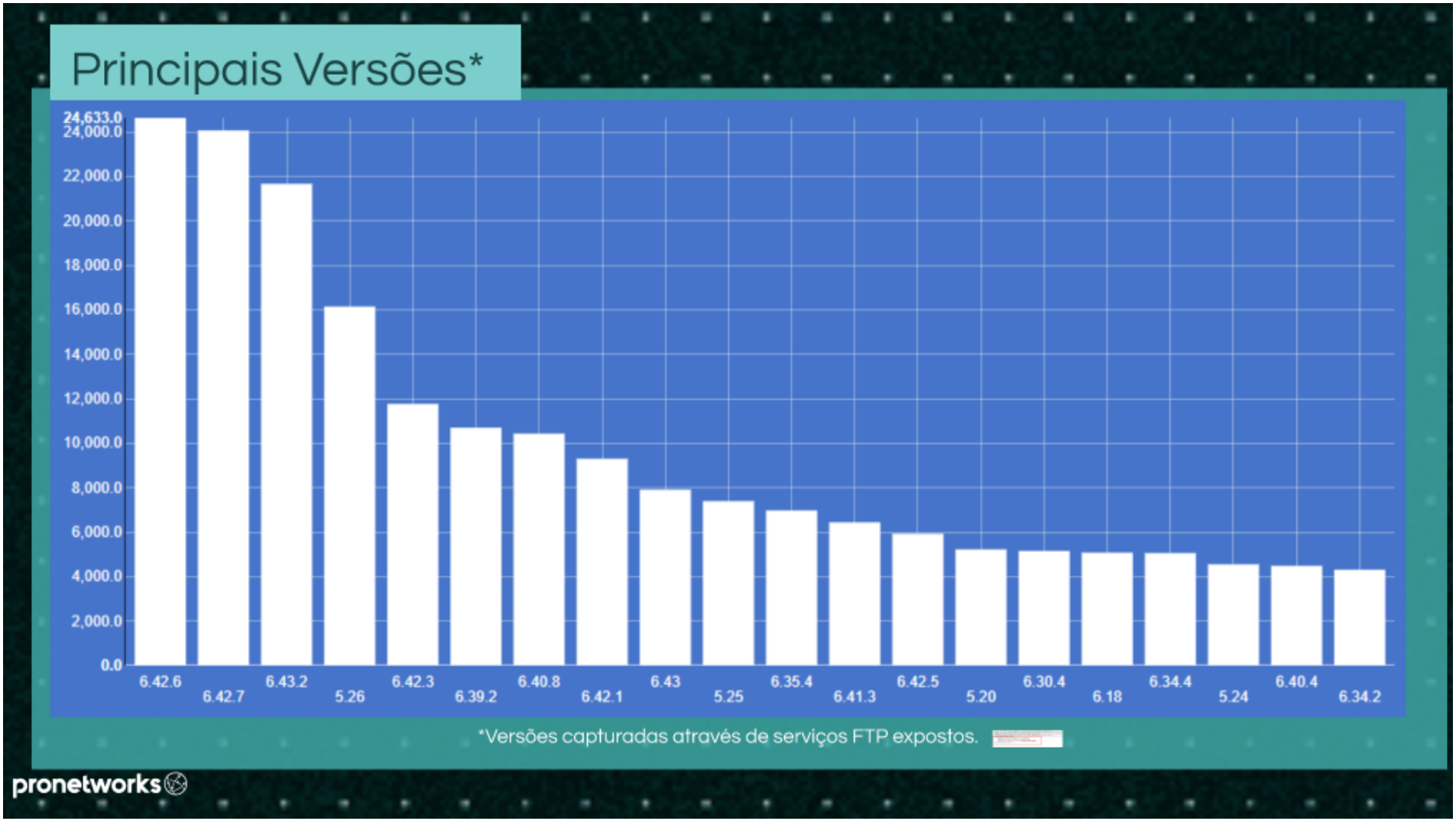
| | |
|---|---|
| 1. Brazil | 804,648 |
| 2. China | 351,486 |
| 3. Indonesia | 251,431 |
| 4. United States | 220,698 |
| 5. Russian Federation | 219,782 |
| 6. Italy | 214,062 |
| 7. Iran, Islamic Republic of | 208,562 |
| 8. India | 203,927 |
| 9. Poland | 152,192 |
| 10. South Africa | 125,655 |

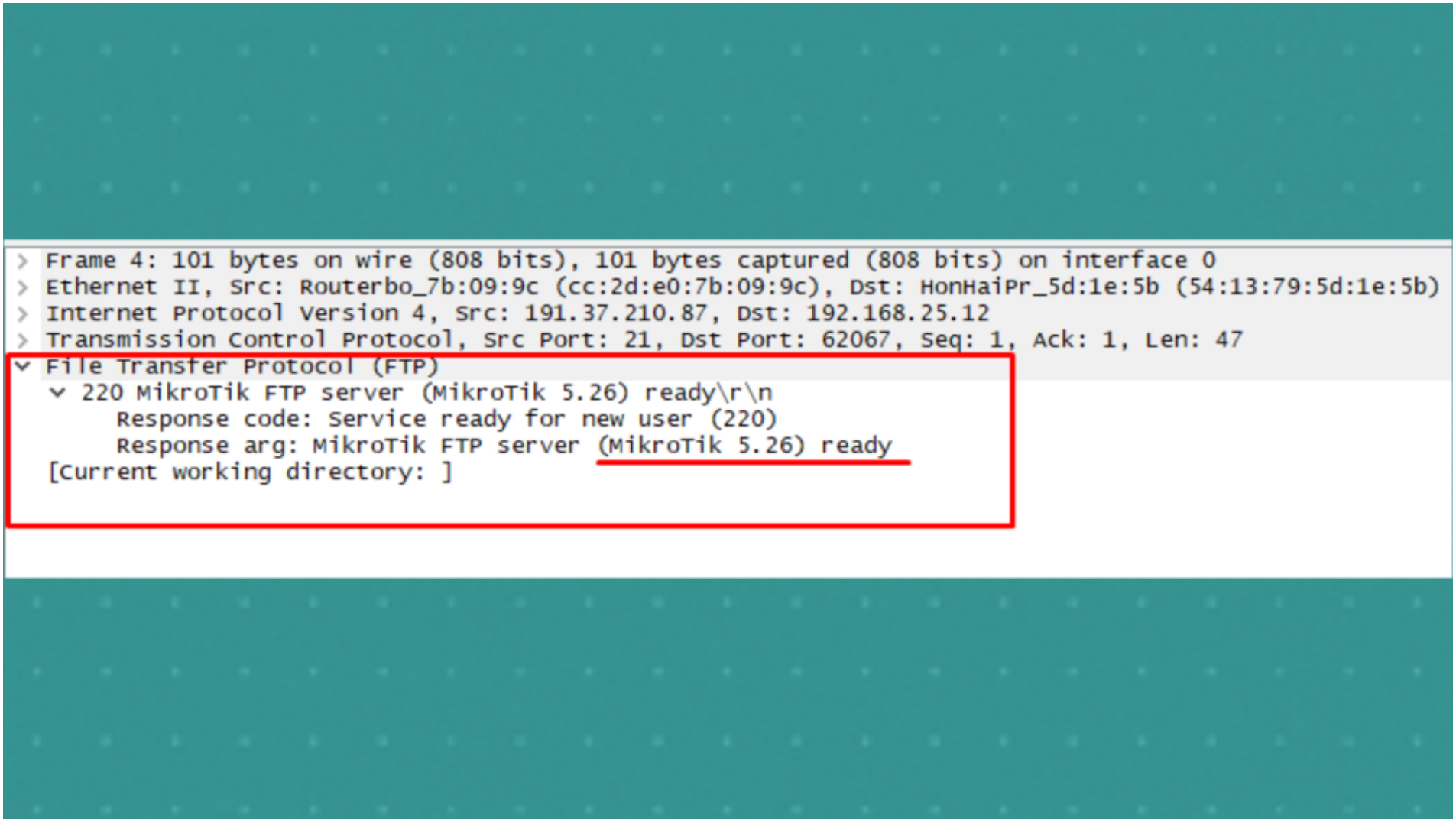
Search for product:"Mikrotik" returned 4,325,406 results on 24-10-2018

Principais Versões

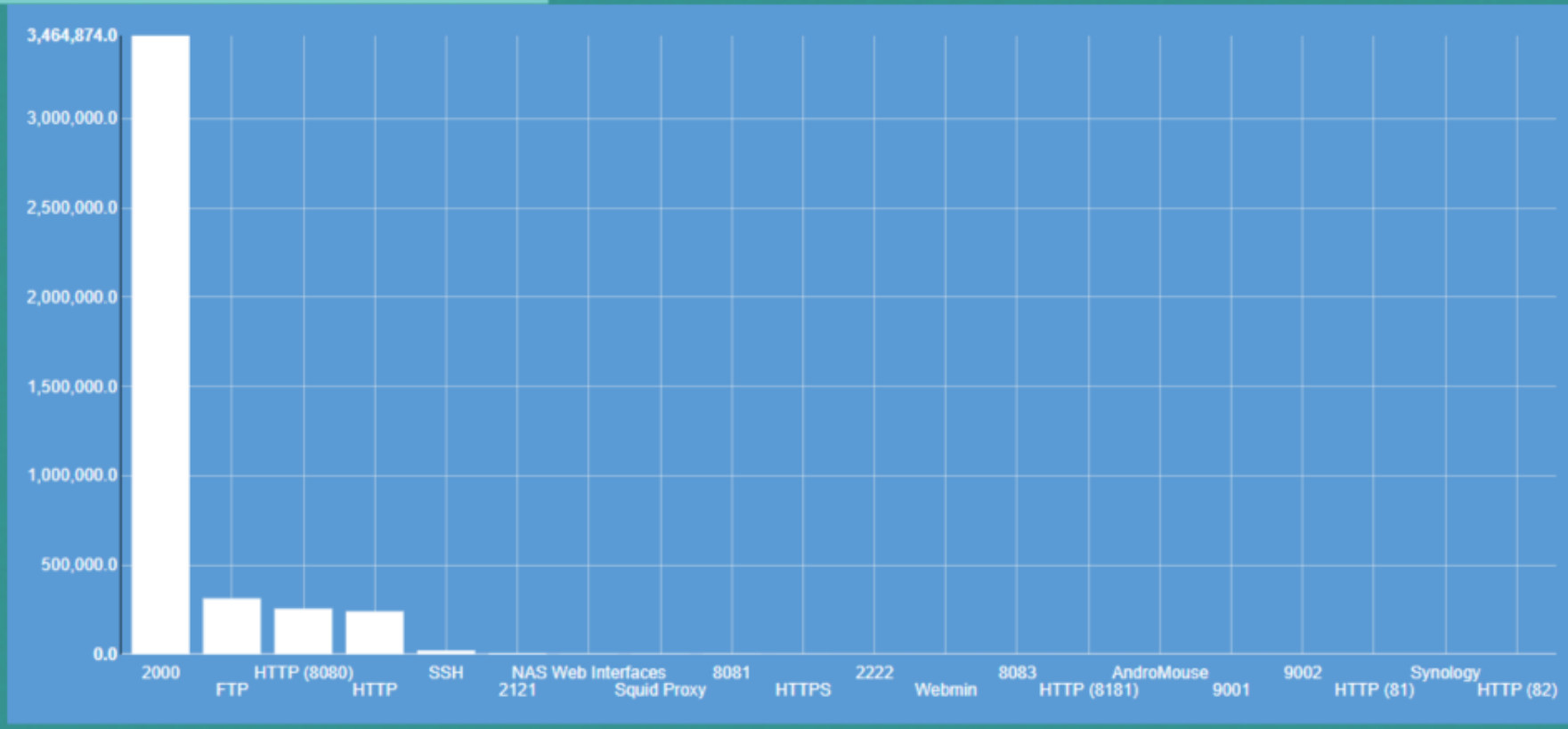
Principais Serviços

pronetworks


Principais Versões*
24,633.0
24,000.0
22,000.0
20,000.0
18,000.0
16,000.0
14,000.0
12,000.0
10,000.0
8,000.0
6,000.0
4,000.0
2,000.0
0.0
6.42.6
6.42.7
6.43.2
5.26
6.42.3
6.39.2
6.40.8
6.42.1
6.43
5.25
6.35.4
6.41.3
6.42.5
5.20
6.30.4
6.18
6.34.4
5.24
6.40.4
6.34.2
*Versões capturadas através de serviços FTP expostos.
pronetworks


Frame 4: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0
Ethernet II, Src: Routerbo_7b:09:9c (cc:2d:e0:7b:09:9c), Dst: HonHaiPr_5d:1e:5b (54:13:79:5d:1e:5b)
Internet Protocol Version 4, Src: 191.37.210.87, Dst: 192.168.25.12
Transmission Control Protocol, Src Port: 21, Dst Port: 62067, Seq: 1, Ack: 1, Len: 47
File Transfer Protocol (FTP)
220 MikroTik FTP server (MikroTik 5.26) ready\r\n
Response code: Service ready for new user (220)
Response arg: MikroTik FTP server (MikroTik 5.26) ready
[Current working directory: ]

# Principais Serviços




pronetworks

# Estatísticas - Mikortik Brasil (Amostra 804,651)

| | |
|---|---|
| 1. Sao Paulo | 24,389 |
| 2. Rio De Janeiro | 17,480 |
| 3. Recife | 14,506 |
| 4. Salvador | 12,189 |
| 5. Fortaleza | 10,453 |
| 6. Brasilia | 7,736 |
| 7. Goiania | 5,535 |
| 8. Belo Horizonte | 5,407 |
| 9. Sao Goncalo | 4,560 |
| 10. Macapa | 4,460 |

Search for product:"Mikrotik" country:"BR" returned 804,651 results on 24-10-2018

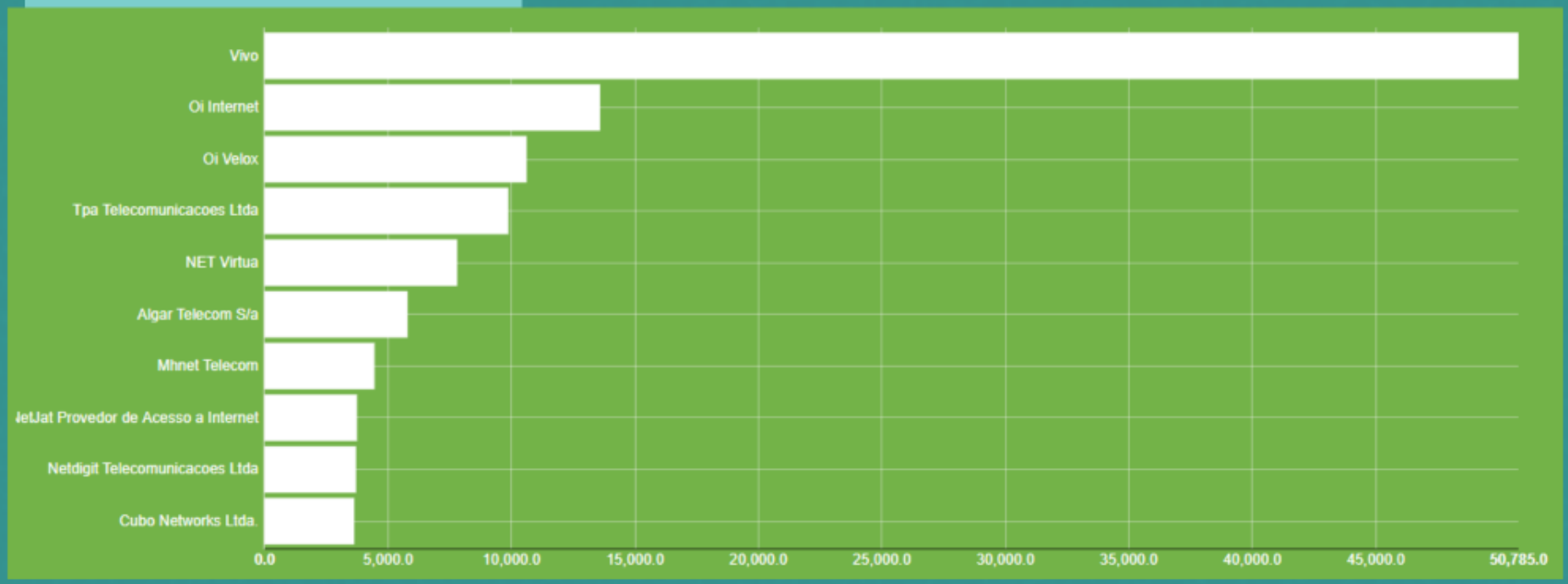
Principais Organizações

Principais Versões

Somos Campeões!!!

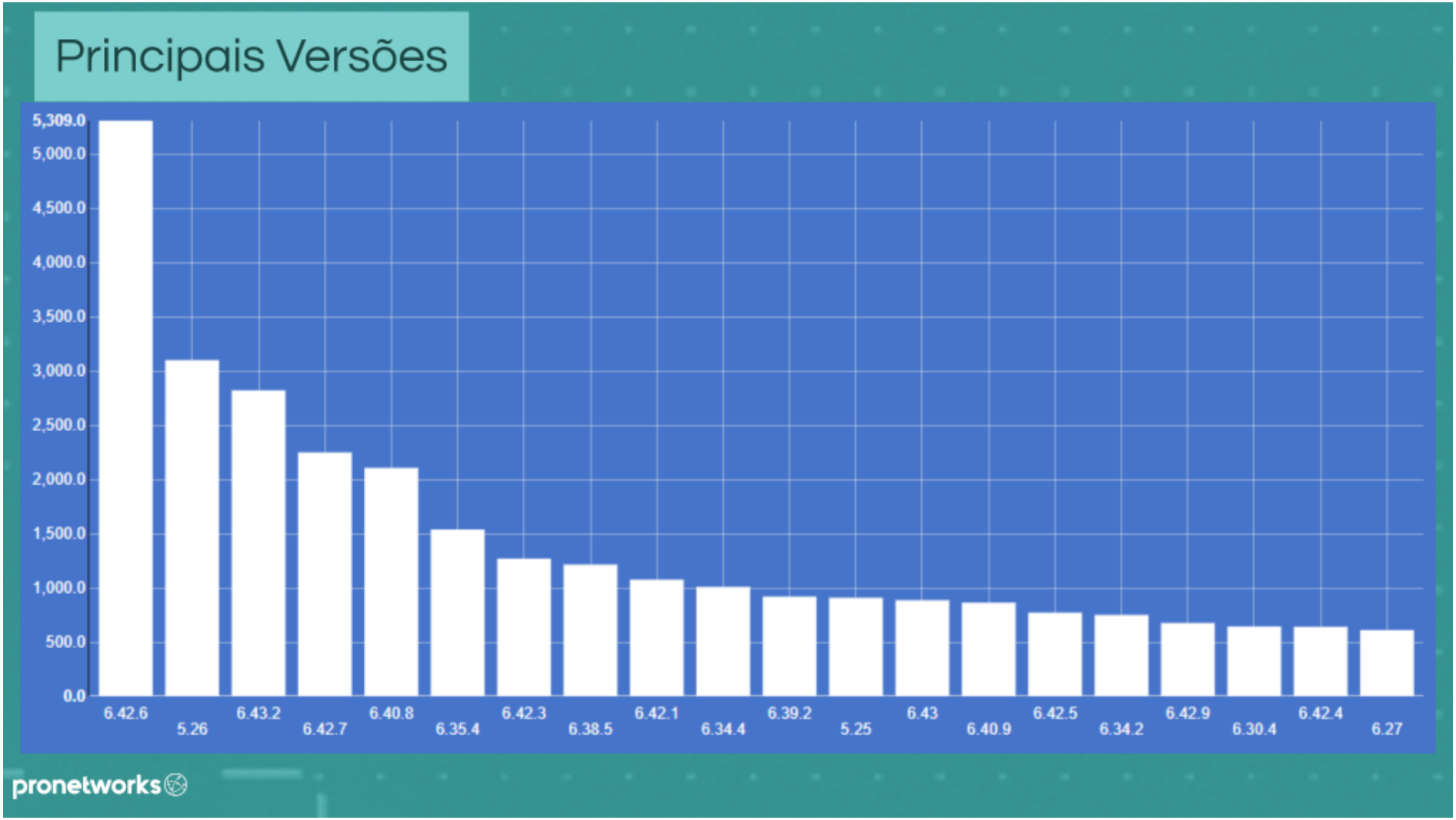

pronetworks

# Principais Organizações




pronetworks

# Principais Versões




pronetworks

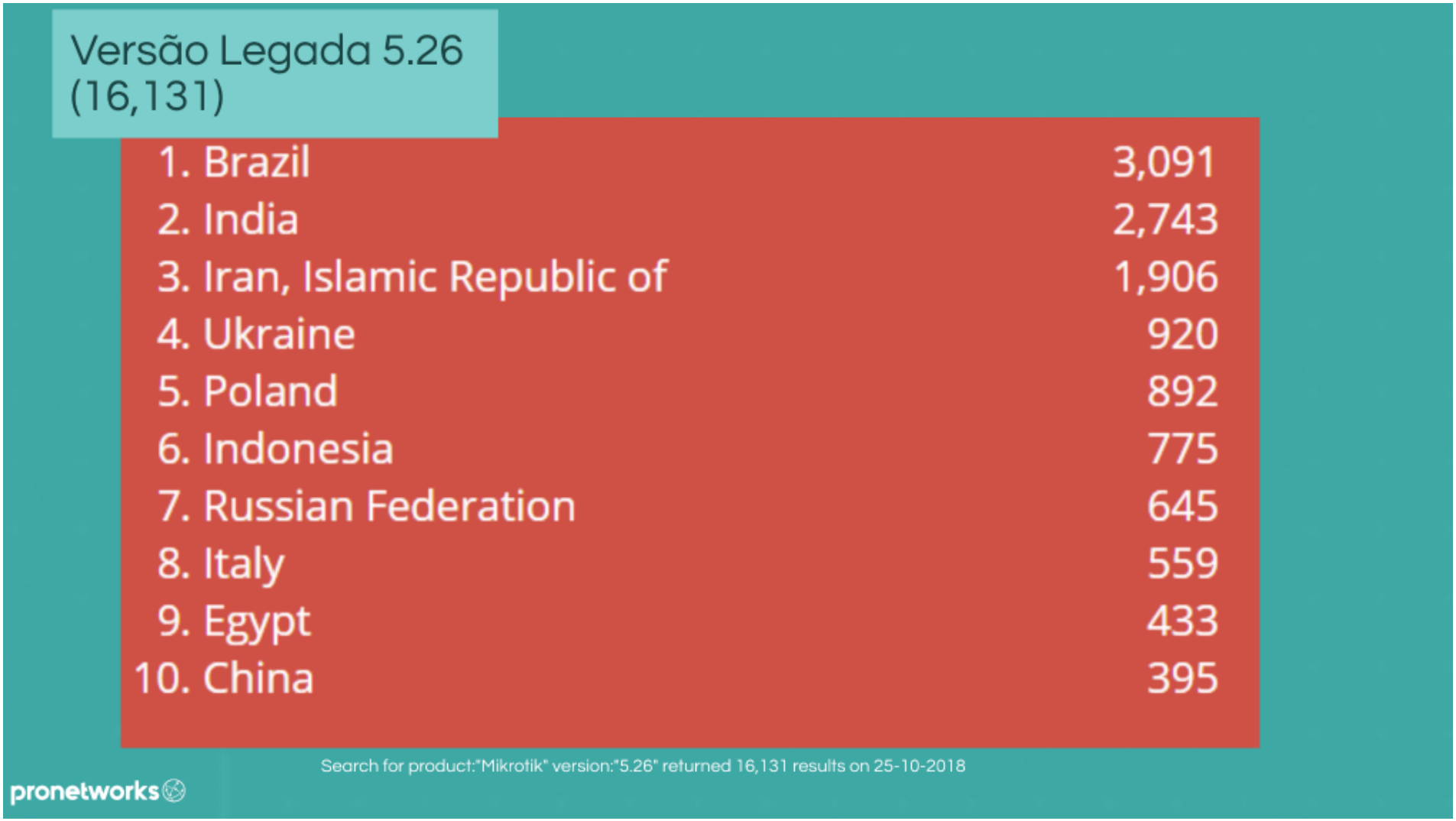

Versão Legada

Coinhive

Serviços comuns

Análise proporcional

pronetworks

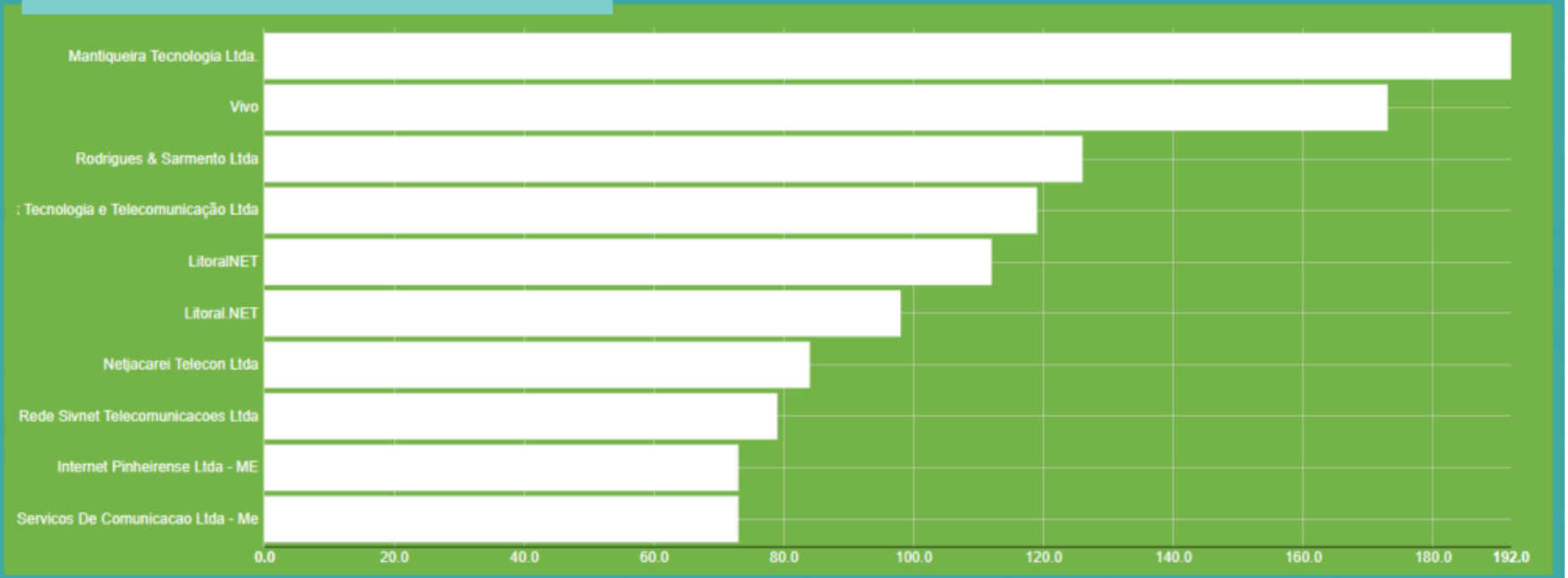

Versão Legada 5.26
(16,131)
1. Brazil 3,091
2. India 2,743
3. Iran, Islamic Republic of 1,906
4. Ukraine 920
5. Poland 892
6. Indonesia 775
7. Russian Federation 645
8. Italy 559
9. Egypt 433
10. China 395
Search for product:"Mikrotik" version:"5.26" returned 16,131 results on 25-10-2018
pronetworks

## Principais Cidades

| | |
|---|---|
| 1. Tibau | 215 |
| 2. Sao Lourenco | 158 |
| 3. Tenente Ananias | 129 |
| 4. Artur Nogueira | 128 |
| 5. Araxa | 100 |
| 6. Areia Branca | 85 |
| 7. Joao Pinheiro | 74 |
| 8. Viamao | 71 |
| 9. Grossos | 59 |
| 10. Jacarei | 57 |

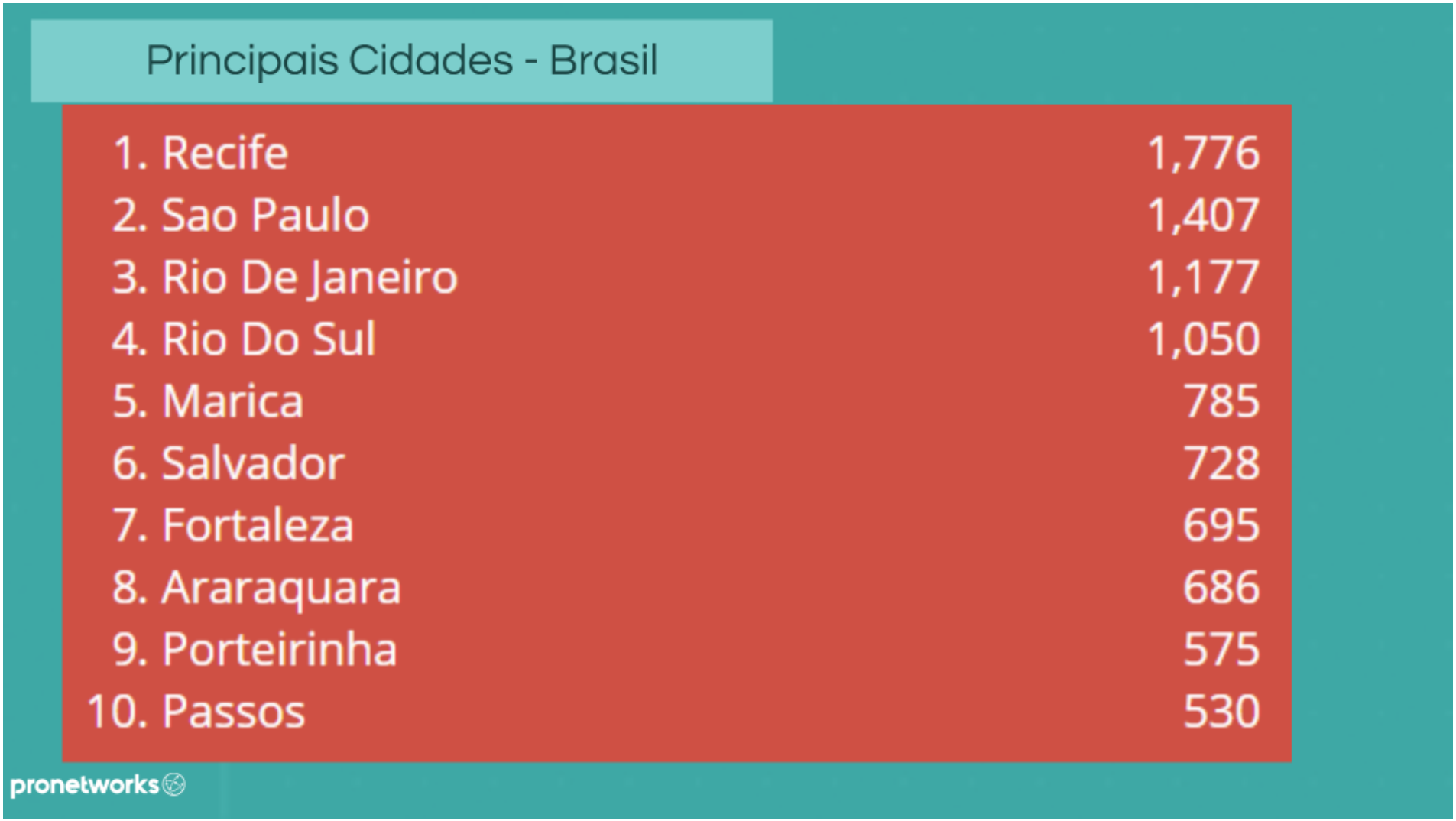
pronetworks

# Principais Organizações

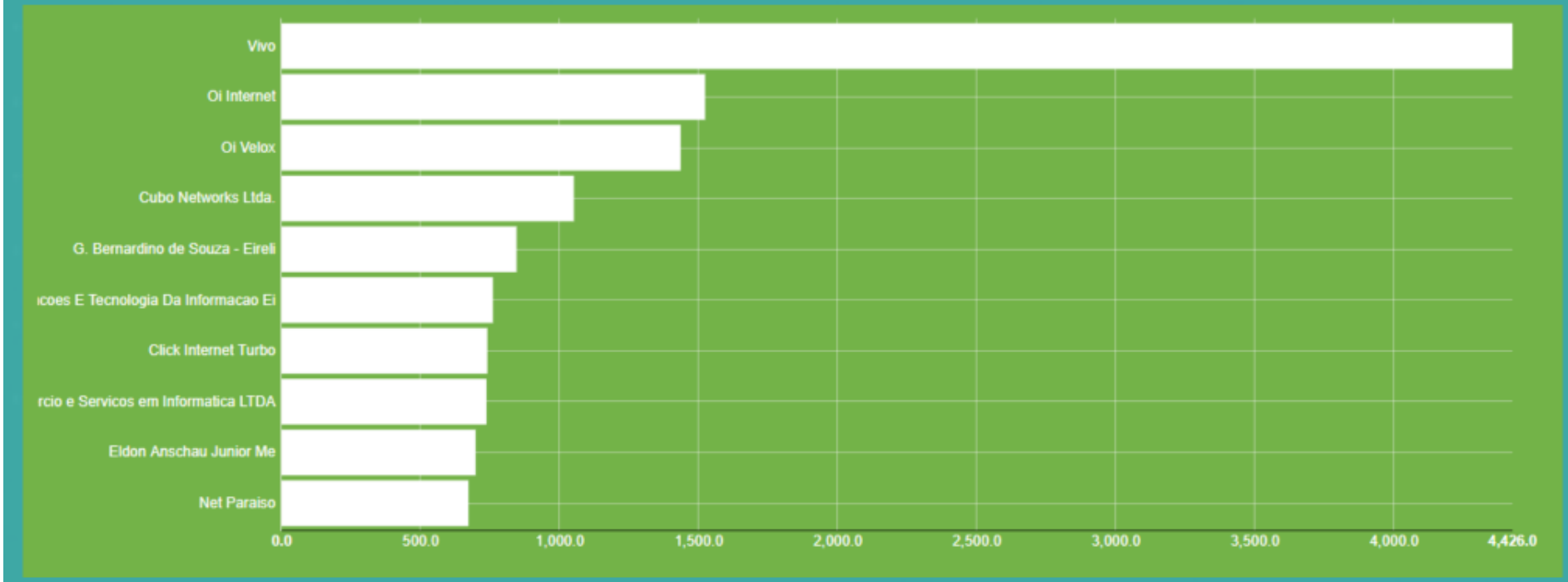



pronetworks


Script Coinhive - Mundo
Total: (217,862)
1. Brazil 60,115
2. India 23,291
3. Indonesia 21,808
4. Iran, Islamic Republic of 14,414
5. South Africa 8,990
6. Thailand 5,577
7. United States 5,186
8. Russian Federation 5,017
9. Bangladesh 3,481
10. Argentina 3,434
pronetworks
Search for product:"Mikrotik" http.component:"coinhive" returned 217,862 results on 28-10-2018


Principais Cidades - Brasil
1. Recife 1,776
2. Sao Paulo 1,407
3. Rio De Janeiro 1,177
4. Rio Do Sul 1,050
5. Marica 785
6. Salvador 728
7. Fortaleza 695
8. Araraquara 686
9. Porteirinha 575
10. Passos 530
pronetworks

# Principais Empresas



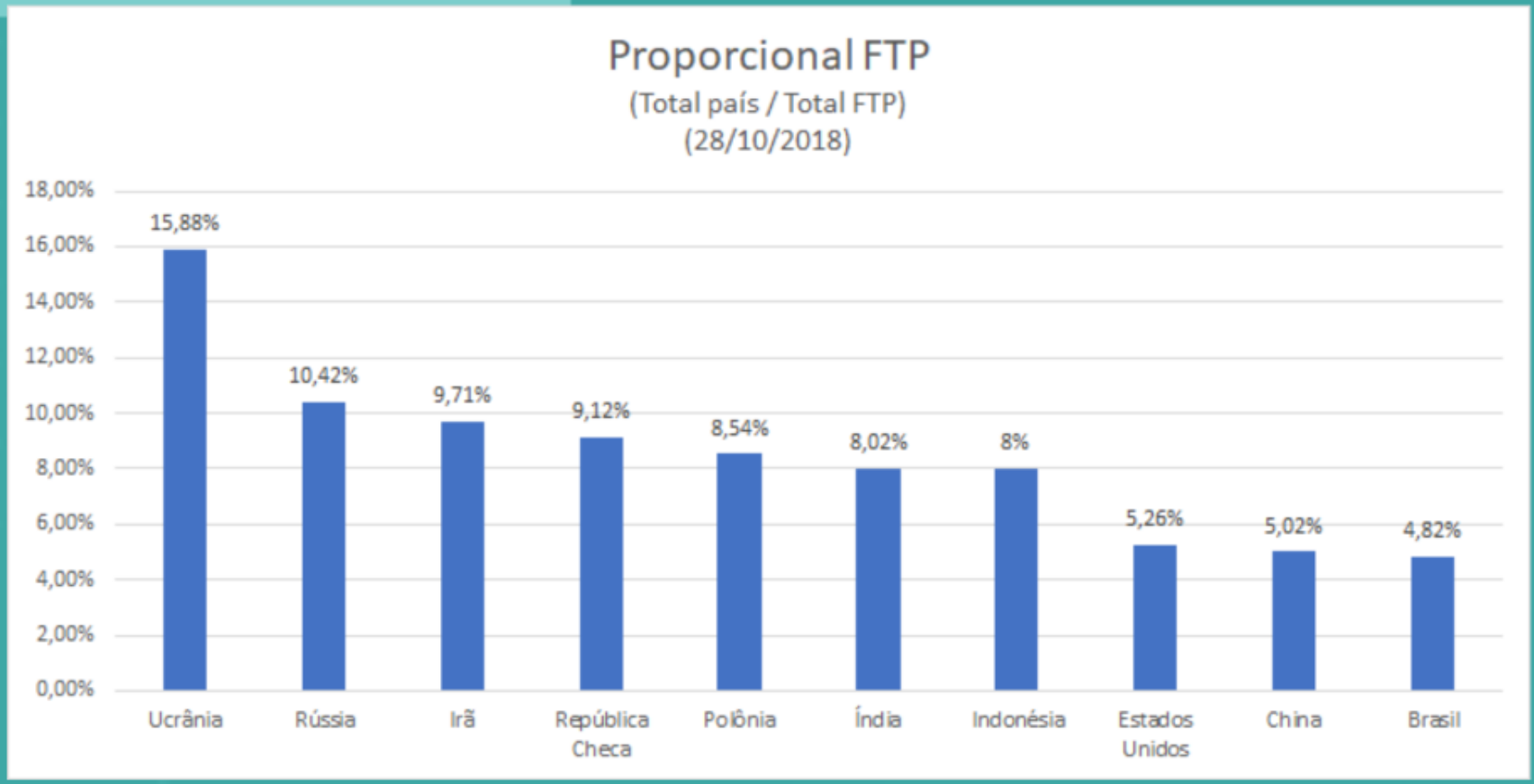

pronetworks


Total FTP
1. Brazil 38,504
2. Russian Federation 22,735
3. Iran, Islamic Republic of 20,123
4. Indonesia 19,871
5. China 17,627
6. India 16,034
7. Ukraine 15,989
8. Poland 12,982
9. United States 11,885
10. Czechia 8,993
Search for product:"Mikrotik" port:"21" returned 310,097 results on 28-10-2018
pronetworks


Porta 8080
1. Brazil 59,232
2. Indonesia 21,236
3. Iran, Islamic Republic of 20,794
4. India 18,229
5. Russian Federation 12,952
6. South Africa 9,334
7. Thailand 9,210
8. Italy 6,290
9. Ukraine 5,296
10. Argentina 5,264
pronetworks
Search for product:"Mikrotik" port:"8080" returned 251,210 results on 28-10-2018

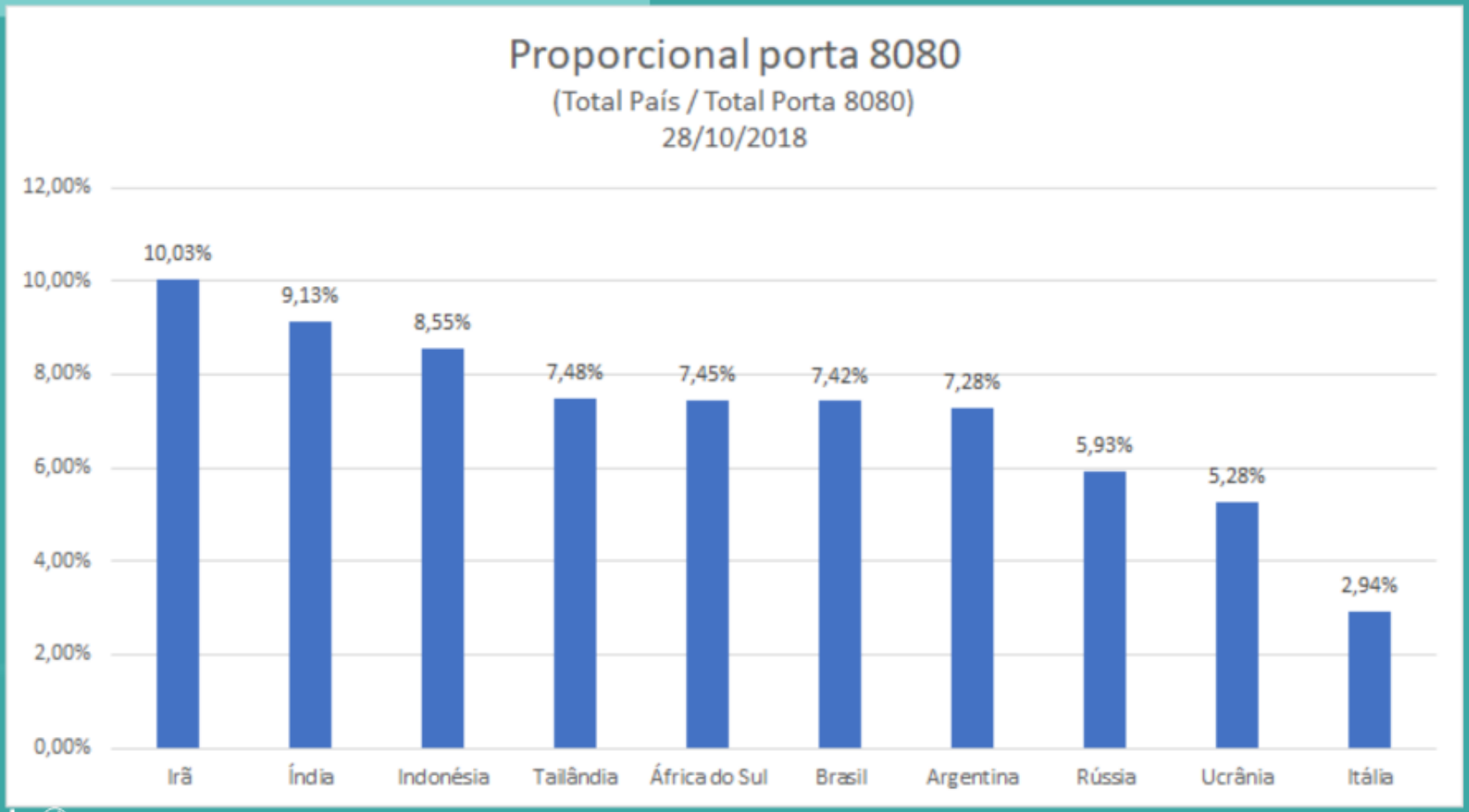

HTTP 80
1. Brazil 43,243
2. India 35,838
3. Indonesia 23,689
4. Iran, Islamic Republic of 9,534
5. Argentina 8,961
6. United States 8,446
7. Bangladesh 5,779
8. Russian Federation 5,746
9. Italy 5,169
10. Poland 5,082
pronetworks
Search for product:"Mikrotik" port:"80" returned 223,724 results on 28-10-2018

# Analise proporcional FTP



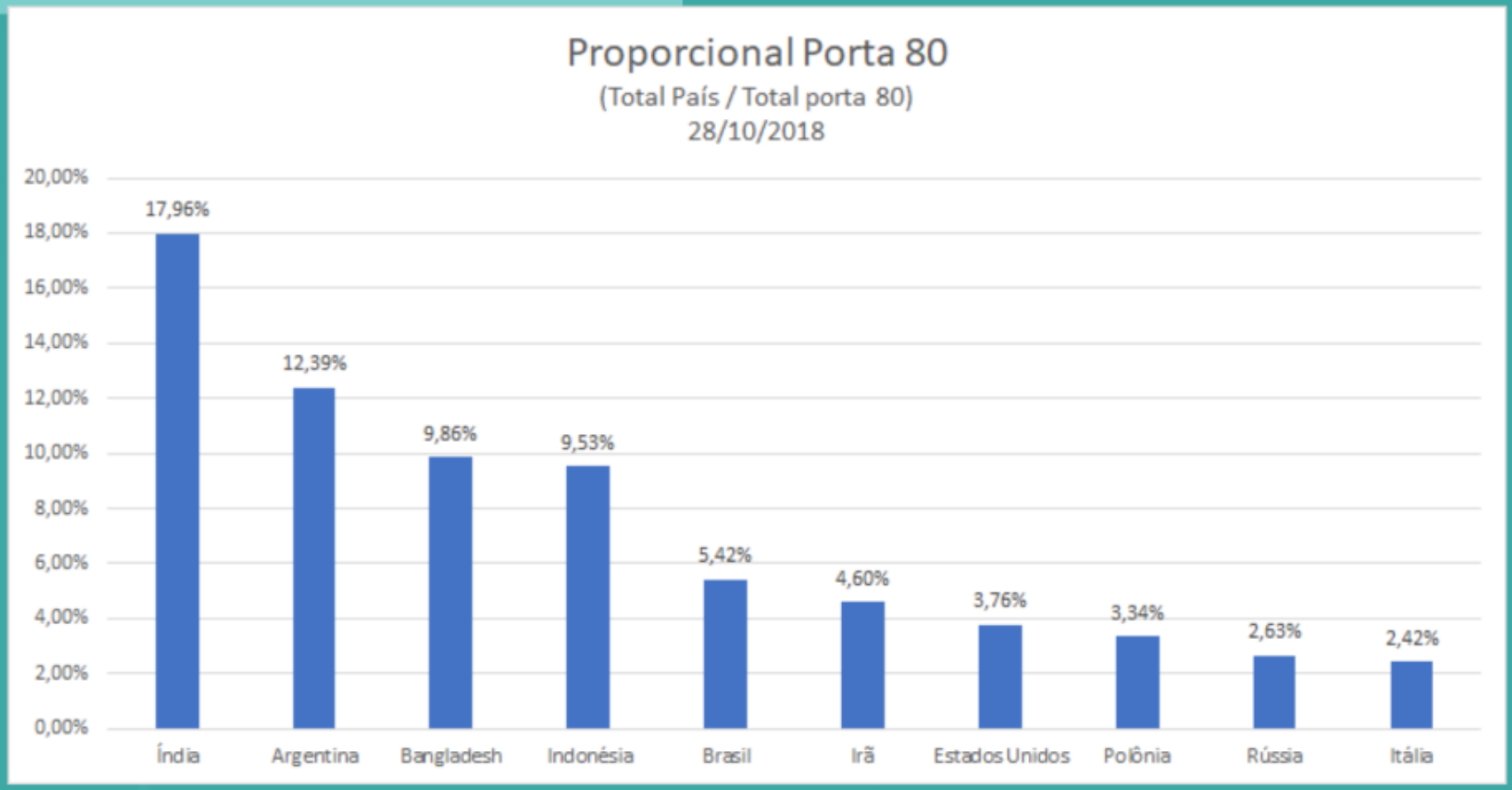

pronetworks

# Analise proporcional 8080



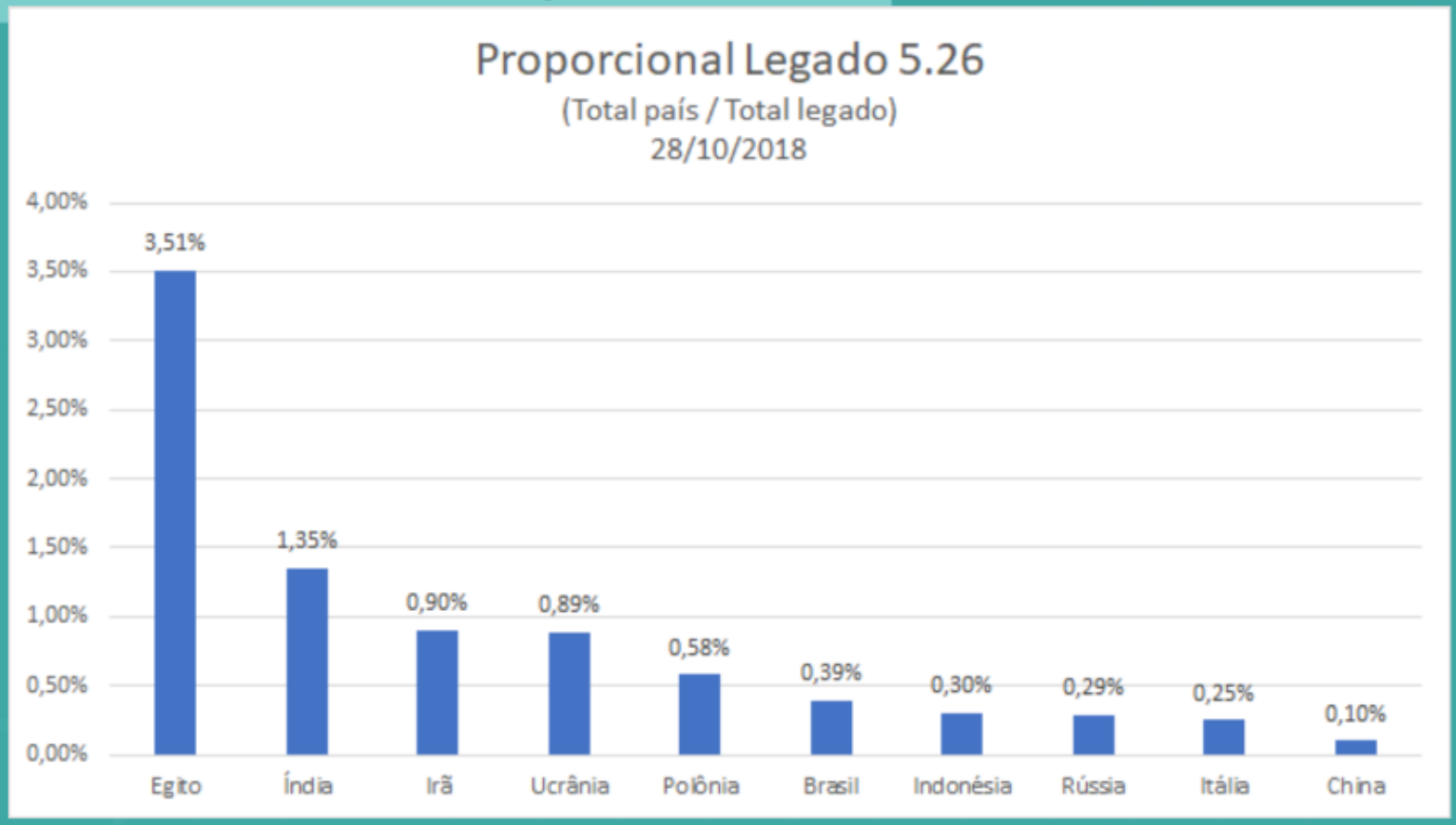

pronetworks

# Analise proporcional 80




pronetworks

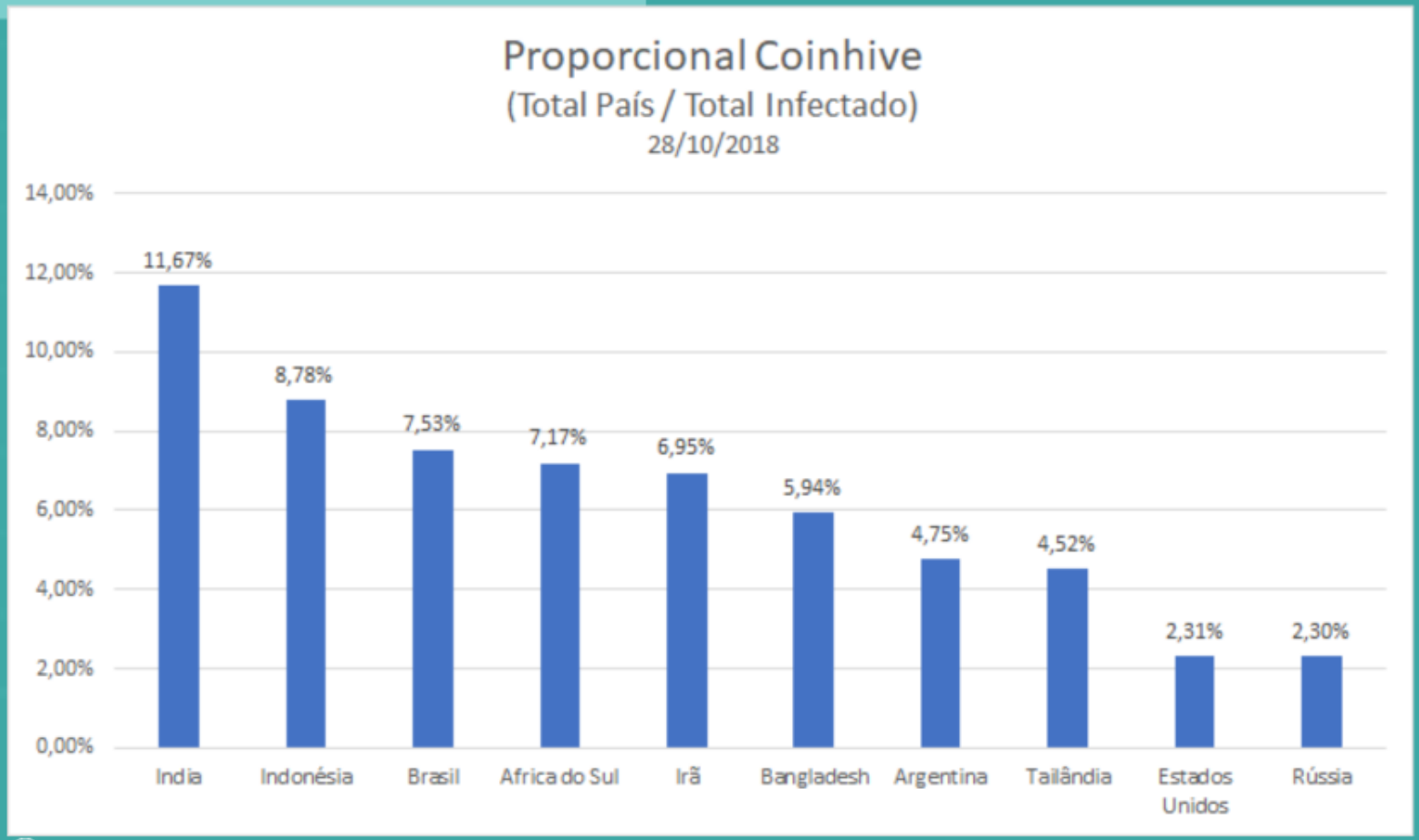
# Analise proporcional legado 5.26*



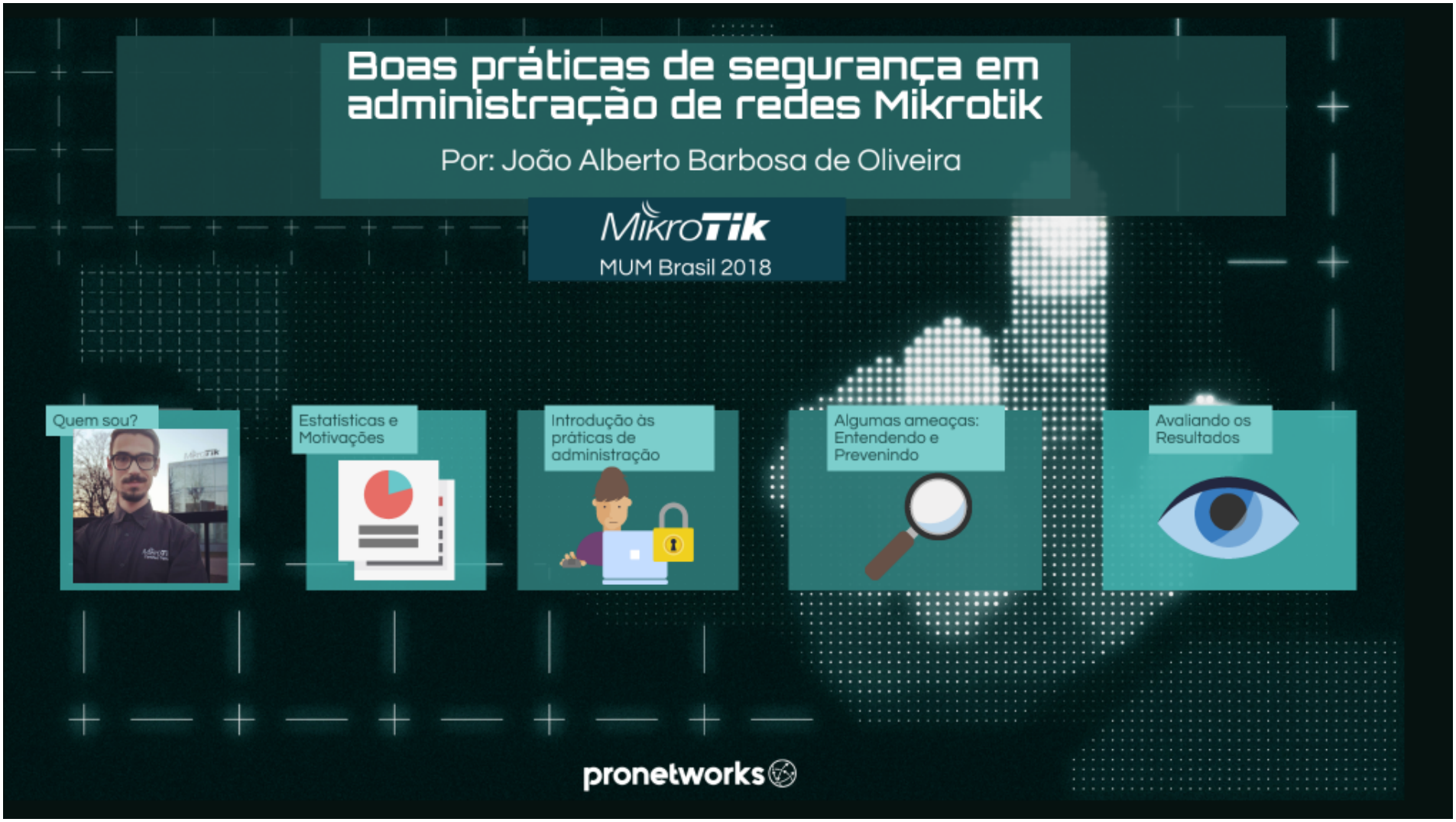

*versões com base em dados extraídos dos serviços FTP

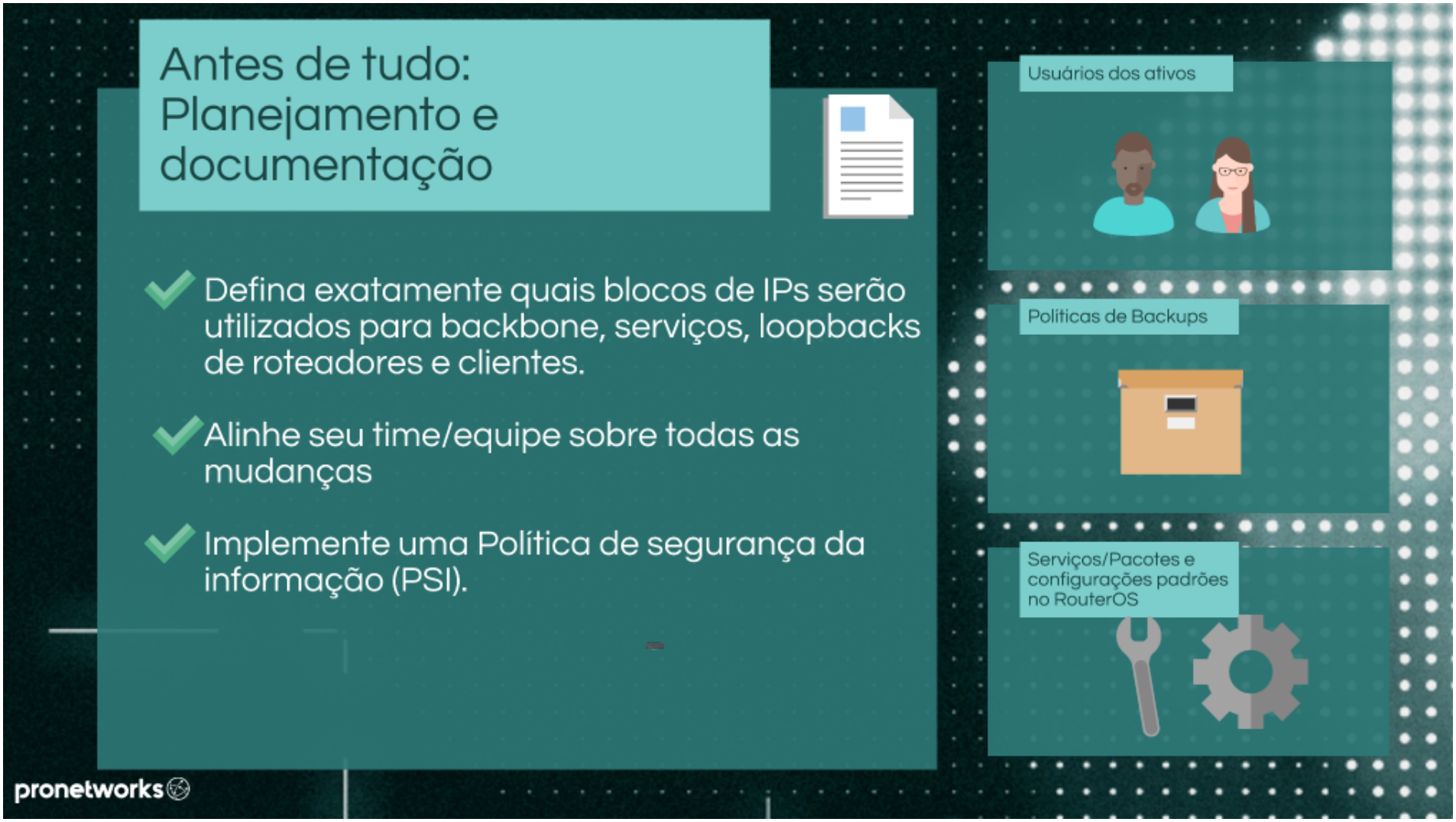
pronetworks

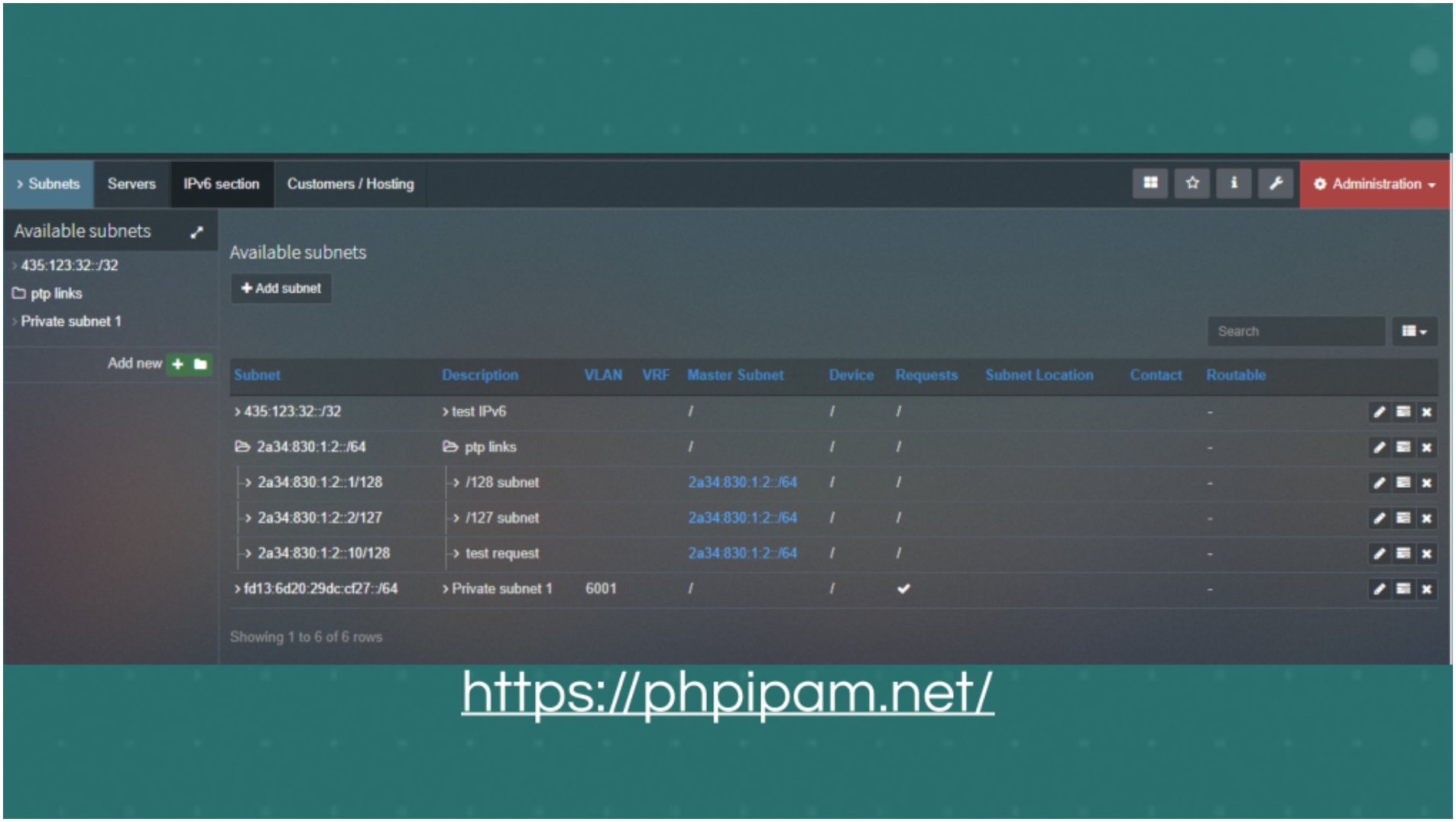
# Analise proporcional Coinhive




pronetworks


Boas práticas de segurança em administração de redes Mikrotik
Por: João Alberto Barbosa de Oliveira
MikroTik
MUM Brasil 2018
Quem sou?
Estatísticas e Motivações
Introdução às práticas de administração
Algumas ameaças: Entendendo e Prevenindo
Avaliando os Resultados
pronetworks


Antes de tudo:
Planejamento e
documentação
Defina exatamente quais blocos de IPs serão utilizados para backbone, serviços, loopbacks de roteadores e clientes.
Alinhe seu time/equipe sobre todas as mudanças
Implemente uma Política de segurança da informação (PSI).
Usuários dos ativos
Políticas de Backups
Serviços/Pacotes e configurações padrões no RouterOS
pronetworks



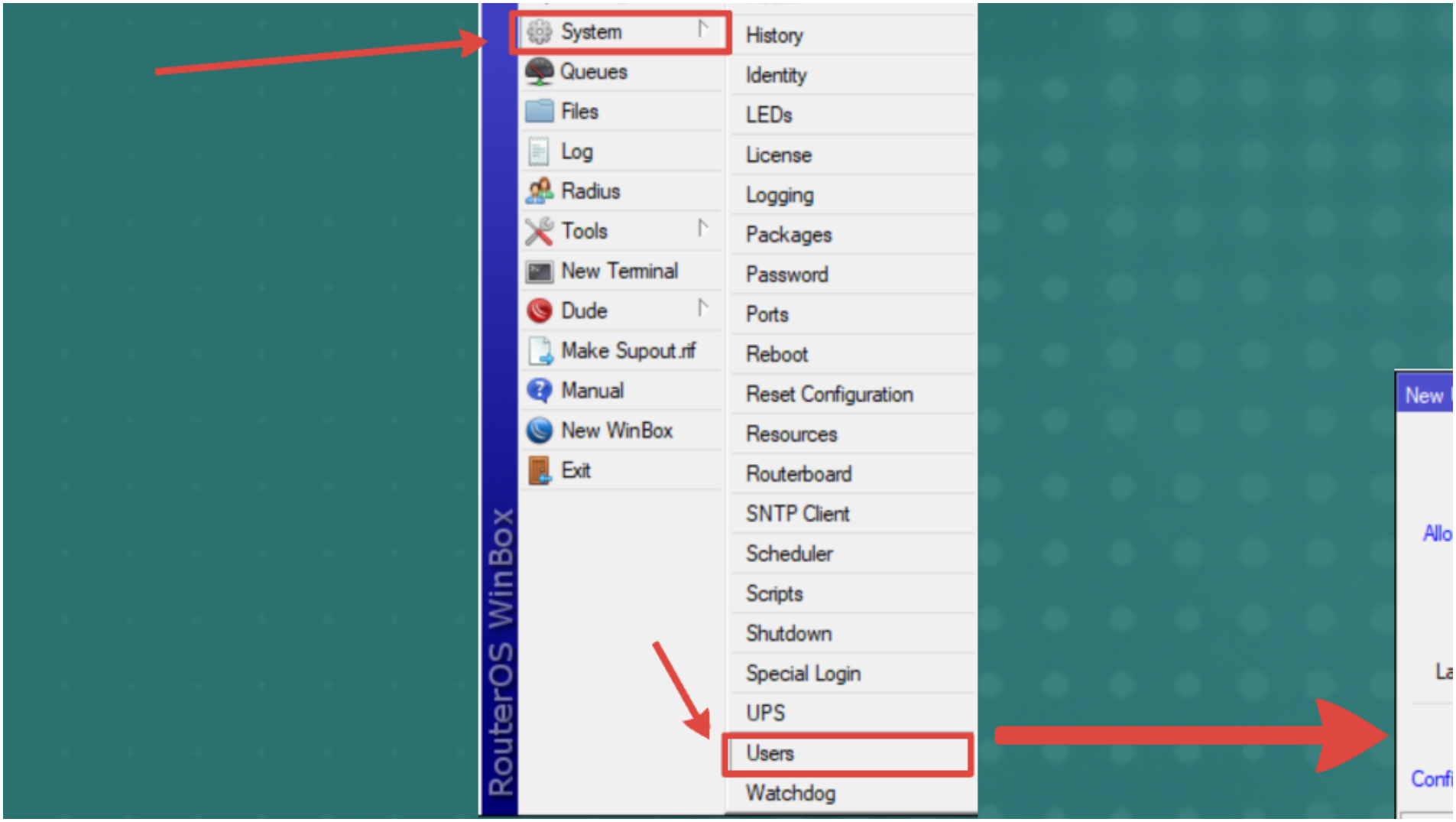

https://phpipam.net/

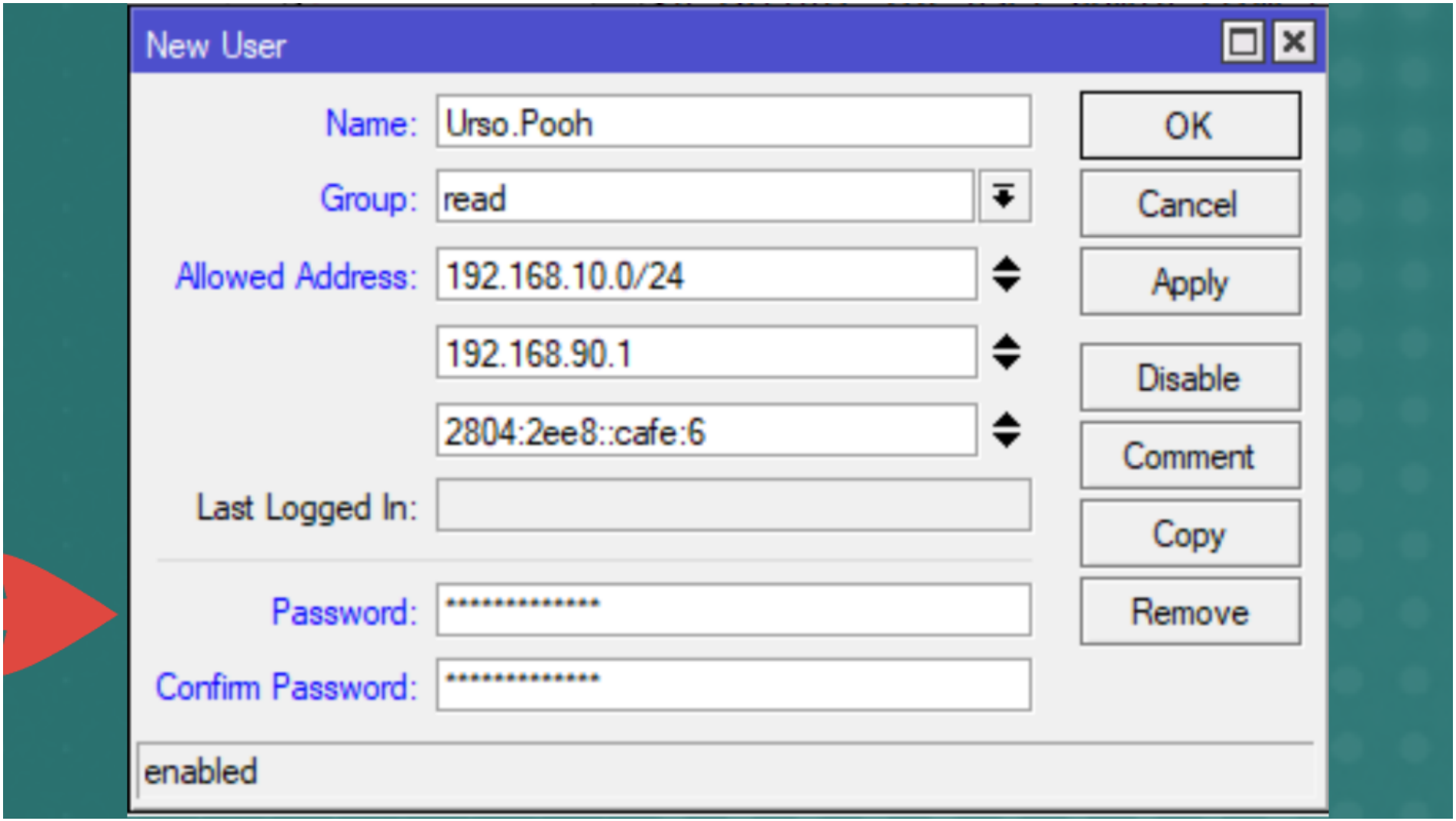
# Usuários dos ativos

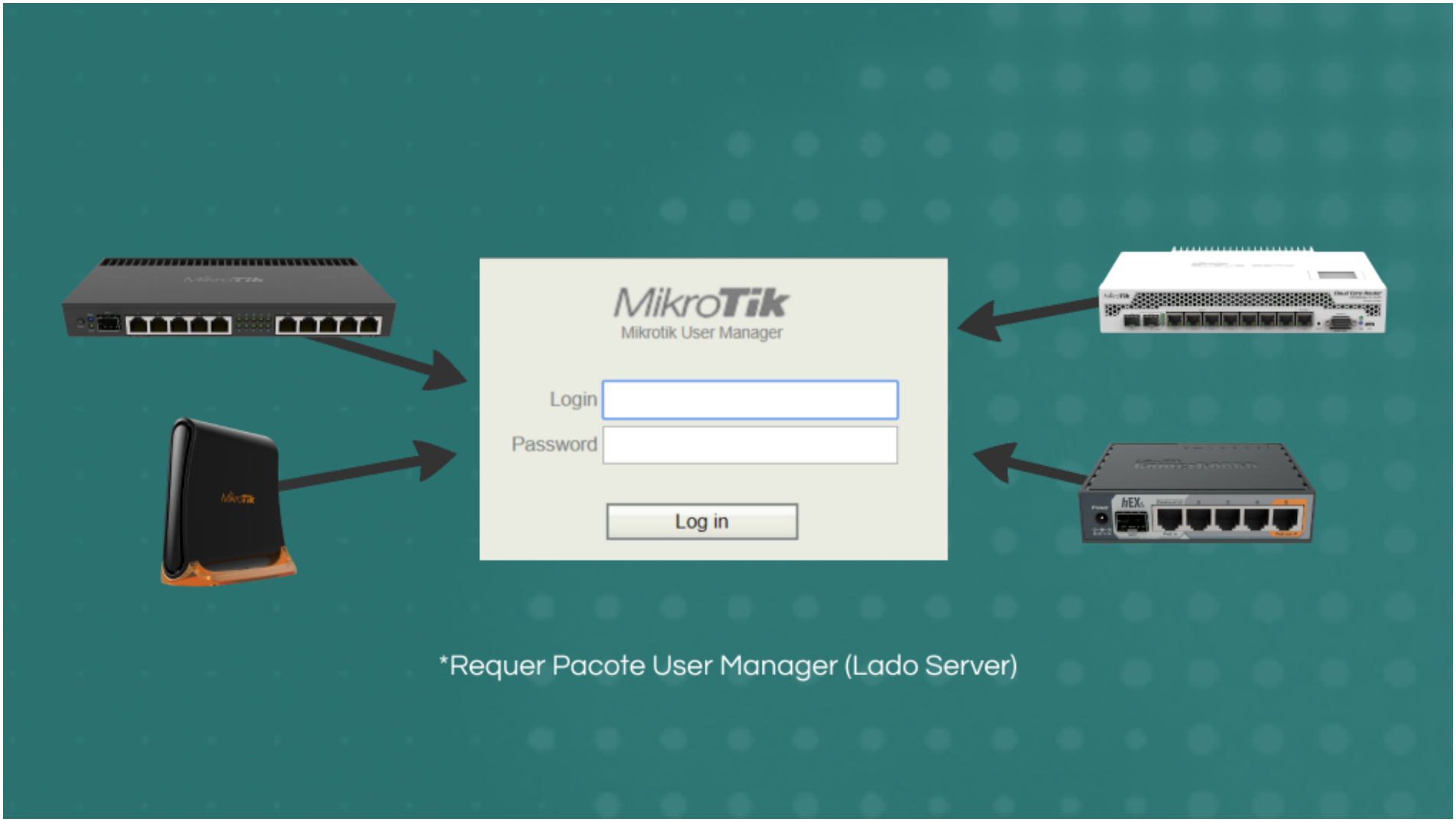
## Senhas de Usuários:

- SENHA: A PRIMEIRA recomendação antes de qualquer outra configuração!
- No Mikrotik RouterOS podemos acessar a base local de usuários no menu "/user";
- O usuário padrão é "admin" com senha "em branco". É estritamente recomendado a alteração do mesmo!
- Crie uma conta para cada usuário.
- Recomenda-se o uso de senhas fortes e com trocas periódicas!
- O RouterOS proporciona a possibilidade de autenticação via Radius*;

pronetworks


RouterOS WinBox
System
Queues
Files
Log
Radius
Tools
New Terminal
Dude
Make Supout.rif
Manual
New WinBox
Exit
History
Identity
LEDs
License
Logging
Packages
Password
Ports
Reboot
Reset Configuration
Resources
Routerboard
SNTP Client
Scheduler
Scripts
Shutdown
Special Login
UPS
Users
Watchdog


New User
Name:
Urso.Pooh
Group:
read
Allowed Address:
192.168.10.0/24
192.168.90.1
2804:2ee8::cafe:6
Last Logged In:
Password:
Confirm Password:
enabled
OK
Cancel
Apply
Disable
Comment
Copy
Remove


MikroTik
Mikrotik User Manager
Login
Password
Log in
*Requer Pacote User Manager (Lado Server)

## Políticas de Backups

- ✓ Extremamente útil na recuperação de desastres;
- ✓ Realize backups periódicos;
- ✓ Automatize o processo;
- ✗ Não salve os backups localmente!

pronetworks

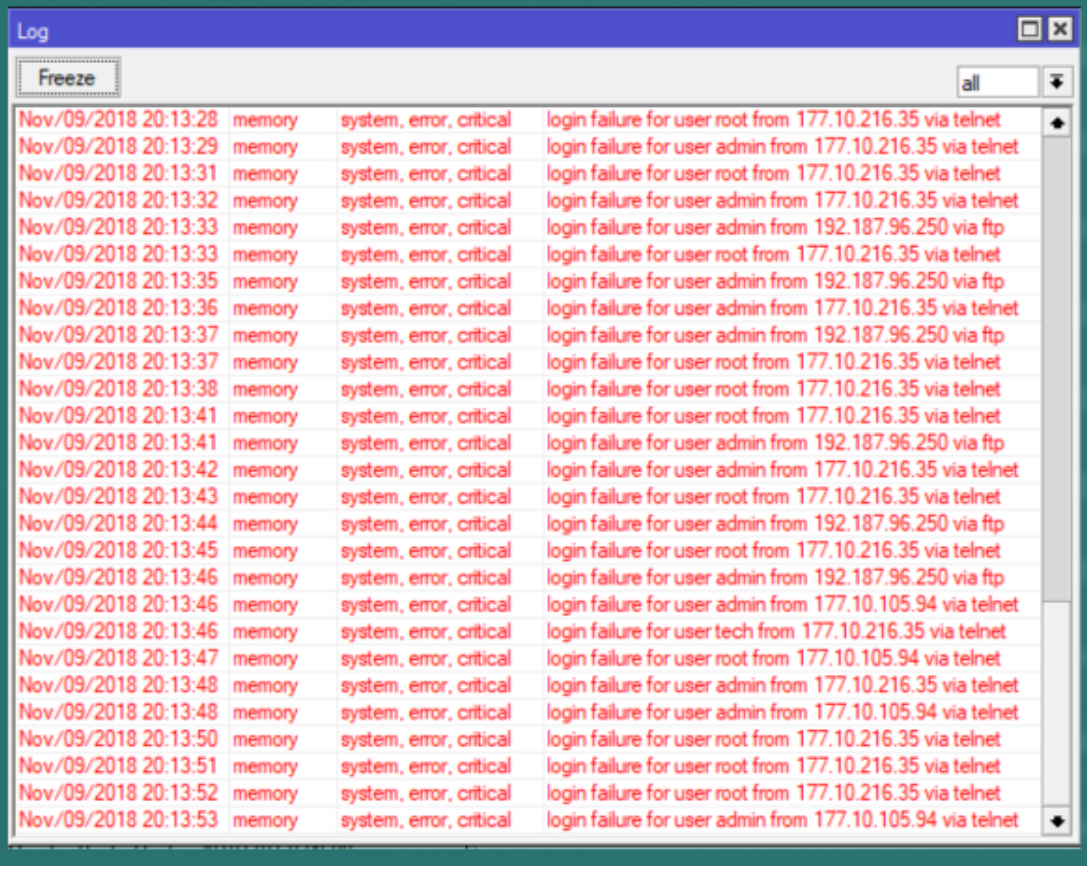
# Serviços/Pacotes e configurações padrões no RouterOS

Para facilitar a primeira Gerência, os dispositivos já vem com alguns serviços habilitados, em caso de não uso é necessário a alteração dos mesmos.

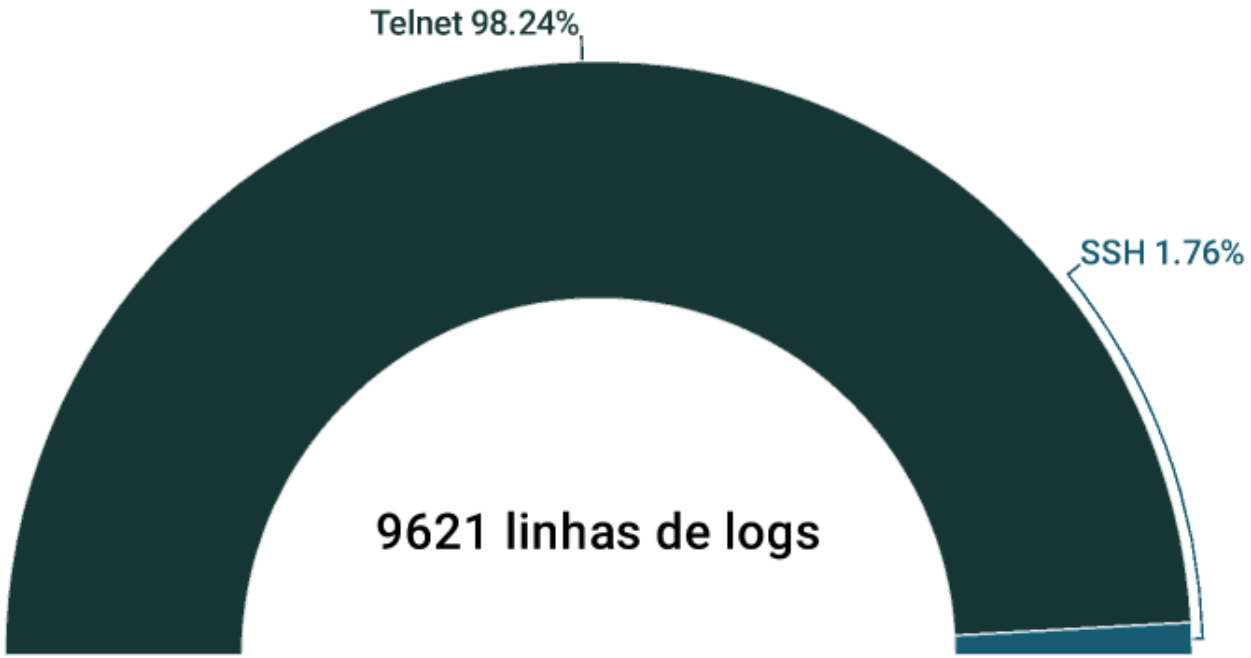
- ✔ Serviços padrões podem ter a porta modificada;
- ✘ Serviços que não oferecem segurança como o TELNET podem ser desabilitados;
- ✘ Serviços inutilizados, devem ser desabilitados;
- 👍 Alternativa: Mudar a porta padrão, e combinar com “knock knock”;

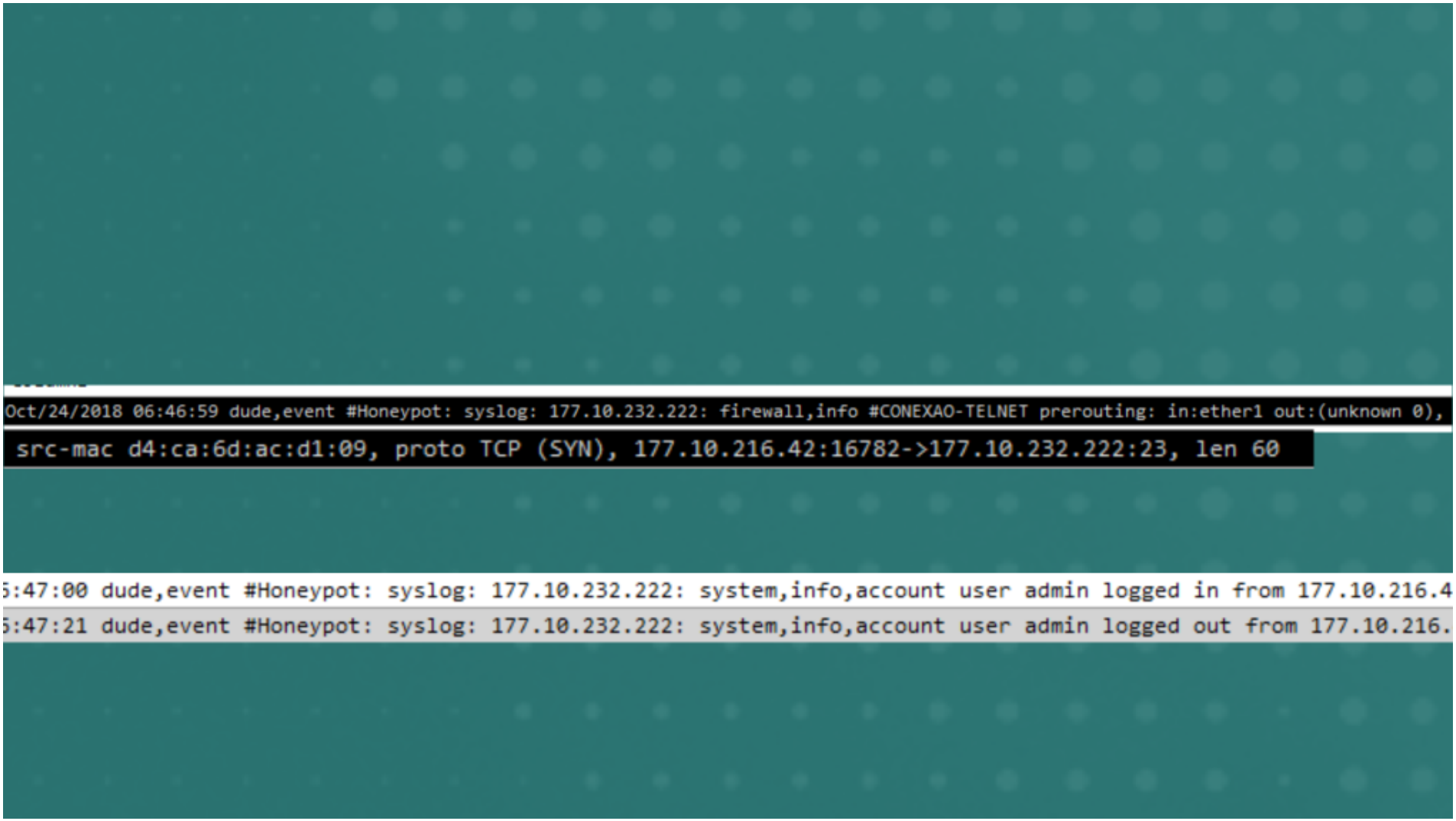

pronetworks

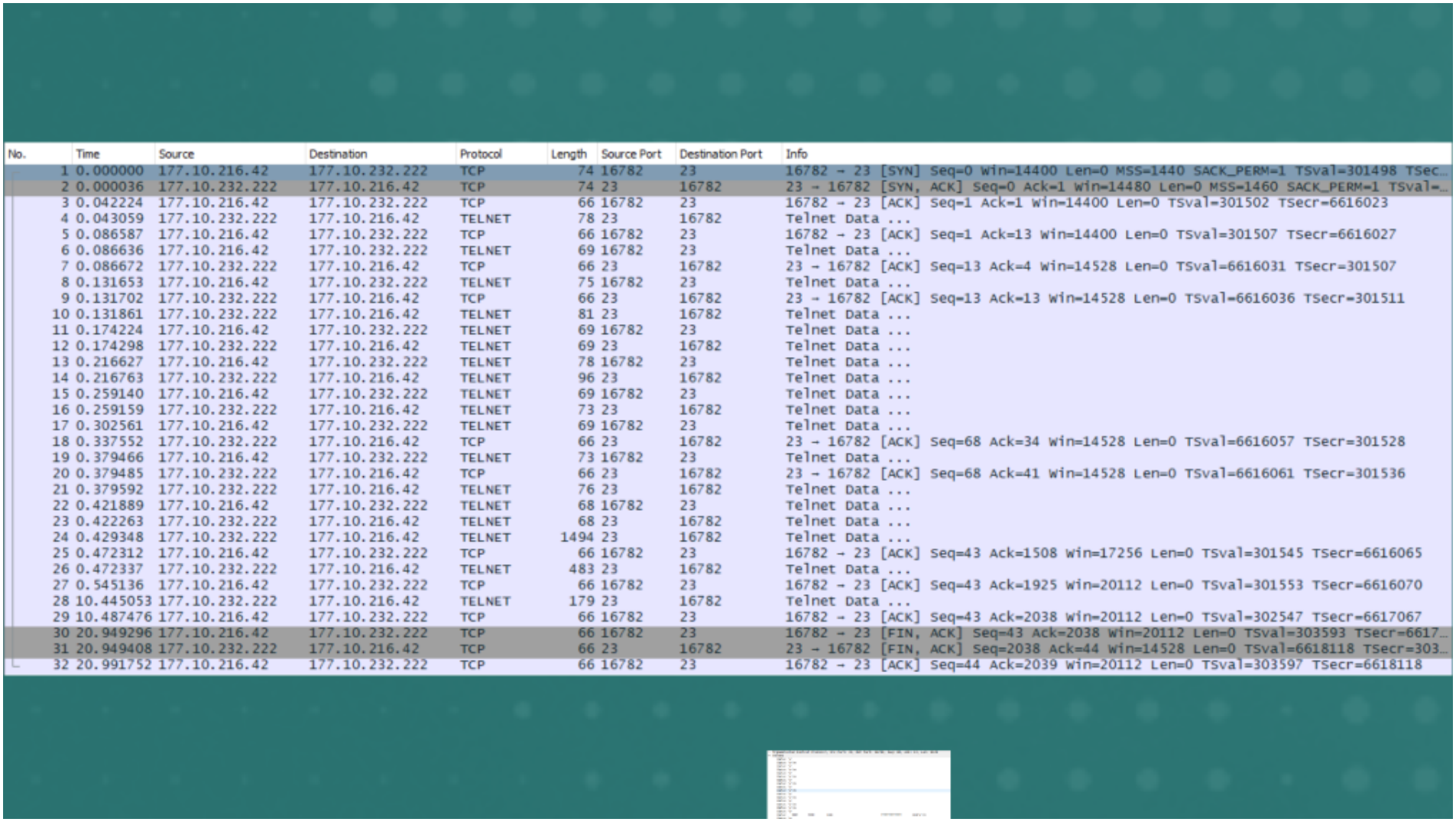
# Conheçe essa tela?



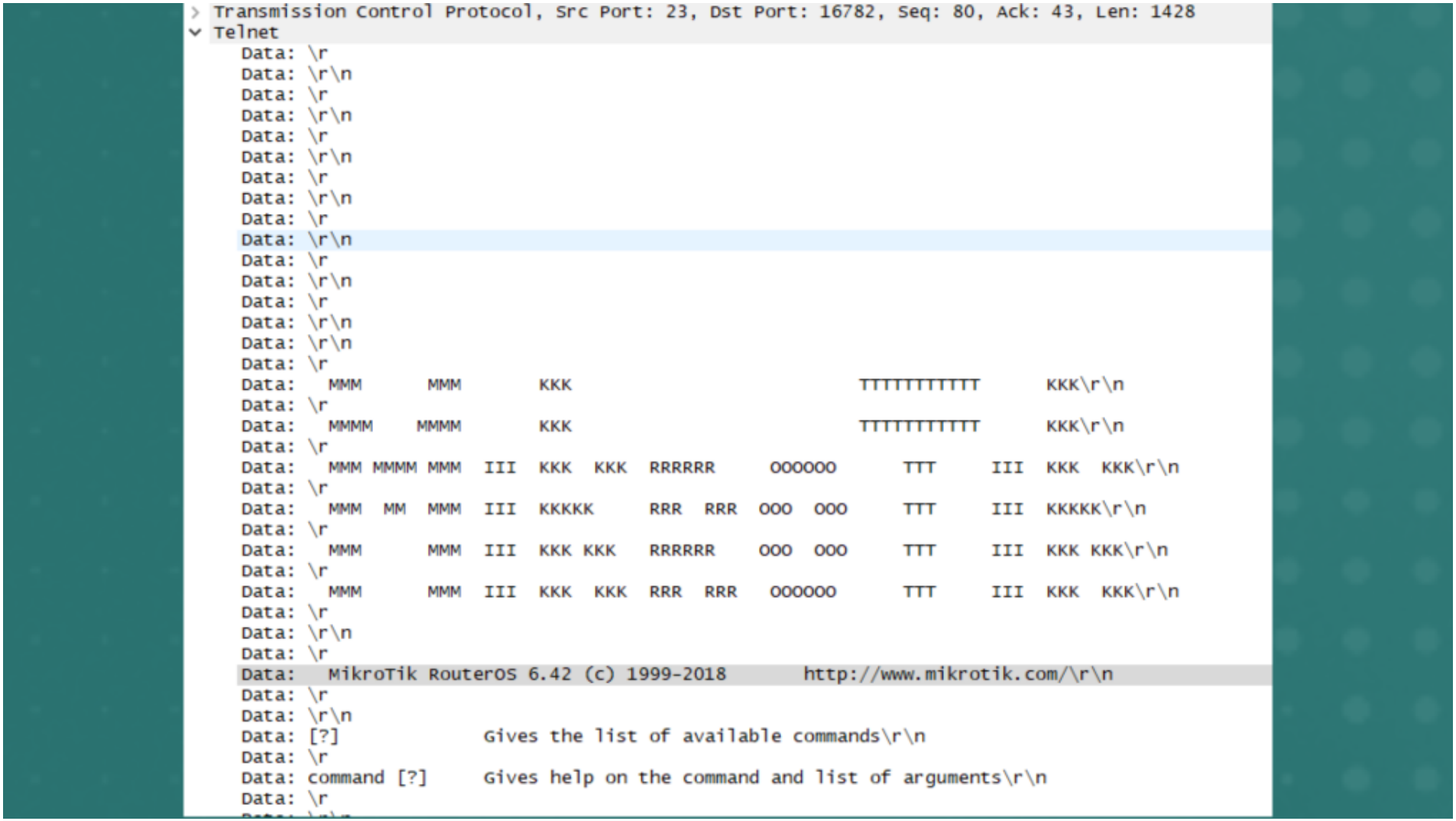

pronetworks

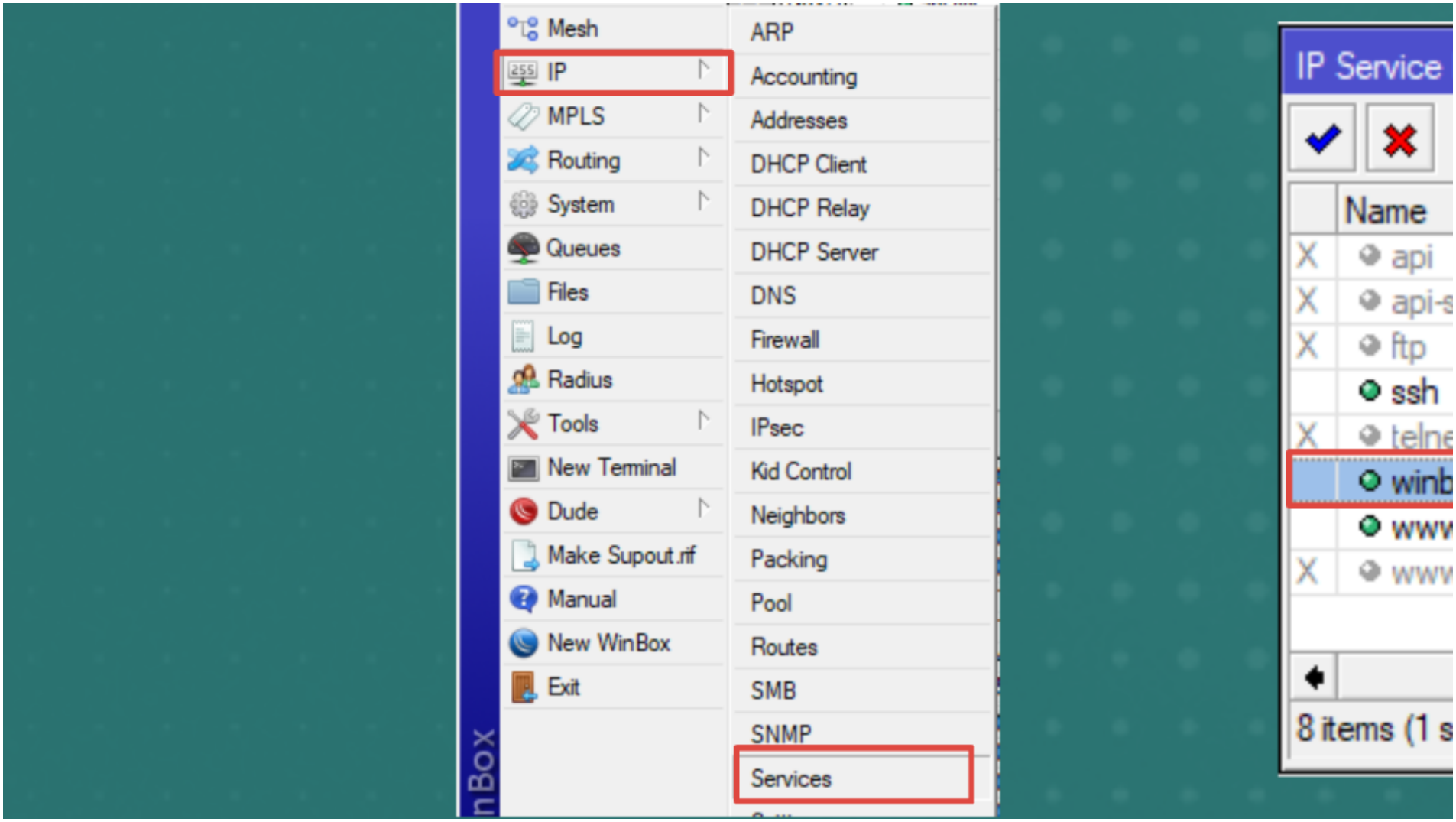

Telnet 98.24%
SSH 1.76%
9621 linhas de logs

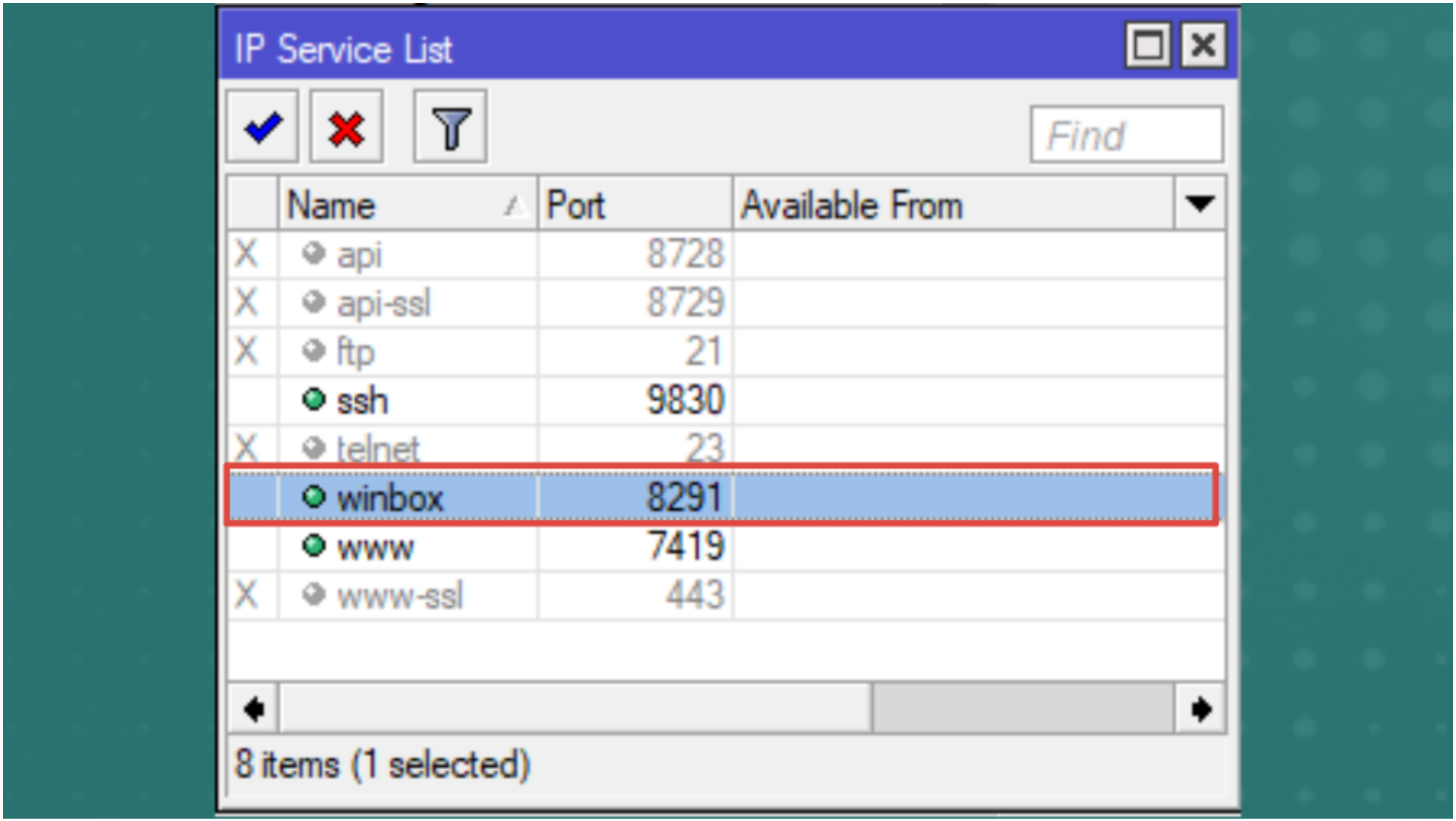

Oct/24/2018 06:46:59 dude,event #Honeypot: syslog: 177.10.232.222: firewall,info #CONEXAO-TELNET prerouting: in:ether1 out:(unknown 0),
src-mac d4:ca:6d:ac:d1:09, proto TCP (SYN), 177.10.216.42:16782->177.10.232.222:23, len 60
:47:00 dude,event #Honeypot: syslog: 177.10.232.222: system,info,account user admin logged in from 177.10.216.4
:47:21 dude,event #Honeypot: syslog: 177.10.232.222: system,info,account user admin logged out from 177.10.216.

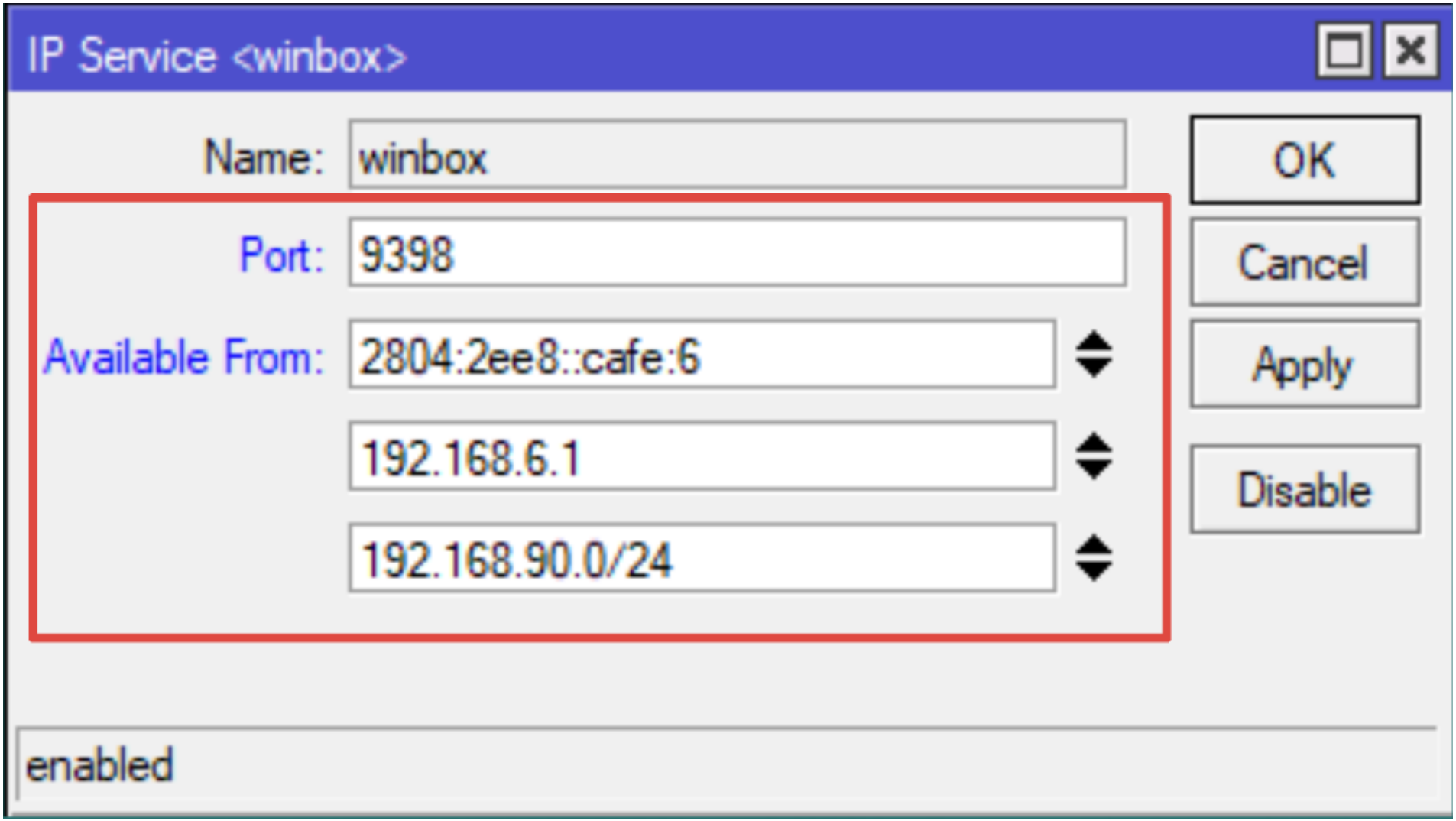


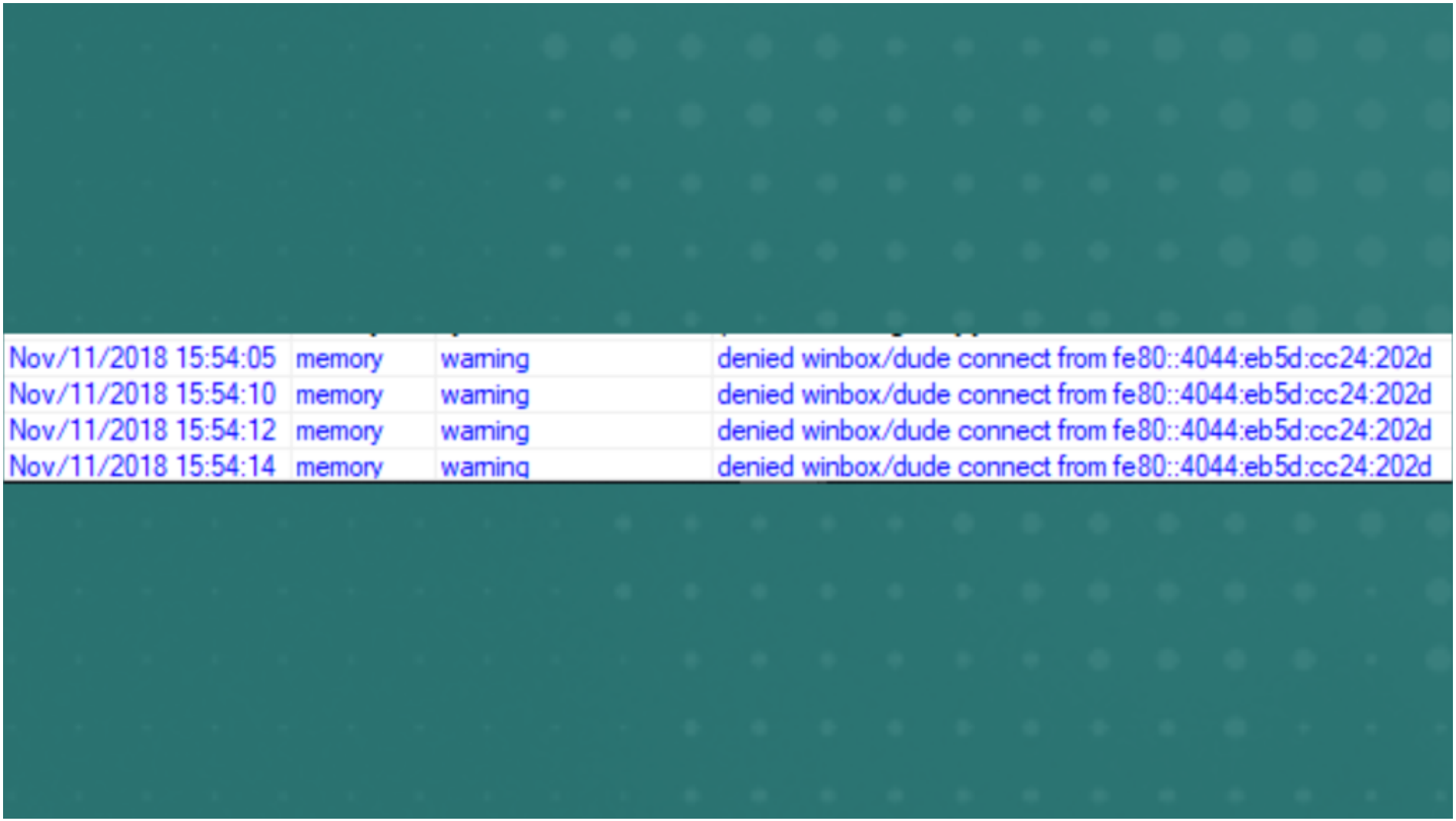
| No. | Time | Source | Destination | Protocol | Length | Source Port | Destination Port | Info |
|---|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | 177.10.216.42 | 177.10.232.222 | TCP | 74 | 16782 | 23 | 16782 → 23 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=301498 TSec… |
| 2 | 0.000036 | 177.10.232.222 | 177.10.216.42 | TCP | 74 | 23 | 16782 | 23 → 16782 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=… |
| 3 | 0.042224 | 177.10.216.42 | 177.10.232.222 | TCP | 66 | 16782 | 23 | 16782 → 23 [ACK] Seq=1 Ack=1 Win=14400 Len=0 TSval=301502 TSecr=6616023 |
| 4 | 0.043059 | 177.10.232.222 | 177.10.216.42 | TELNET | 78 | 23 | 16782 | Telnet Data ... |
| 5 | 0.086587 | 177.10.216.42 | 177.10.232.222 | TCP | 66 | 16782 | 23 | 16782 → 23 [ACK] Seq=1 Ack=13 Win=14400 Len=0 TSval=301507 TSecr=6616027 |
| 6 | 0.086636 | 177.10.216.42 | 177.10.232.222 | TELNET | 69 | 16782 | 23 | Telnet Data ... |
| 7 | 0.086672 | 177.10.232.222 | 177.10.216.42 | TCP | 66 | 23 | 16782 | 23 → 16782 [ACK] Seq=13 Ack=4 Win=14528 Len=0 TSval=6616031 TSecr=301507 |
| 8 | 0.131653 | 177.10.216.42 | 177.10.232.222 | TELNET | 75 | 16782 | 23 | Telnet Data ... |
| 9 | 0.131702 | 177.10.232.222 | 177.10.216.42 | TCP | 66 | 23 | 16782 | 23 → 16782 [ACK] Seq=13 Ack=13 Win=14528 Len=0 TSval=6616036 TSecr=301511 |
| 10 | 0.131861 | 177.10.232.222 | 177.10.216.42 | TELNET | 81 | 23 | 16782 | Telnet Data ... |
| 11 | 0.174224 | 177.10.216.42 | 177.10.232.222 | TELNET | 69 | 16782 | 23 | Telnet Data ... |
| 12 | 0.174298 | 177.10.232.222 | 177.10.216.42 | TELNET | 69 | 23 | 16782 | Telnet Data ... |
| 13 | 0.216627 | 177.10.216.42 | 177.10.232.222 | TELNET | 78 | 16782 | 23 | Telnet Data ... |
| 14 | 0.216763 | 177.10.232.222 | 177.10.216.42 | TELNET | 96 | 23 | 16782 | Telnet Data ... |
| 15 | 0.259140 | 177.10.216.42 | 177.10.232.222 | TELNET | 69 | 16782 | 23 | Telnet Data ... |
| 16 | 0.259159 | 177.10.232.222 | 177.10.216.42 | TELNET | 73 | 23 | 16782 | Telnet Data ... |
| 17 | 0.302561 | 177.10.216.42 | 177.10.232.222 | TELNET | 69 | 16782 | 23 | Telnet Data ... |
| 18 | 0.337552 | 177.10.232.222 | 177.10.216.42 | TCP | 66 | 23 | 16782 | 23 → 16782 [ACK] Seq=68 Ack=34 Win=14528 Len=0 TSval=6616057 TSecr=301528 |
| 19 | 0.379466 | 177.10.216.42 | 177.10.232.222 | TELNET | 73 | 16782 | 23 | Telnet Data ... |
| 20 | 0.379485 | 177.10.232.222 | 177.10.216.42 | TCP | 66 | 23 | 16782 | 23 → 16782 [ACK] Seq=68 Ack=41 Win=14528 Len=0 TSval=6616061 TSecr=301536 |
| 21 | 0.379592 | 177.10.232.222 | 177.10.216.42 | TELNET | 76 | 23 | 16782 | Telnet Data ... |
| 22 | 0.421889 | 177.10.216.42 | 177.10.232.222 | TELNET | 68 | 16782 | 23 | Telnet Data ... |
| 23 | 0.422263 | 177.10.232.222 | 177.10.216.42 | TELNET | 68 | 23 | 16782 | Telnet Data ... |
| 24 | 0.429348 | 177.10.232.222 | 177.10.216.42 | TELNET | 1494 | 23 | 16782 | Telnet Data ... |
| 25 | 0.472312 | 177.10.216.42 | 177.10.232.222 | TCP | 66 | 16782 | 23 | 16782 → 23 [ACK] Seq=43 Ack=1508 Win=17256 Len=0 TSval=301545 TSecr=6616065 |
| 26 | 0.472337 | 177.10.232.222 | 177.10.216.42 | TELNET | 483 | 23 | 16782 | Telnet Data ... |
| 27 | 0.545136 | 177.10.216.42 | 177.10.232.222 | TCP | 66 | 16782 | 23 | 16782 → 23 [ACK] Seq=43 Ack=1925 Win=20112 Len=0 TSval=301553 TSecr=6616070 |
| 28 | 10.445053 | 177.10.232.222 | 177.10.216.42 | TELNET | 179 | 23 | 16782 | Telnet Data ... |
| 29 | 10.487476 | 177.10.216.42 | 177.10.232.222 | TCP | 66 | 16782 | 23 | 16782 → 23 [ACK] Seq=43 Ack=2038 Win=20112 Len=0 TSval=302547 TSecr=6617067 |
| 30 | 20.949296 | 177.10.216.42 | 177.10.232.222 | TCP | 66 | 16782 | 23 | 16782 → 23 [FIN, ACK] Seq=43 Ack=2038 Win=20112 Len=0 TSval=303593 TSecr=6617… |
| 31 | 20.949408 | 177.10.232.222 | 177.10.216.42 | TCP | 66 | 23 | 16782 | 23 → 16782 [FIN, ACK] Seq=2038 Ack=44 Win=14528 Len=0 TSval=6618118 TSecr=303… |
| 32 | 20.991752 | 177.10.216.42 | 177.10.232.222 | TCP | 66 | 16782 | 23 | 16782 → 23 [ACK] Seq=44 Ack=2039 Win=20112 Len=0 TSval=303597 TSecr=6618118 |


Transmission Control Protocol, Src Port: 23, Dst Port: 16782, Seq: 80, Ack: 43, Len: 1428
Telnet
Data: \r
Data: \r\n
Data: \r
Data: \r\n
Data: \r
Data: \r\n
Data: \r
Data: \r\n
Data: \r
Data: \r\n
Data: \r
Data: \r\n
Data: \r\n
Data: \r
Data: MMM MMM KKK TTTTTTTTTTT KKK\r\n
Data: \r
Data: MMMM MMMM KKK TTTTTTTTTTT KKK\r\n
Data: \r
Data: MMM MMMM MMM III KKK KKK RRRRRR OOOOOO TTT III KKK KKK\r\n
Data: \r
Data: MMM MM MMM III KKKKK RRR RRR OOO OOO TTT III KKKKK\r\n
Data: \r
Data: MMM MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK\r\n
Data: \r
Data: MMM MMM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK\r\n
Data: \r
Data: \r\n
Data: \r
Data: MikroTik RouterOS 6.42 (c) 1999-2018 http://www.mikrotik.com/\r\n
Data: \r
Data: \r\n
Data: [?] Gives the list of available commands\r\n
Data: \r
Data: command [?] Gives help on the command and list of arguments\r\n
Data: \r


Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Dude
Make Supout.rif
Manual
New WinBox
Exit
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Kid Control
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
IP Service
Name
api
ssh
8 items (1 s


IP Service List
Find
Name
Port
Available From
X api 8728
X api-ssl 8729
X ftp 21
ssh 9830
X telnet 23
winbox 8291
www 7419
X www-ssl 443
8 items (1 selected)


IP Service <winbox>
Name:
winbox
Port:
9398
Available From:
2804:2ee8::cafe:6
192.168.6.1
192.168.90.0/24
OK
Cancel
Apply
Disable
enabled


Nov/11/2018 15:54:05 memory warning denied winbox/dude connect from fe80::4044:eb5d:cc24:202d
Nov/11/2018 15:54:10 memory warning denied winbox/dude connect from fe80::4044:eb5d:cc24:202d
Nov/11/2018 15:54:12 memory warning denied winbox/dude connect from fe80::4044:eb5d:cc24:202d
Nov/11/2018 15:54:14 memory warning denied winbox/dude connect from fe80::4044:eb5d:cc24:202d

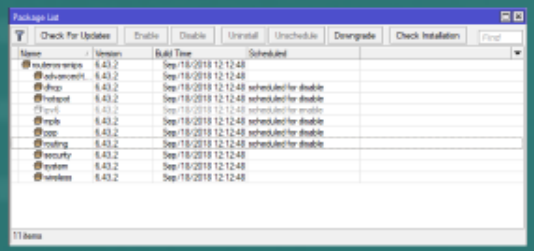
# Os IPs permitidos podem ser:

- IPs controlados de locais confiáveis e setores confiáveis de uma empresa.
- IPs de servidores VPN
- IPs Dinâmicos - Por address lists (em firewall)

# Pacotes no RouterOS

- Uma boa prática é habilitar apenas pacotes que sejam utilizados;
- Pacotes/serviços funcionando desnecessariamente, além de não serem úteis, podem servir de caminho para possíveis explorações;

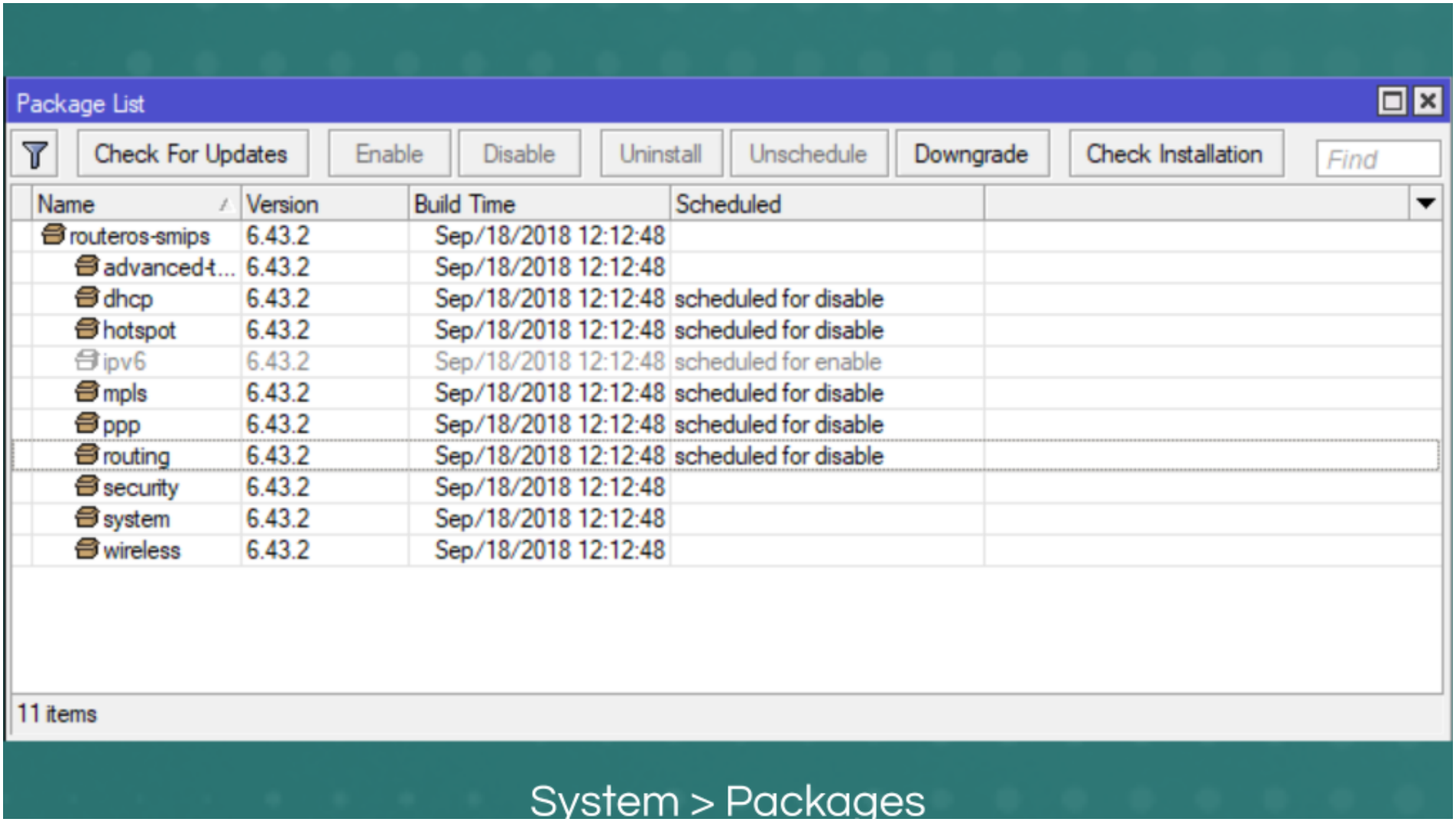
Segue uma lista de exemplo de pacotes:




System > Packages

https://wiki.mikrotik.com/wiki/Manual:System/Packages

pronetworks

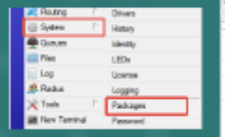
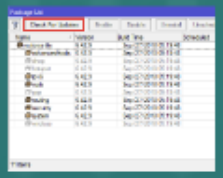
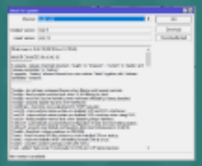



System > Packages

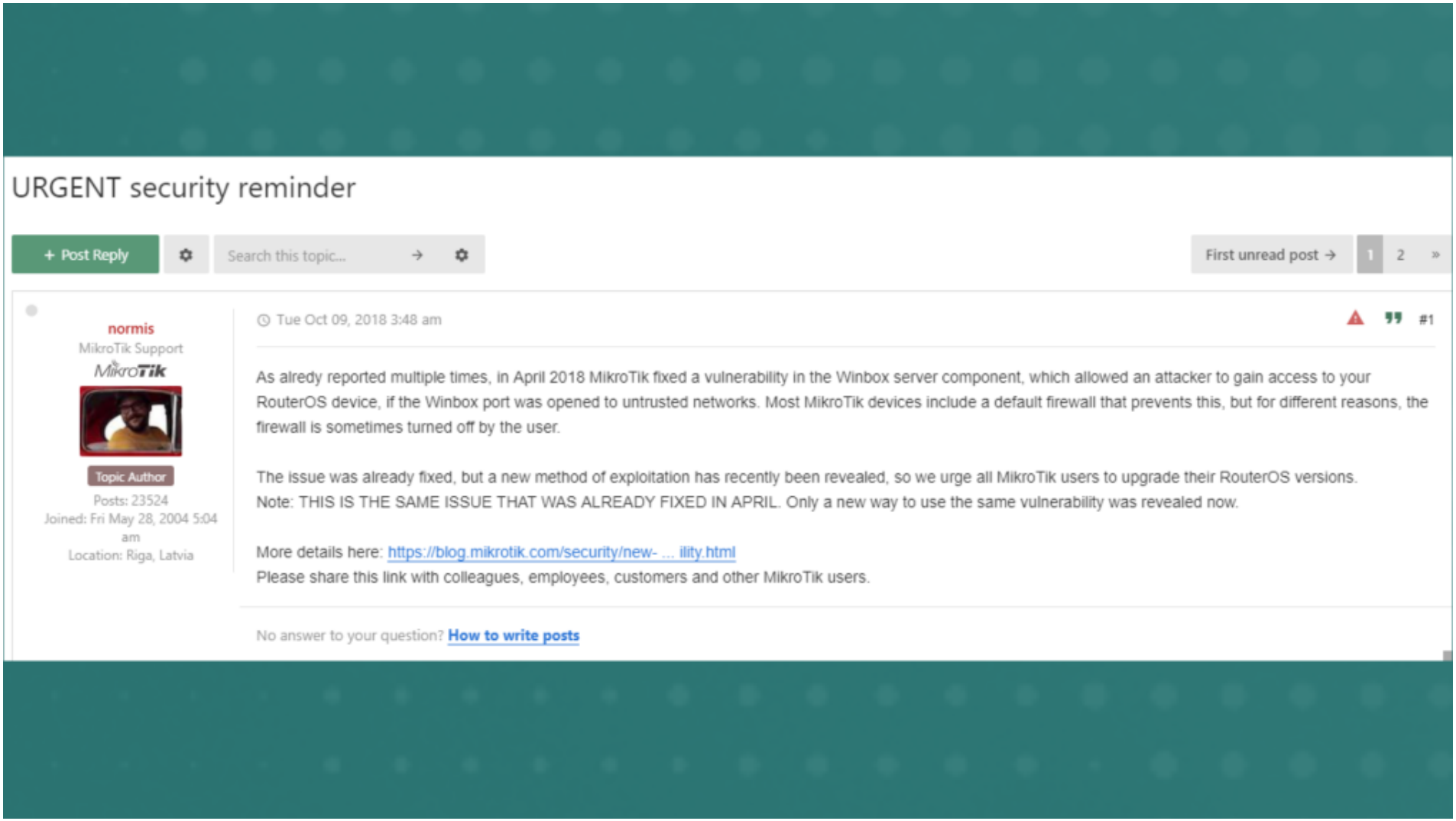
# A importância de atualizar o RouterOS

- Antes de atualizar, é importante ler os CHANGELOGS
- Changelogs são registros de correções e podem ser facilmente acessados em: https://mikrotik.com/download/changelogs
- A Mikrotik prioriza e corrige o mais breve possível questões de segurança, fique atento!



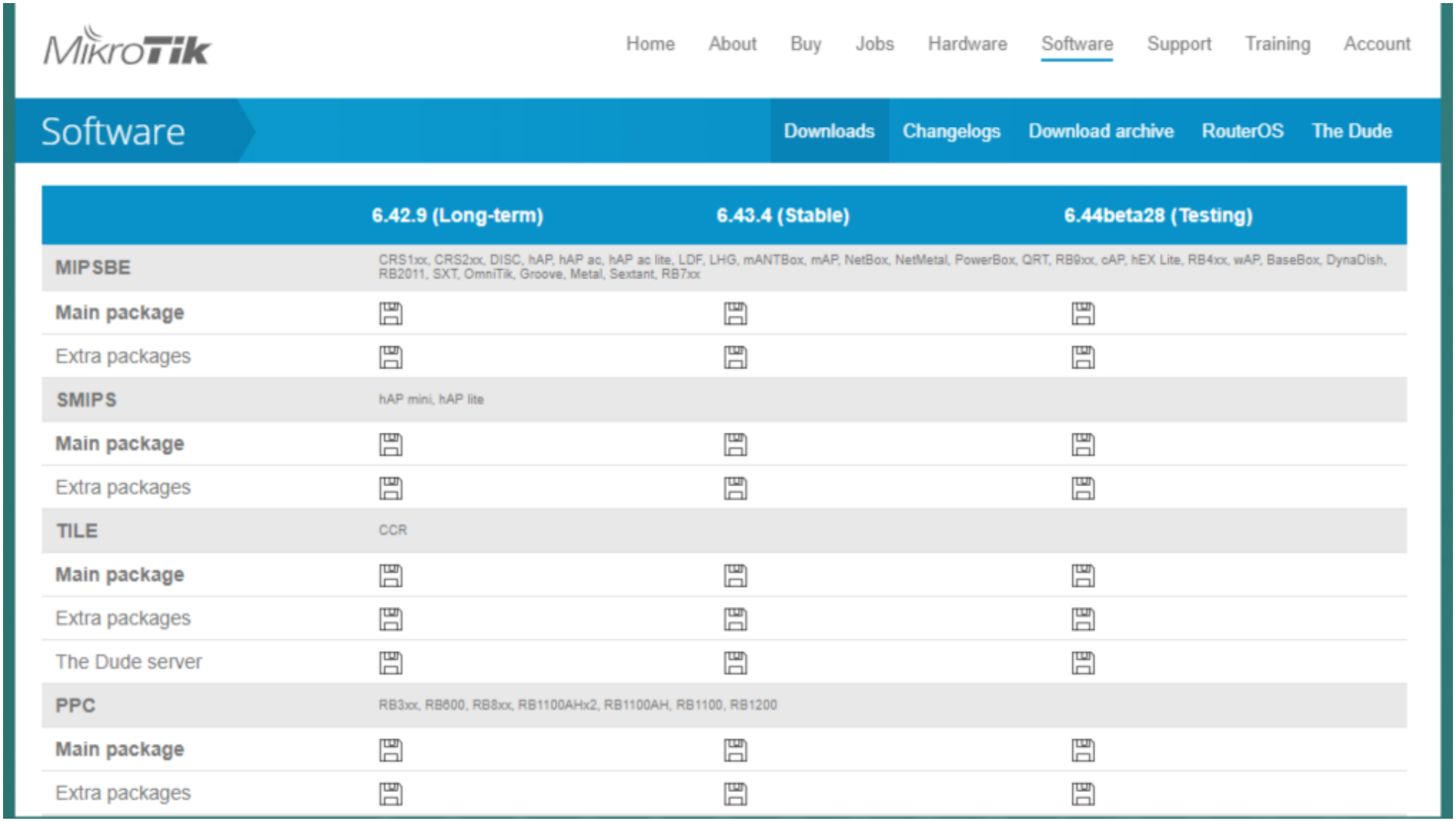
pronetworks

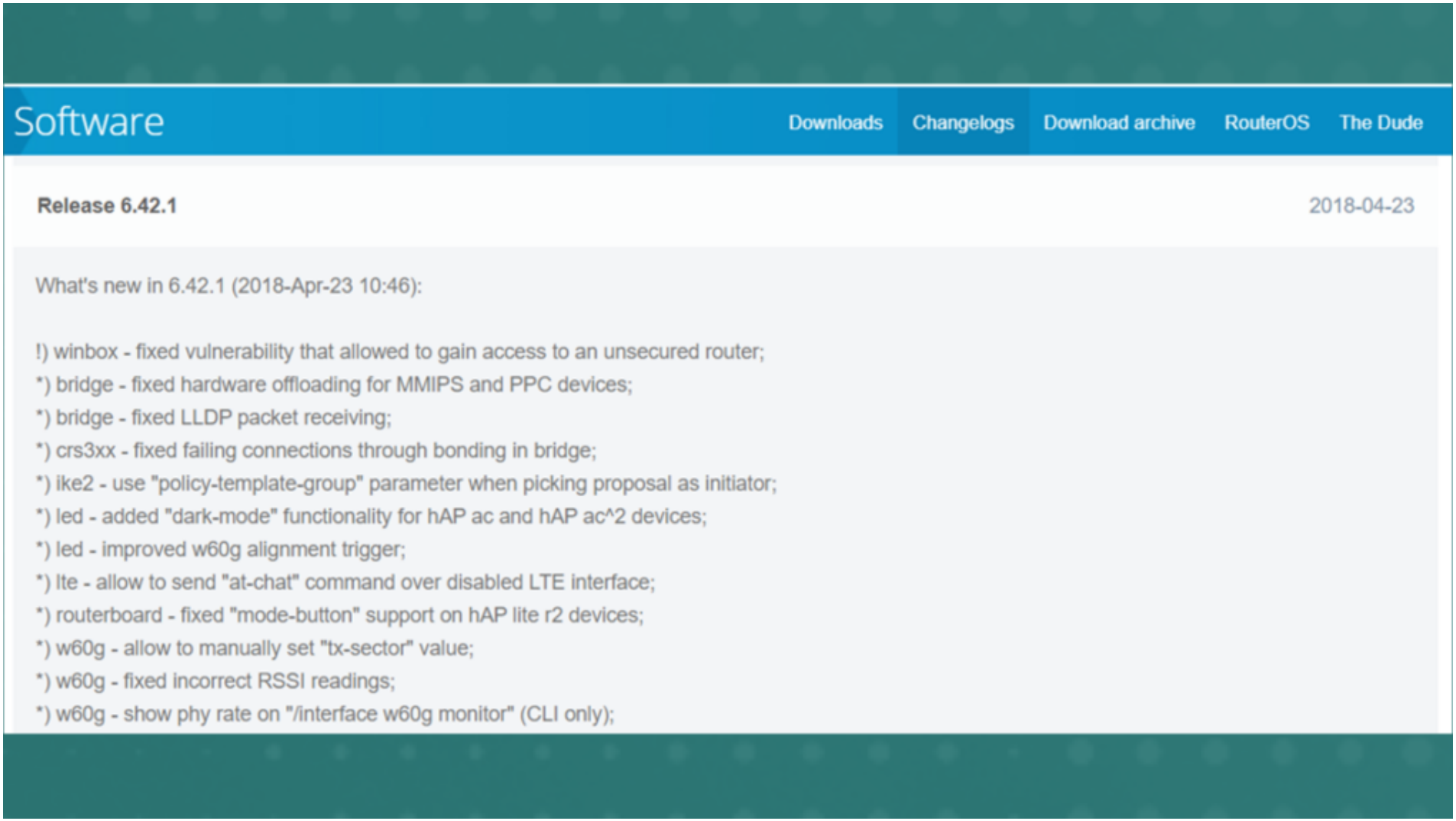

URGENT security reminder
+ Post Reply
Search this topic...
First unread post →
1
2
»
normis
MikroTik Support
MikroTik
Topic Author
Posts: 23524
Joined: Fri May 28, 2004 5:04 am
Location: Riga, Latvia
Tue Oct 09, 2018 3:48 am
#1
As alredy reported multiple times, in April 2018 MikroTik fixed a vulnerability in the Winbox server component, which allowed an attacker to gain access to your RouterOS device, if the Winbox port was opened to untrusted networks. Most MikroTik devices include a default firewall that prevents this, but for different reasons, the firewall is sometimes turned off by the user.
The issue was already fixed, but a new method of exploitation has recently been revealed, so we urge all MikroTik users to upgrade their RouterOS versions.
Note: THIS IS THE SAME ISSUE THAT WAS ALREADY FIXED IN APRIL. Only a new way to use the same vulnerability was revealed now.
More details here: https://blog.mikrotik.com/security/new- ... ility.html
Please share this link with colleagues, employees, customers and other MikroTik users.
No answer to your question? How to write posts

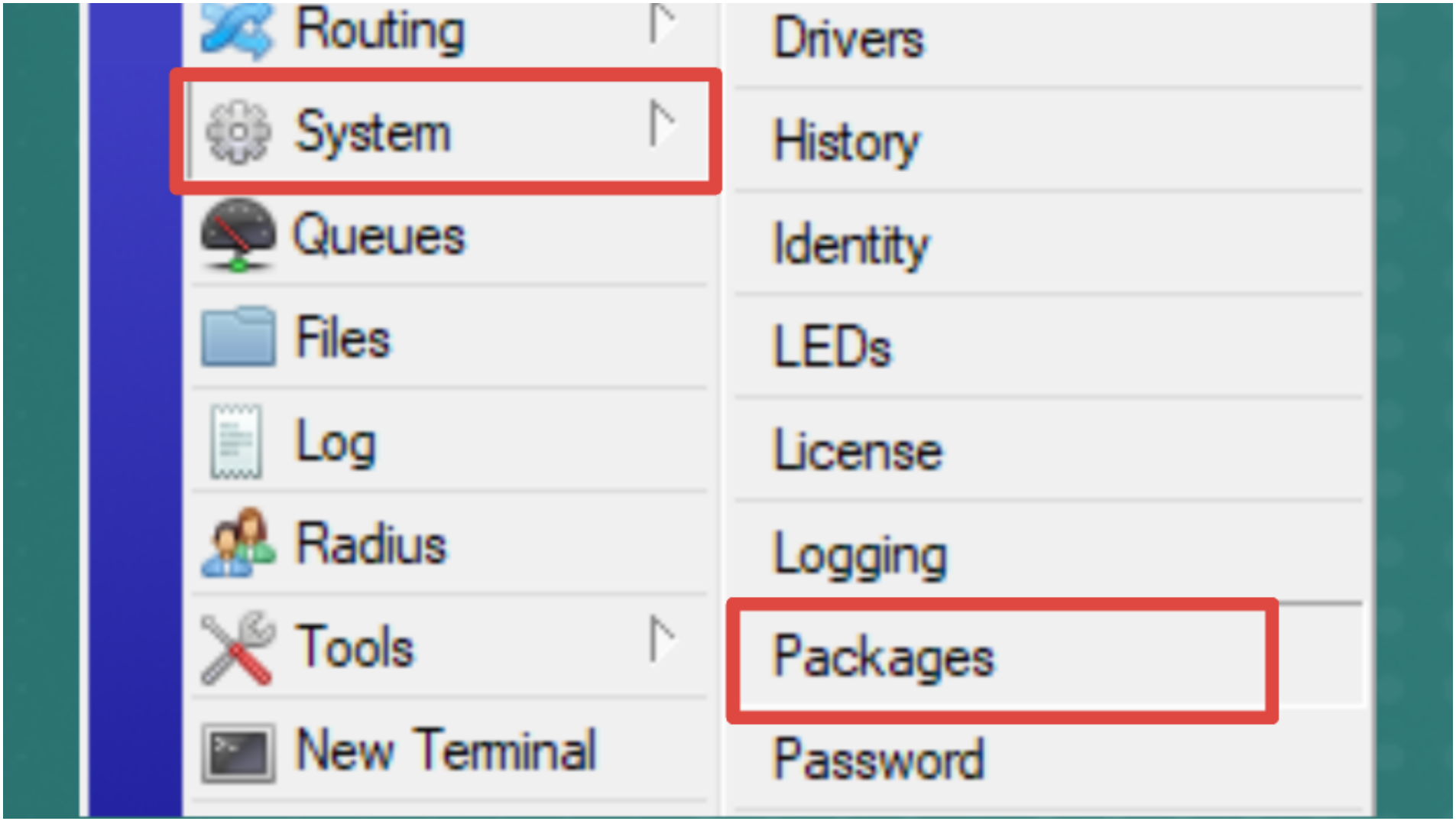
# NEW EXPLOIT FOR MIKROTIK ROUTER WINBOX VULNERABILITY

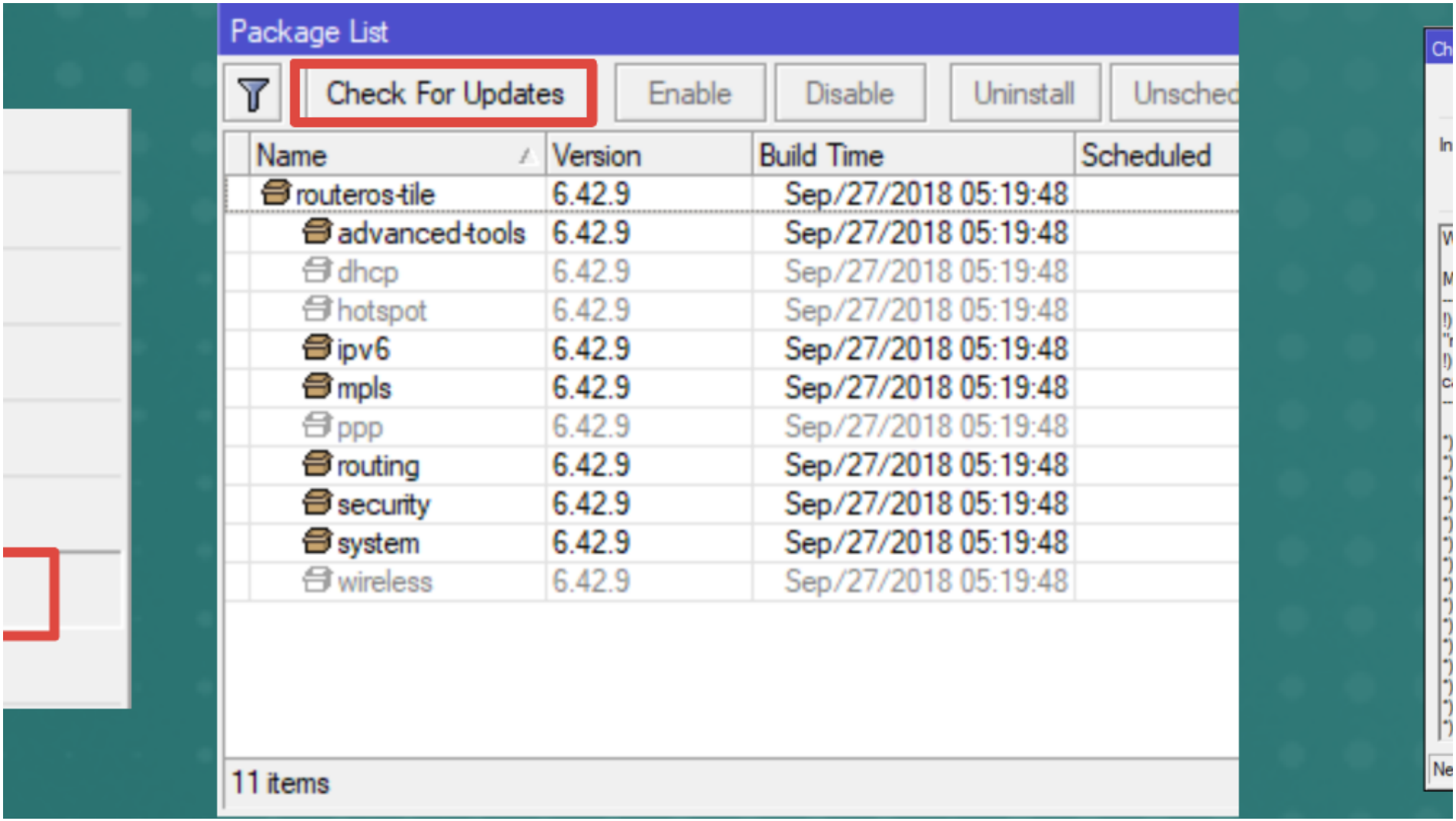
9th Oct, 2018 | Security

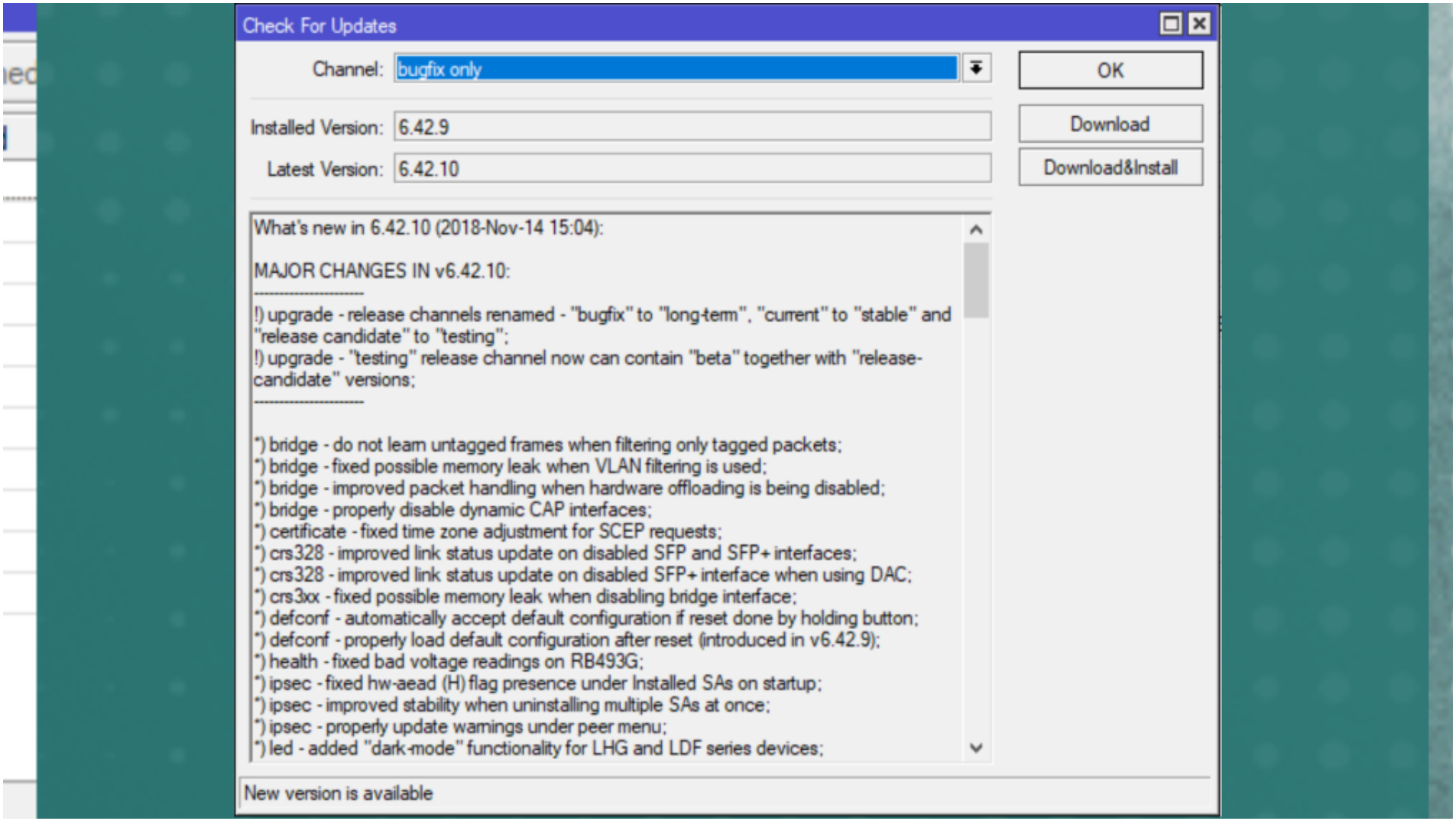
https://blog.mikrotik.com/security/new-exploit-for-mikrotik-router-winbox-vulnerability.html

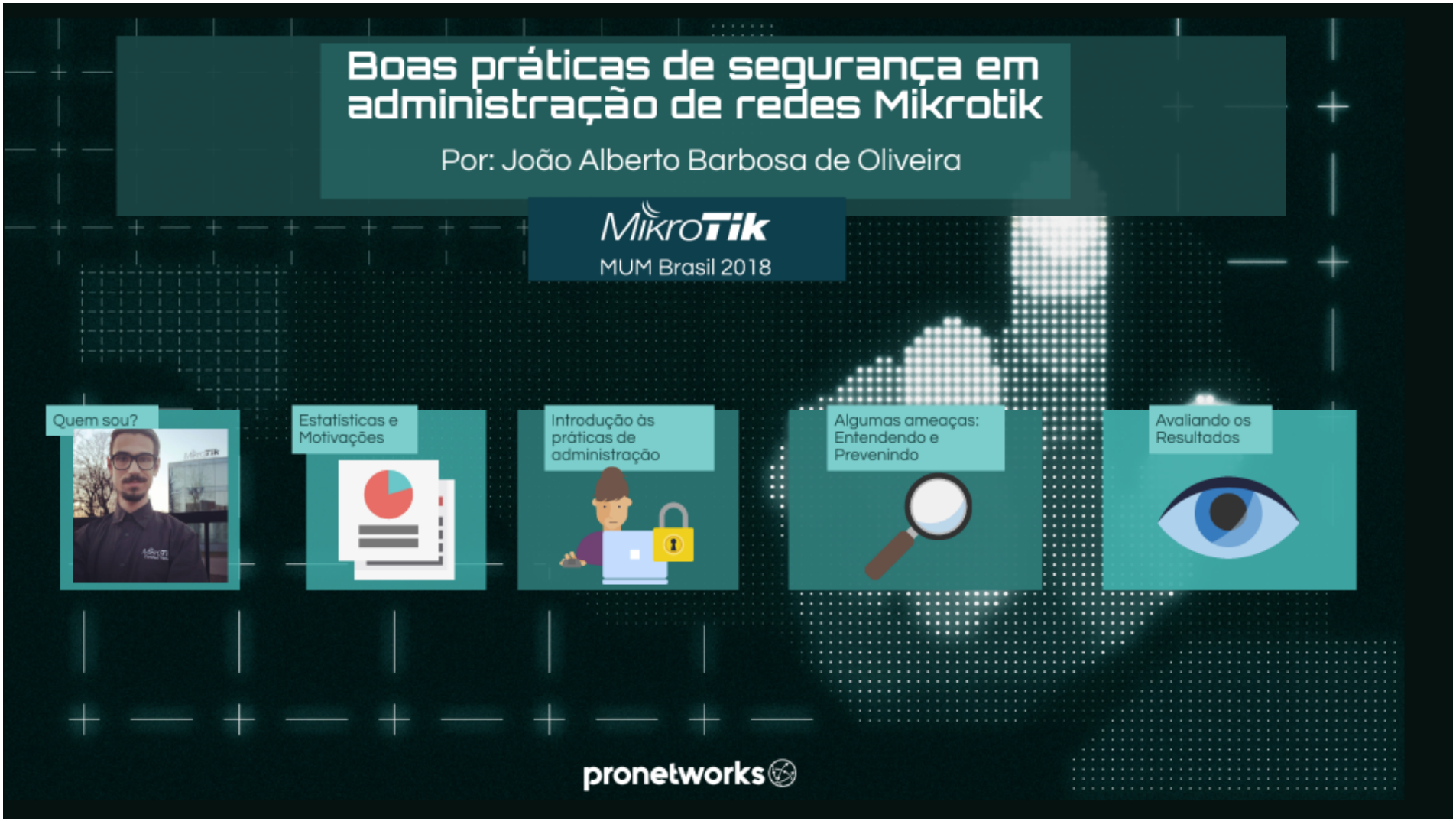

MikroTik
Home
About
Buy
Jobs
Hardware
Software
Support
Training
Account
Software
Downloads
Changelogs
Download archive
RouterOS
The Dude
6.42.9 (Long-term)
6.43.4 (Stable)
6.44beta28 (Testing)
MIPSBE
CRS1xx, CRS2xx, DISC, hAP, hAP ac, hAP ac lite, LDF, LHG, mANTBox, mAP, NetBox, NetMetal, PowerBox, QRT, RB9xx, cAP, hEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx
Main package
Extra packages
SMIPS
hAP mini, hAP lite
Main package
Extra packages
TILE
CCR
Main package
Extra packages
The Dude server
PPC
RB3xx, RB600, RB8xx, RB1100AHx2, RB1100AH, RB1100, RB1200
Main package
Extra packages


Software
Downloads
Changelogs
Download archive
RouterOS
The Dude
Release 6.42.1
2018-04-23
What's new in 6.42.1 (2018-Apr-23 10:46):
!) winbox - fixed vulnerability that allowed to gain access to an unsecured router;
*) bridge - fixed hardware offloading for MMIPS and PPC devices;
*) bridge - fixed LLDP packet receiving;
*) crs3xx - fixed failing connections through bonding in bridge;
*) ike2 - use "policy-template-group" parameter when picking proposal as initiator;
*) led - added "dark-mode" functionality for hAP ac and hAP ac^2 devices;
*) led - improved w60g alignment trigger;
*) lte - allow to send "at-chat" command over disabled LTE interface;
*) routerboard - fixed "mode-button" support on hAP lite r2 devices;
*) w60g - allow to manually set "tx-sector" value;
*) w60g - fixed incorrect RSSI readings;
*) w60g - show phy rate on "/interface w60g monitor" (CLI only);


Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Drivers
History
Identity
LEDs
License
Logging
Packages
Password


Package List
Check For Updates
Enable
Disable
Uninstall
Unsched
Name
Version
Build Time
Scheduled
routeros-tile 6.42.9 Sep/27/2018 05:19:48
advanced-tools 6.42.9 Sep/27/2018 05:19:48
dhcp 6.42.9 Sep/27/2018 05:19:48
hotspot 6.42.9 Sep/27/2018 05:19:48
ipv6 6.42.9 Sep/27/2018 05:19:48
mpls 6.42.9 Sep/27/2018 05:19:48
ppp 6.42.9 Sep/27/2018 05:19:48
routing 6.42.9 Sep/27/2018 05:19:48
security 6.42.9 Sep/27/2018 05:19:48
system 6.42.9 Sep/27/2018 05:19:48
wireless 6.42.9 Sep/27/2018 05:19:48
11 items

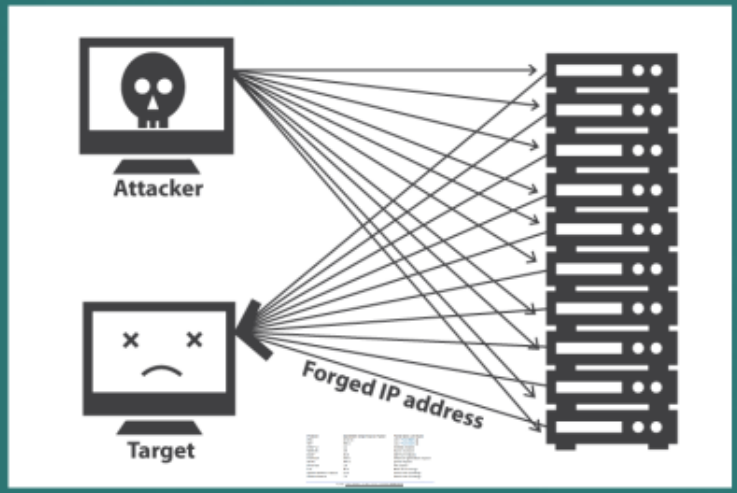

Check For Updates
Channel:
bugfix only
OK
Installed Version:
6.42.9
Download
Latest Version:
6.42.10
Download&Install
What's new in 6.42.10 (2018-Nov-14 15:04):
MAJOR CHANGES IN v6.42.10:
----------
!) upgrade - release channels renamed - "bugfix" to "long-term", "current" to "stable" and "release candidate" to "testing";
!) upgrade - "testing" release channel now can contain "beta" together with "release-candidate" versions;
----------
*) bridge - do not learn untagged frames when filtering only tagged packets;
*) bridge - fixed possible memory leak when VLAN filtering is used;
*) bridge - improved packet handling when hardware offloading is being disabled;
*) bridge - properly disable dynamic CAP interfaces;
*) certificate - fixed time zone adjustment for SCEP requests;
*) crs328 - improved link status update on disabled SFP and SFP+ interfaces;
*) crs328 - improved link status update on disabled SFP+ interface when using DAC;
*) crs3xx - fixed possible memory leak when disabling bridge interface;
*) defconf - automatically accept default configuration if reset done by holding button;
*) defconf - properly load default configuration after reset (introduced in v6.42.9);
*) health - fixed bad voltage readings on RB493G;
*) ipsec - fixed hw-aead (H) flag presence under Installed SAs on startup;
*) ipsec - improved stability when uninstalling multiple SAs at once;
*) ipsec - properly update warnings under peer menu;
*) led - added "dark-mode" functionality for LHG and LDF series devices;
New version is available

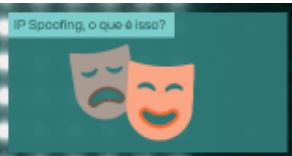

Boas práticas de segurança em administração de redes Mikrotik
Por: João Alberto Barbosa de Oliveira
MikroTik
MUM Brasil 2018
Quem sou?
Estatísticas e Motivações
Introdução às práticas de administração
Algumas ameaças: Entendendo e Prevenindo
Avaliando os Resultados
pronetworks

# Como funcionam os ataques de amplificação?

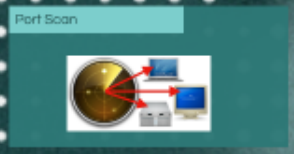
Serviços mal configurados proporcionam essa possibilidade, onde o ataque consiste em “forjar” a origem, apontando para a vítma;

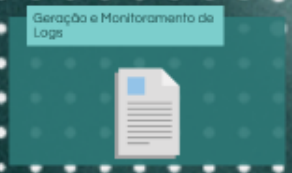
Exemplo de serviços utilizados: DNS, NTP e SNMP;



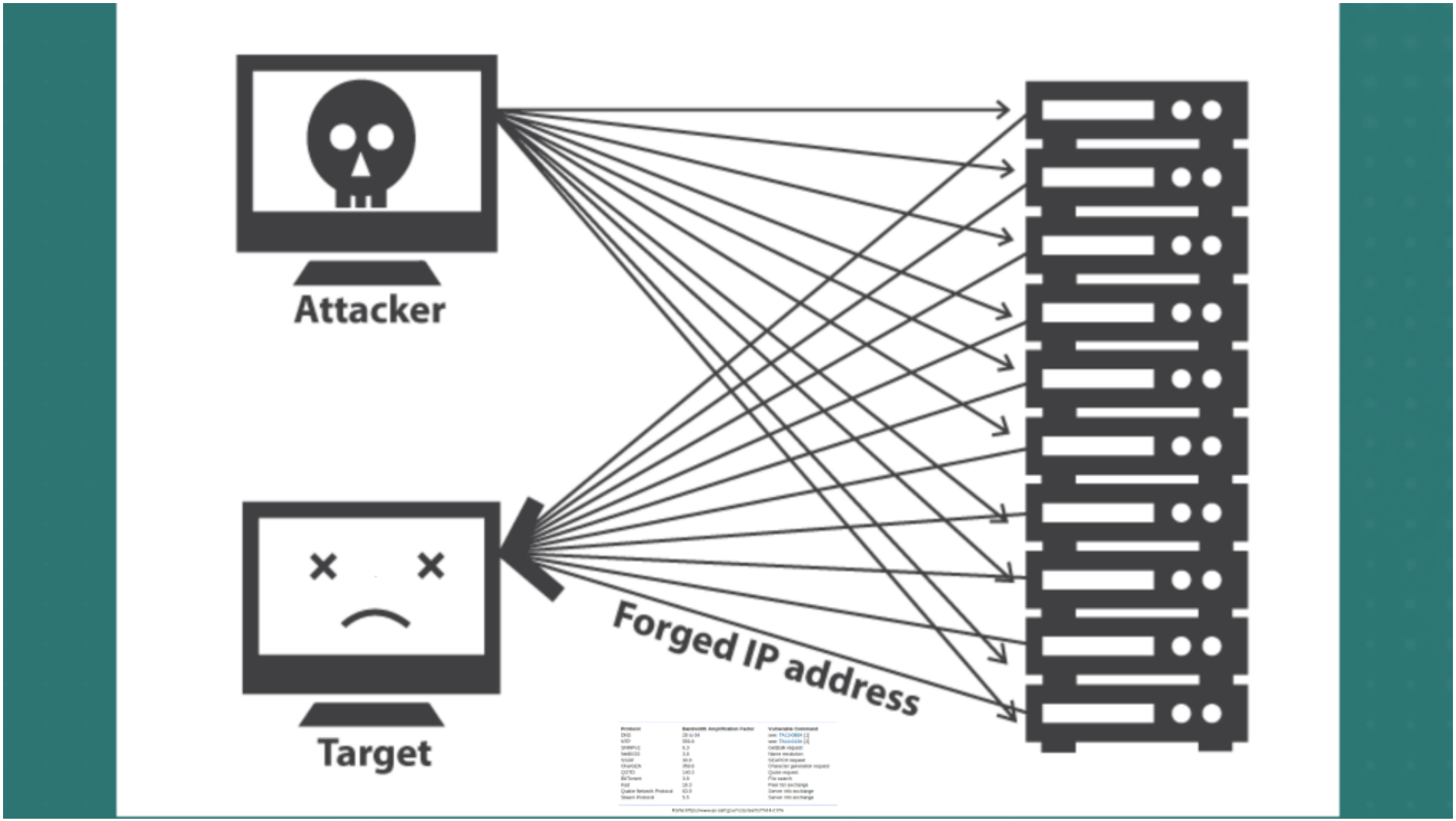






pronetworks


Attacker
Target
Forged IP address

Conceitos base:

DoS: Denial of Service

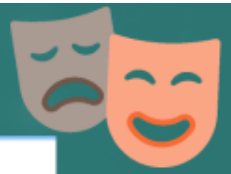
DDoS: Distributed Denial of Service

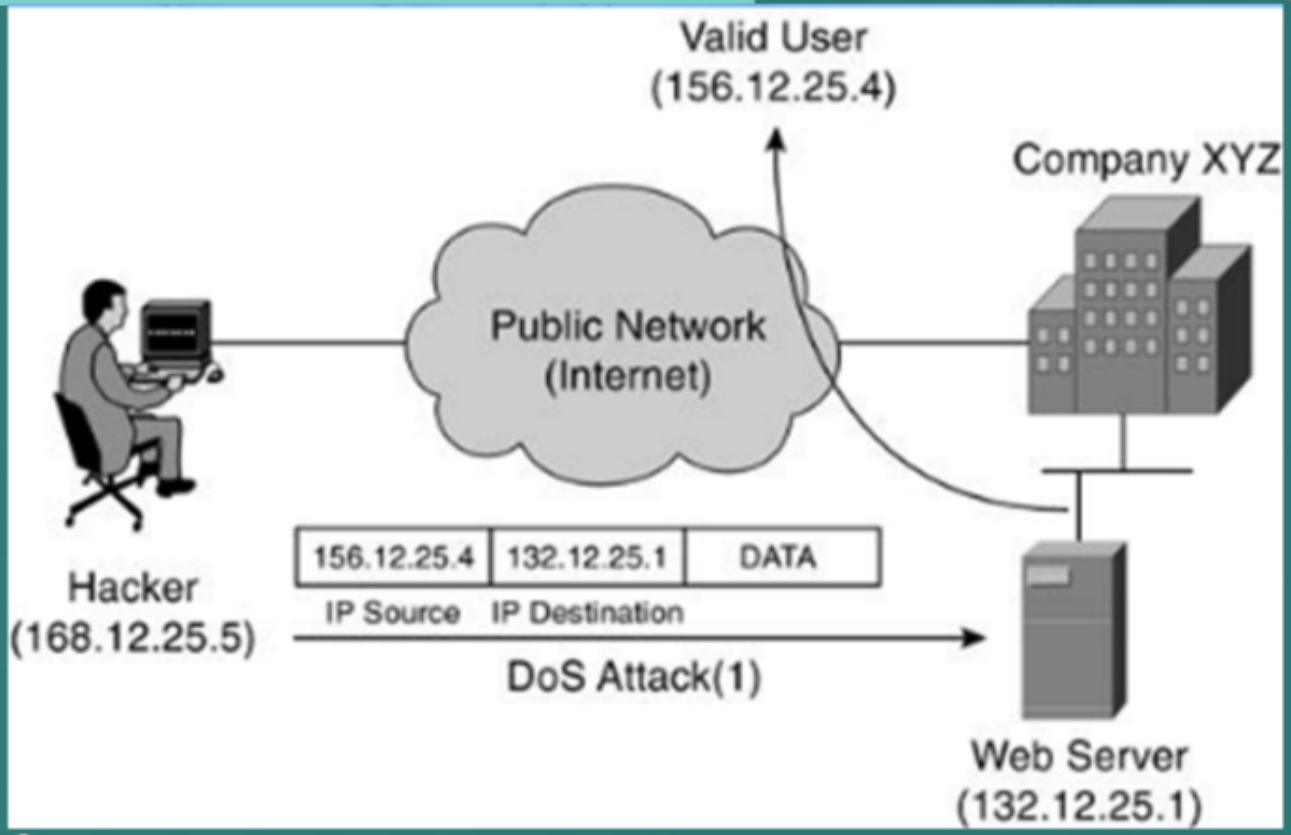
DRDoS: Distributed Reflection Denial of Service

| Protocol | Bandwidth Amplification Factor | Vulnerable Command |
|---|---|---|
| DNS | 28 to 54 | see: TA13-088A [1] |
| NTP | 556.9 | see: TA14-013A [2] |
| SNMPv2 | 6.3 | GetBulk request |
| NetBIOS | 3.8 | Name resolution |
| SSDP | 30.8 | SEARCH request |
| CharGEN | 358.8 | Character generation request |
| QOTD | 140.3 | Quote request |
| BitTorrent | 3.8 | File search |
| Kad | 16.3 | Peer list exchange |
| Quake Network Protocol | 63.9 | Server info exchange |
| Steam Protocol | 5.5 | Server info exchange |

Fonte: https://www.us-cert.gov/ncas/alerts/TA14-017A

# IP Spoofing, o que é isso?





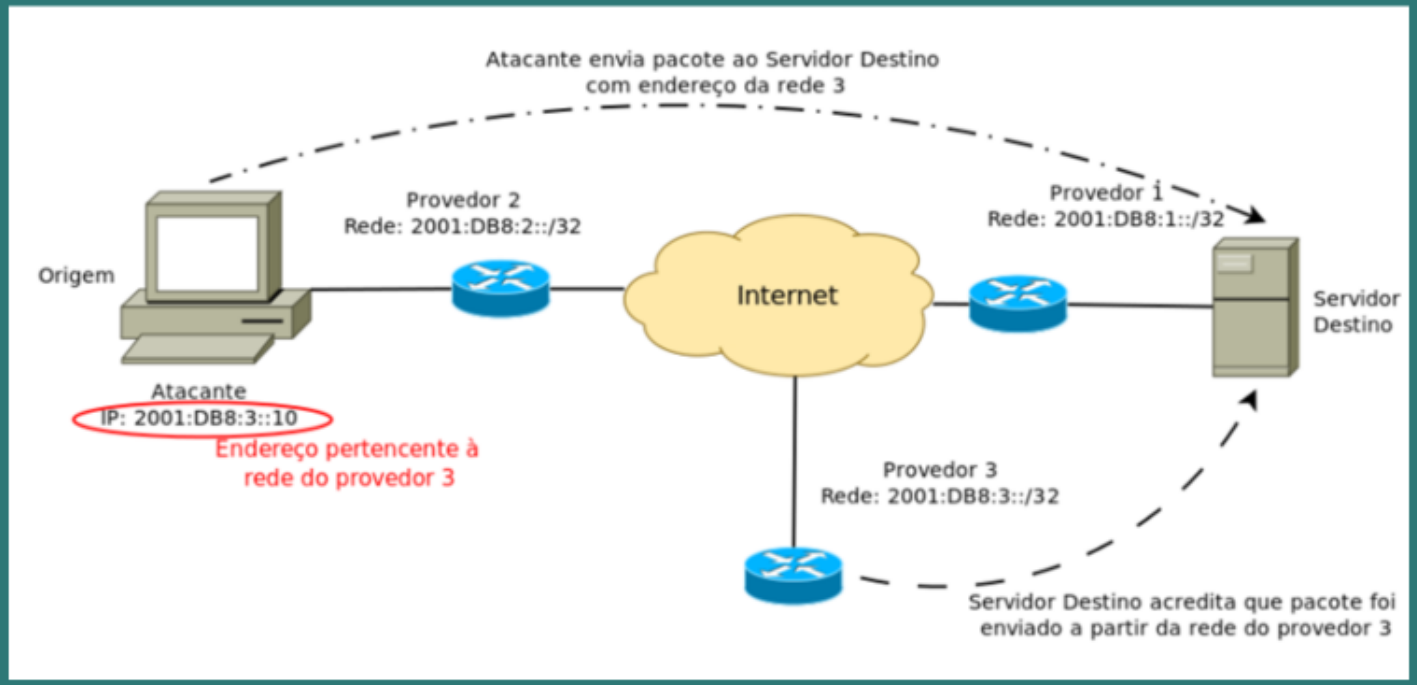

pronetworks

## Conceito: Antispoofing

- Descrito na BCP 84 e RFC 3704;
- Evita a origem de ataques de IP's forjados;
- Auxilia na prevenção de ataques na internet.

pronetworks

# Conceito: Antispoofing




fonte:http://bcp.nic.br/wp-content/uploads/2012/12/spoofing3.png

pronetworks

# Quais IPs são forjados?

- IP's de uso privado, especial ou reservado (bogons RFC 1918, RFC 5735, e RFC 6598);
- IP's de sua rede;
- Exemplos:

```
0.0.0.0/8
10.0.0.0/8
100.64.0.0/10
127.0.0.0/8
169.254.0.0/16
172.16.0.0/12
192.0.0.0/24
192.0.2.0/24
192.168.0.0/16
198.18.0.0/15
198.51.100.0/24
203.0.113.0/24
224.0.0.0/3
```

## IPv6 address types (www.iana.org)

| | |
|---|---|
| 2000::/3 through 3fff::/3 | Global Unicast |
| fc00::/7 through fdff::/7 | Unique local unicast |
| fe80::/10 through febf::/10 | Link local unicast |
| ff00::/8 through ffff::/8 | multicast |

pronetworks

# Conceito: Filtro Antispoofing

- Filtragem permitindo pacotes originados apenas nas redes de origens;
- Filtro RFP (Reverse Path Forwarding);
- Política de Blackhole;

pronetworks

# Exemplos para Mikrotik

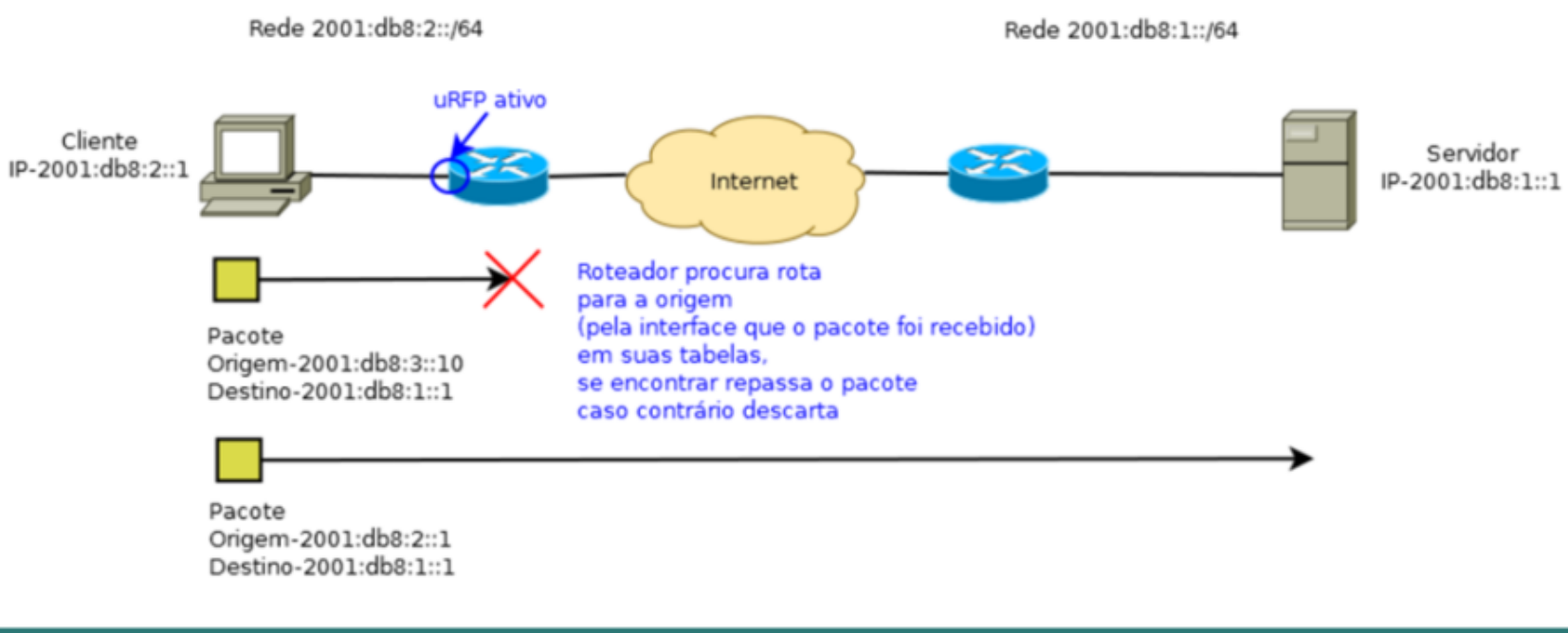
## Configuração para IPv6

```
ipv6 address
# Endereco da interface do roteador.
# Troque este endereço pelo que é usado em sua rede!
add address=2001:db8:cafe:faca::1/64 advertise=no interface=ether1
…
/ipv6 firewall address-list
# Permite o IP alocado para o CPE do cliente
# Troque este endereço pelo que é usado em sua rede!
add address=2001:DB8:CAFE:FACA::2/64 list=FILTRO-CLIENTE-V6
# Permite o range de IPs alocados para o seu cliente
# Troque este endereço pelo que é usado em sua rede!
add address=2001:DB8:CAFE::/48 list=FILTRO-CLIENTE-V6
/ipv6 firewall filter
add chain=forward in-interface=ether1 src-address-list=FILTRO-CLIENTE-V6
add action=drop chain=forward in-interface=ether1
```

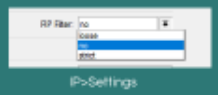
Mais em:
https://bcp.nic.br/antispoofing

pronetworks

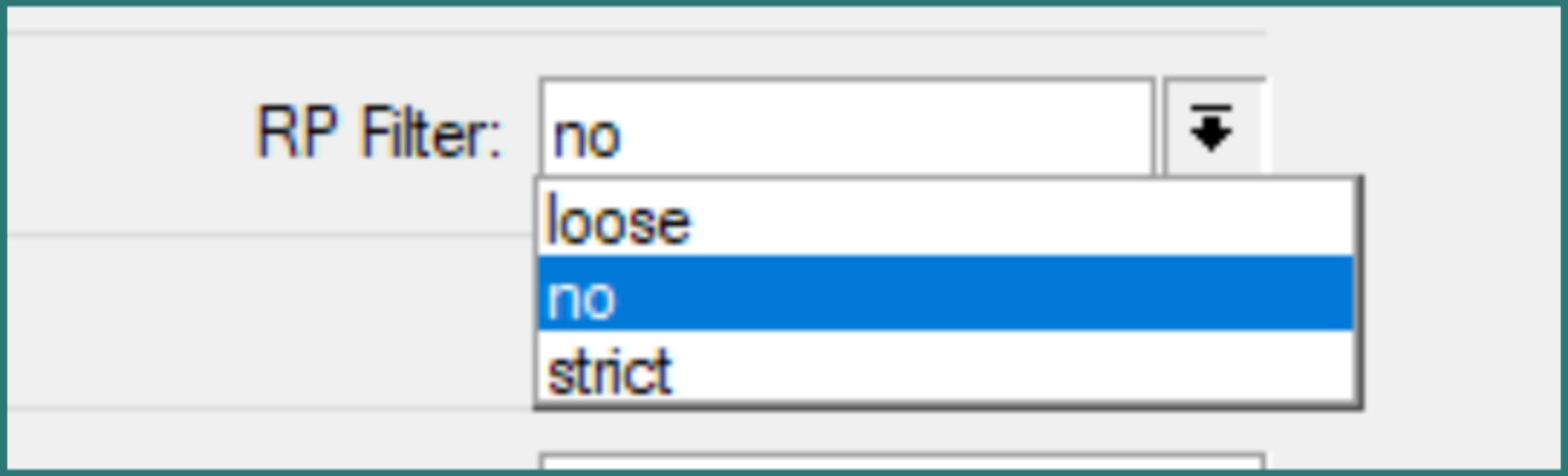
# Exemplo: (uRFP)




Fonte:http://bcp.nic.br/wp-content/uploads/2012/12/rpf.png



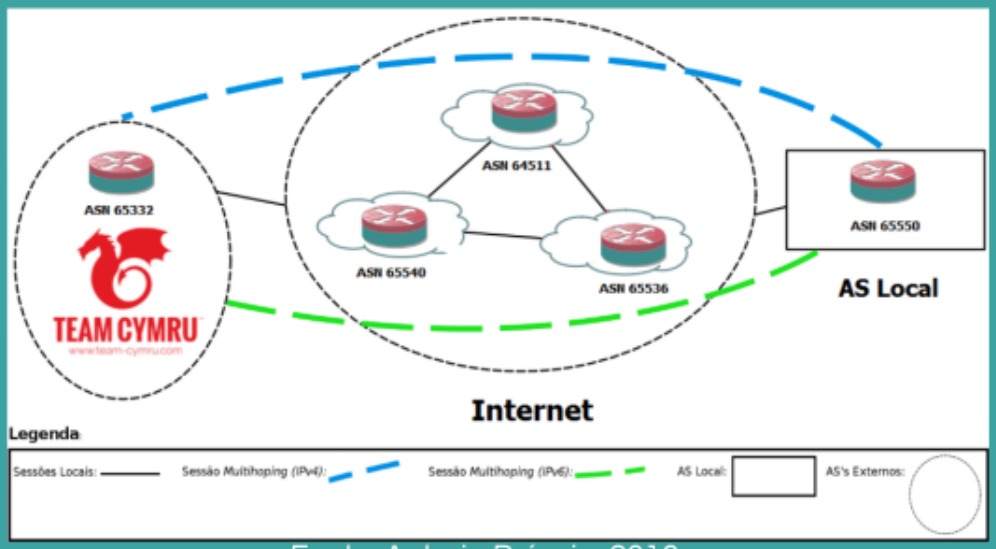
pronetworks




IP>Settings

# Team CYMRU

- Oferece alguns serviços, dentre eles um Peering para envio de prefixos Bogons via BGP.

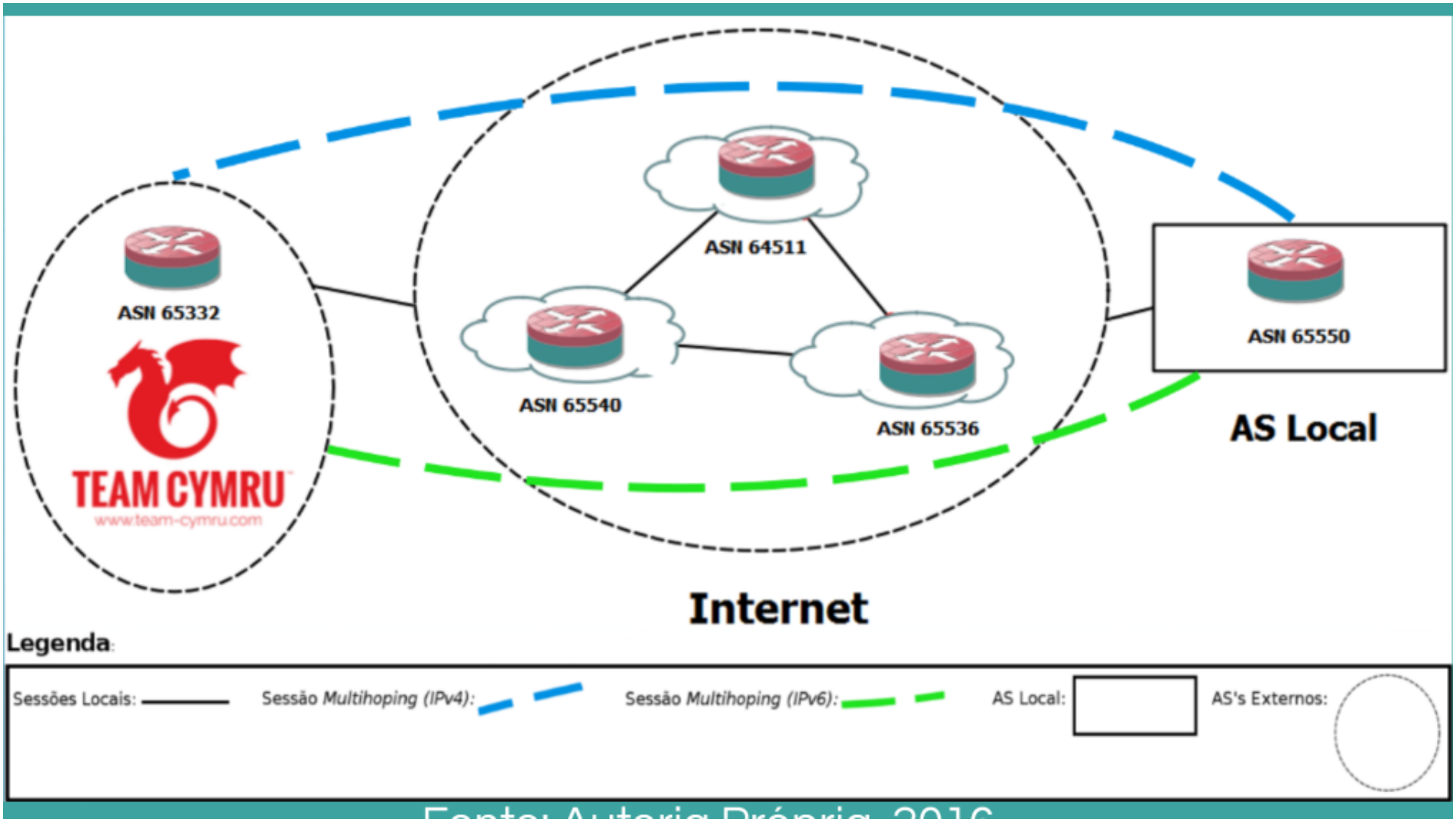



Fonte: Autoria Própria, 2016

Mais detalhes

TEAM CYMRU

pronetworks




Fonte: Autoria Própria, 2016

## Mais detalhes


- Site oficial
  https://www.team-cymru.com

- "Boas práticas em roteamento de borda para novos sistemas autônomos provedores de acesso
  by João Alberto Barbosa de Oliveira"

  https://mum.mikrotik.com/2017/BR/agenda#0DMjN0O2g9

- Revista Mirante V. 11, N. 6 (2018) pág. 44-57.
  http://www.revista.ueg.br/index.php/mirante/issue/view/410

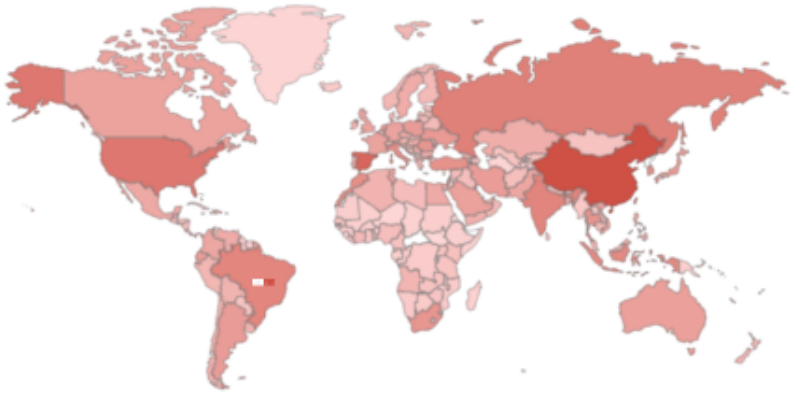
pronetworks

# Prevenindo abusos de serviços

- Serviços como DNS, SNMP, e NTP, facilmente podem ser abusados por terceiros;
- Alguns serviços servem para o chamado “amplificação de ataques”, utilizado em ataques do tipo DoS/DDoS/DRDoS;



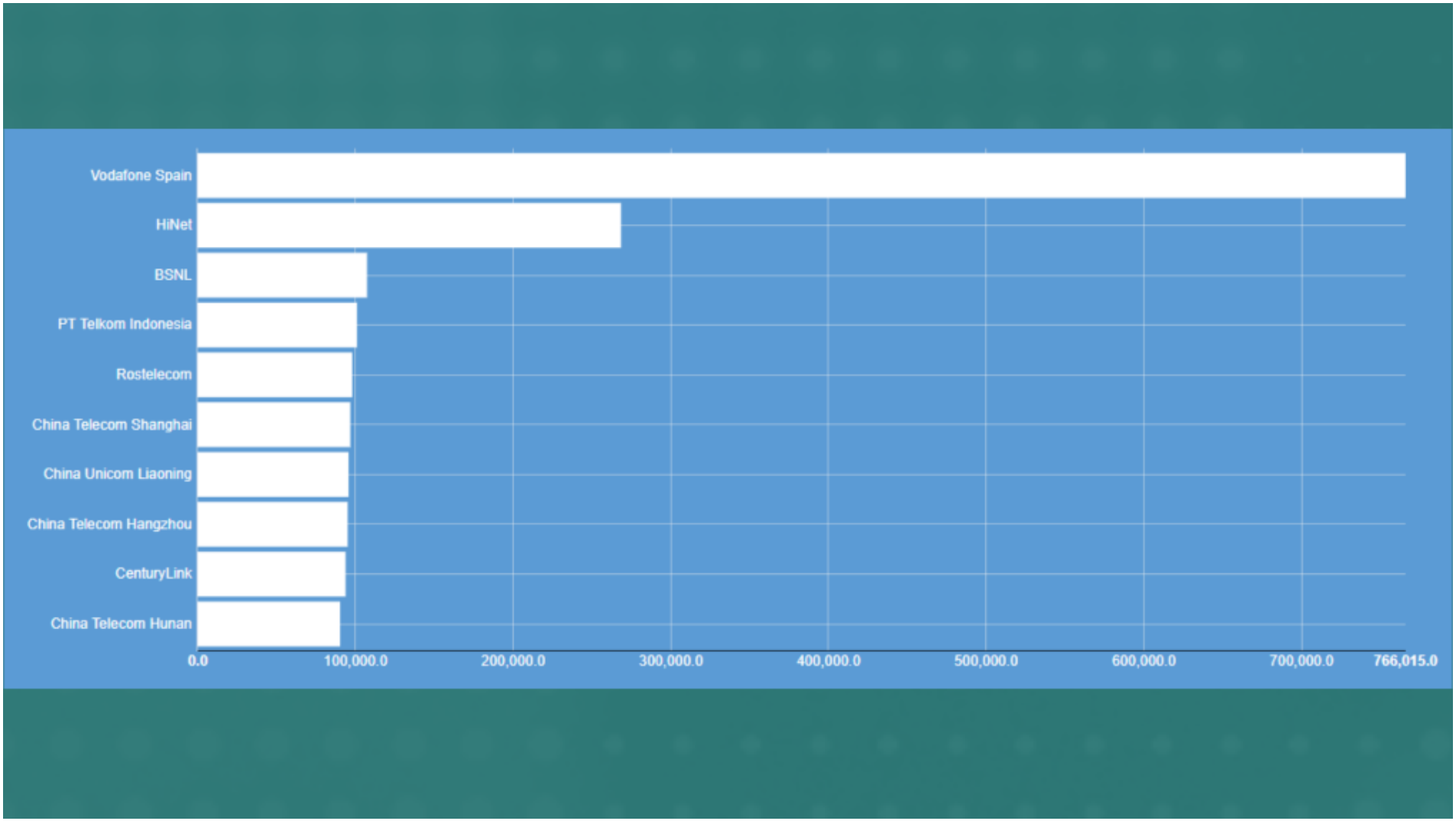

pronetworks



## Top Countries

| | |
|---|---|
| 1. China | 1,830,183 |
| 2. Spain | 812,738 |
| 3. United States | 386,451 |
| 4. Taiwan | 283,736 |
| 5. Russian Federation | 241,515 |
| 6. India | 195,373 |
| 7. Brazil | 188,310 |
| 8. Indonesia | 139,239 |
| 9. Italy | 118,202 |
| 10. Morocco | 105,825 |

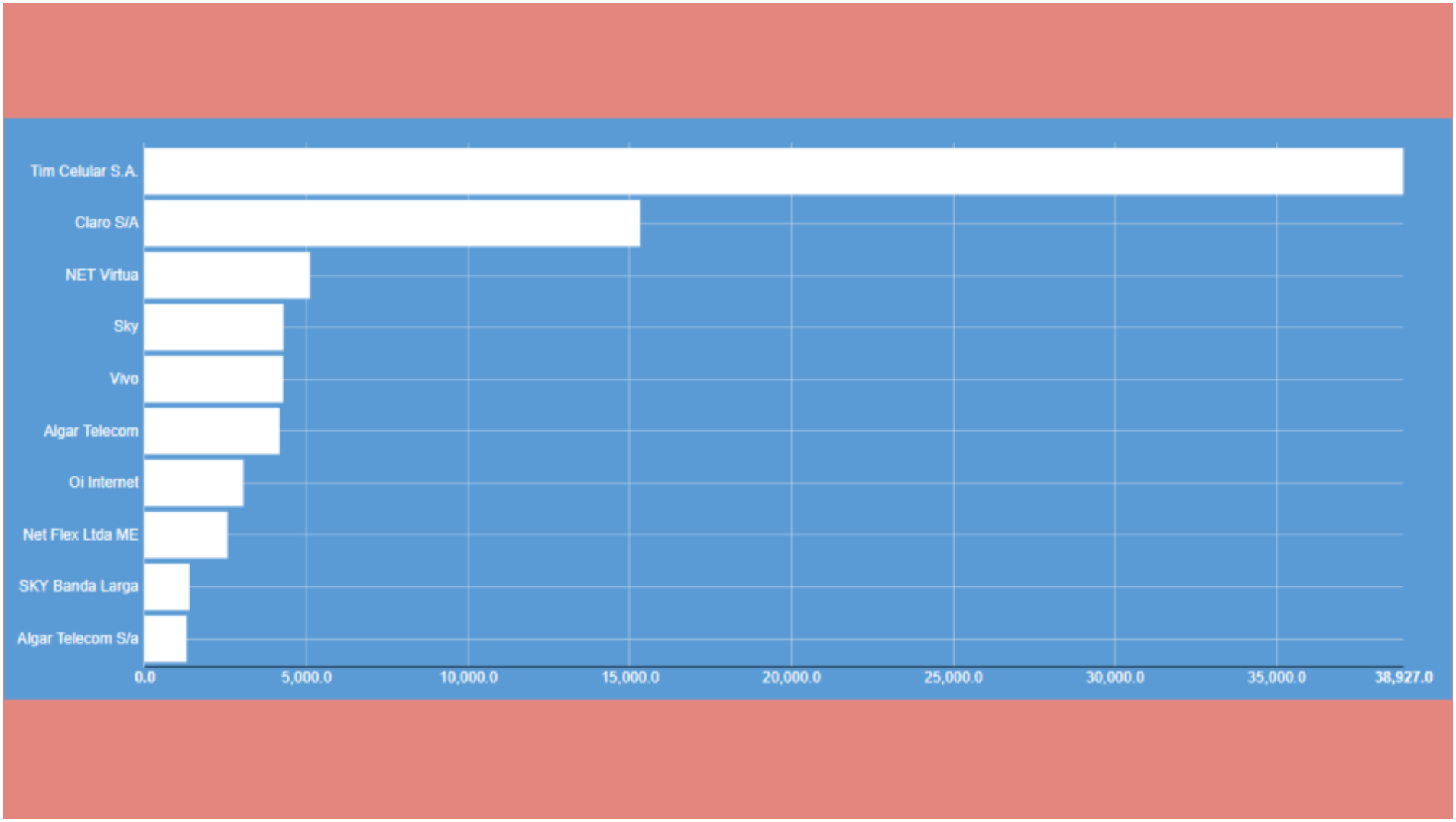
Search for port:53 recursion enabled returned 5,788,167 results on 11-11-2018


Vodafone Spain
HiNet
BSNL
PT Telkom Indonesia
Rostelecom
China Telecom Shanghai
China Unicom Liaoning
China Telecom Hangzhou
CenturyLink
China Telecom Hunan
0.0
100,000.0
200,000.0
300,000.0
400,000.0
500,000.0
600,000.0
700,000.0
766,015.0

## Top Cities

| | |
|---|---|
| 1. Sao Paulo | 19,832 |
| 2. Rio De Janeiro | 11,849 |
| 3. Campinas | 4,693 |
| 4. Recife | 3,549 |
| 5. Brasilia | 2,694 |
| 6. Belo Horizonte | 2,341 |
| 7. Duque De Caxias | 2,112 |
| 8. Fortaleza | 2,035 |
| 9. Salvador | 1,977 |
| 10. Curitiba | 1,811 |

Search for port:"53" recursion enabled country:"BR" returned 188,307 results on 11-11-2018


Tim Celular S.A.
Claro S/A
NET Virtua
Sky
Vivo
Algar Telecom
Oi Internet
Net Flex Ltda ME
SKY Banda Larga
Algar Telecom S/a
0.0
5,000.0
10,000.0
15,000.0
20,000.0
25,000.0
30,000.0
35,000.0
38,927.0

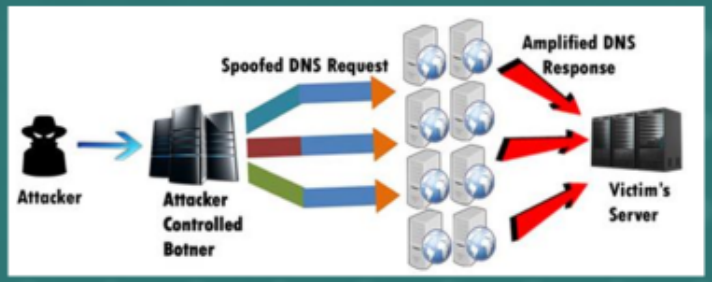
# Prevenindo abusos de serviços: DNS

OBJETIVO: Evitar ataques de amplificação de DNS, através de consultas externas não autorizadas.

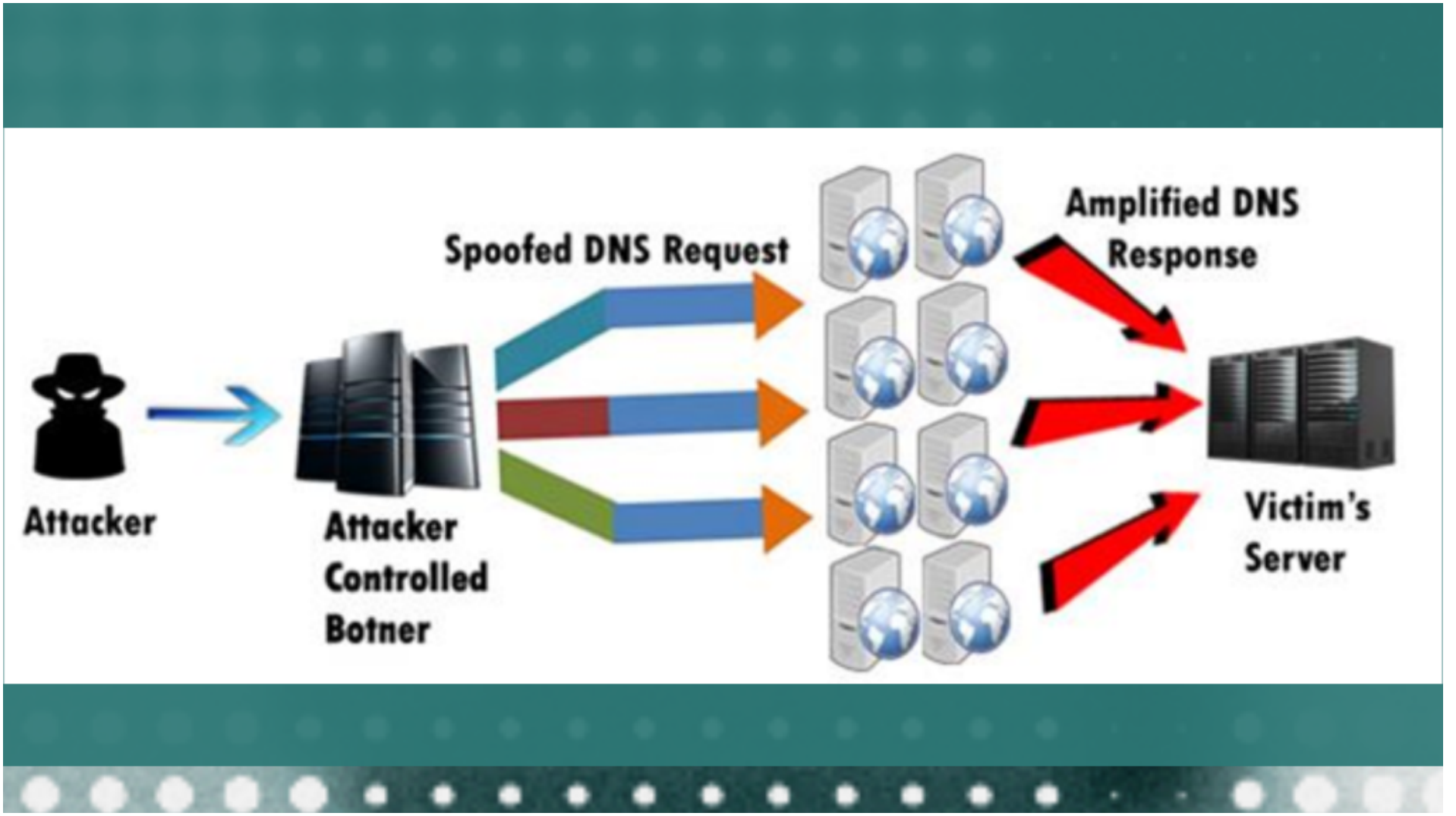
Basicamente temos 2 formas de evitar abuso nesse serviço:

1 - Desabilitando a opção “allow remote requests”;

2 - Controle em Firewall:




pronetworks

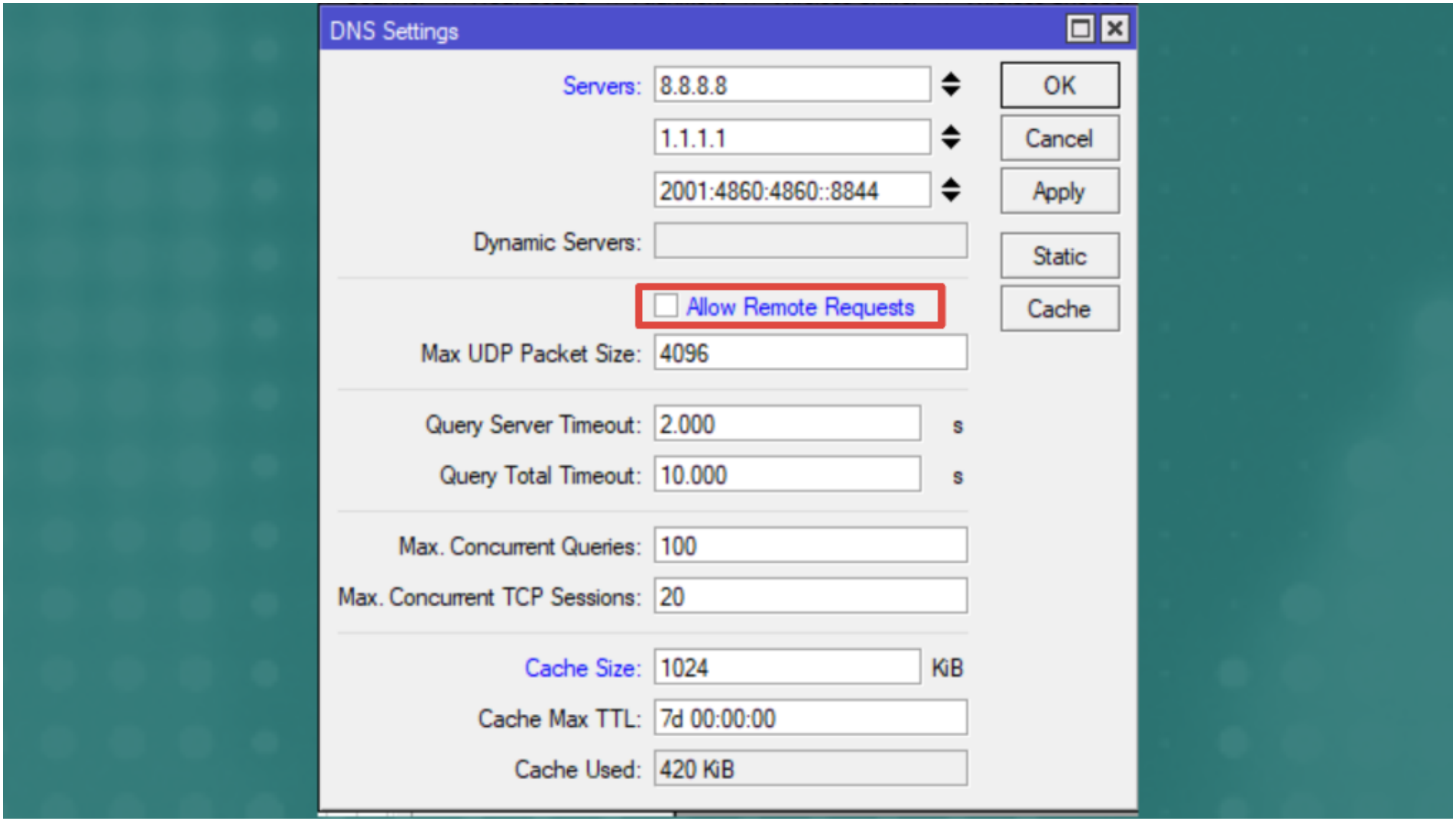

Spoofed DNS Request
Amplified DNS Response
Attacker
Attacker Controlled Botner
Victim's Server

Analisando o problema com a ferramenta "torch"

| Eth. ... | Protocol | Src. | Dst. | VLAN Id | DSCP | Tx Rate | Rx Rate | Tx Pack... | Rx Pack... |
|---|---|---|---|---|---|---|---|---|---|
| 800 (ip) | 17 (udp) | 87.67.138.3:2607 | 177.10.232.222:53 (dns) | | | 641.9 kbps | 124.8 k | 53 | 195 |
| 800 (ip) | 17 (udp) | 45.60.15.39:65186 | 177.10.232.222:53 (dns) | | | 24.2 kbps | 960 bps | 2 | 2 |
| 800 (ip) | 17 (udp) | 45.60.15.39:35979 | 177.10.232.222:53 (dns) | | | 24.2 kbps | 960 bps | 2 | 2 |
| 800 (ip) | 17 (udp) | 45.60.15.39:19387 | 177.10.232.222:53 (dns) | | | 24.2 kbps | 960 bps | 2 | 2 |
| 800 (ip) | 17 (udp) | 45.60.15.39:39835 | 177.10.232.222:53 (dns) | | | 12.1 kbps | 480 bps | 1 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:47494 | 177.10.232.222:53 (dns) | | | 12.1 kbps | 480 bps | 1 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:3401 | 177.10.232.222:53 (dns) | | | 12.1 kbps | 480 bps | 1 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:59848 | 177.10.232.222:53 (dns) | | | 12.1 kbps | 480 bps | 1 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:64228 | 177.10.232.222:53 (dns) | | | 12.1 kbps | 480 bps | 1 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:26303 | 177.10.232.222:53 (dns) | | | 12.1 kbps | 480 bps | 1 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:37318 | 177.10.232.222:53 (dns) | | | 0 bps | 1440 bps | 0 | 3 |
| 800 (ip) | 17 (udp) | 45.60.15.39:48243 | 177.10.232.222:53 (dns) | | | 0 bps | 480 bps | 0 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:13189 | 177.10.232.222:53 (dns) | | | 0 bps | 480 bps | 0 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:45764 | 177.10.232.222:53 (dns) | | | 0 bps | 480 bps | 0 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:44089 | 177.10.232.222:53 (dns) | | | 0 bps | 480 bps | 0 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:29357 | 177.10.232.222:53 (dns) | | | 0 bps | 480 bps | 0 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:31294 | 177.10.232.222:53 (dns) | | | 0 bps | 480 bps | 0 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:40641 | 177.10.232.222:53 (dns) | | | 0 bps | 480 bps | 0 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:53042 | 177.10.232.222:53 (dns) | | | 0 bps | 480 bps | 0 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:11747 | 177.10.232.222:53 (dns) | | | 0 bps | 480 bps | 0 | 1 |
| 800 (ip) | 17 (udp) | 45.60.15.39:54582 | 177.10.232.222:53 (dns) | | | 0 bps | 0 bps | 0 | 0 |
| 800 (ip) | 17 (udp) | 45.60.15.39:6254 | 177.10.232.222:53 (dns) | | | 0 bps | 0 bps | 0 | 0 |
| 800 (ip) | 17 (udp) | 45.60.15.39:8060 | 177.10.232.222:53 (dns) | | | 0 bps | 0 bps | 0 | 0 |
| 800 (ip) | 17 (udp) | 45.60.15.39:20689 | 177.10.232.222:53 (dns) | | | 0 bps | 0 bps | 0 | 0 |

70 items | Total Tx: 787.2 kbps | Total Rx: 136.3 kbps | Total Tx Packet: 65

Fonte: Autoria própria, 2018


DNS Settings
Servers: 8.8.8.8
1.1.1.1
2001:4860:4860::8844
Dynamic Servers:
Allow Remote Requests
Max UDP Packet Size: 4096
Query Server Timeout: 2.000 s
Query Total Timeout: 10.000 s
Max. Concurrent Queries: 100
Max. Concurrent TCP Sessions: 20
Cache Size: 1024 KiB
Cache Max TTL: 7d 00:00:00
Cache Used: 420 KiB
OK
Cancel
Apply
Static
Cache

# Simples Exemplo de controle em Firewall:

| # | | Action | Chain | Src. Address | Dst. Address | Protocol | Src. Port | Dst. Port | In. Interface | Out. Int... | Bytes | Packets |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ;;; DROP - DNS Request - WAN - UDP | | | | | | | | | | | | |
| 8 | | drop | input | | | 17 (udp) | | 53 | pppoe-joao | | 6.4 KiB | 106 |
| ;;; DROP - DNS Request - WAN - TCP | | | | | | | | | | | | |
| 9 | | drop | input | | | 6 (tcp) | | 53 | pppoe-joao | | 1340 B | 29 |

# Prevenindo Abusos: NTP

- Use apenas este serviço quando for necessário!
- ACLs podem ser construídas com base em suas características (UDP, 123)
- Garanta a consulta apenas de origens desejadas!

Exemplo:

```
/ip firewall address-list
add ! address=! 10.0.54.0/8 list=minha_rede
add ! address=! 192.168.0.0/21 list=minha_rede

/ip firewall filter
add ! action=drop chain=input comment="DESCARTA  NTP External" dst-port=123 protocol=udp src-address-list=minha_rede
```

pronetworks

# ta apenas de orige

Exemplo:

```
/ip firewall address-list
add address=100.64.0.0/19 list=minha-rede
add address=192.168.0.0/21 list=minha-rede

/ip firewall filter
add action=drop chain=input comment="DESCARTA - NTP Externo" dst-port=123 protocol=udp src-address-list=!minha-rede
```

## Prevenindo abusos - SNMP

JAMAIS use configurações padrões do SNMP!

Ex: comunidade publica v.1

É possível tratar as consultas via Firewall

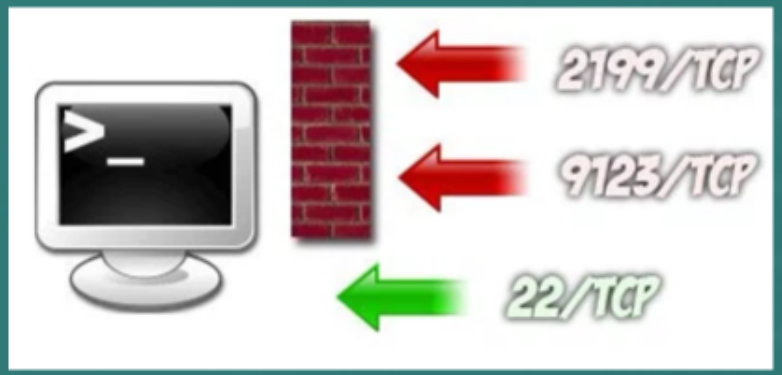
Ex: Caso queira ter um controle maior diante ativos fora de seu domínio

pronetworks

# Protegendo serviços com "Port Knocking"

Como fazer? P
Knocking

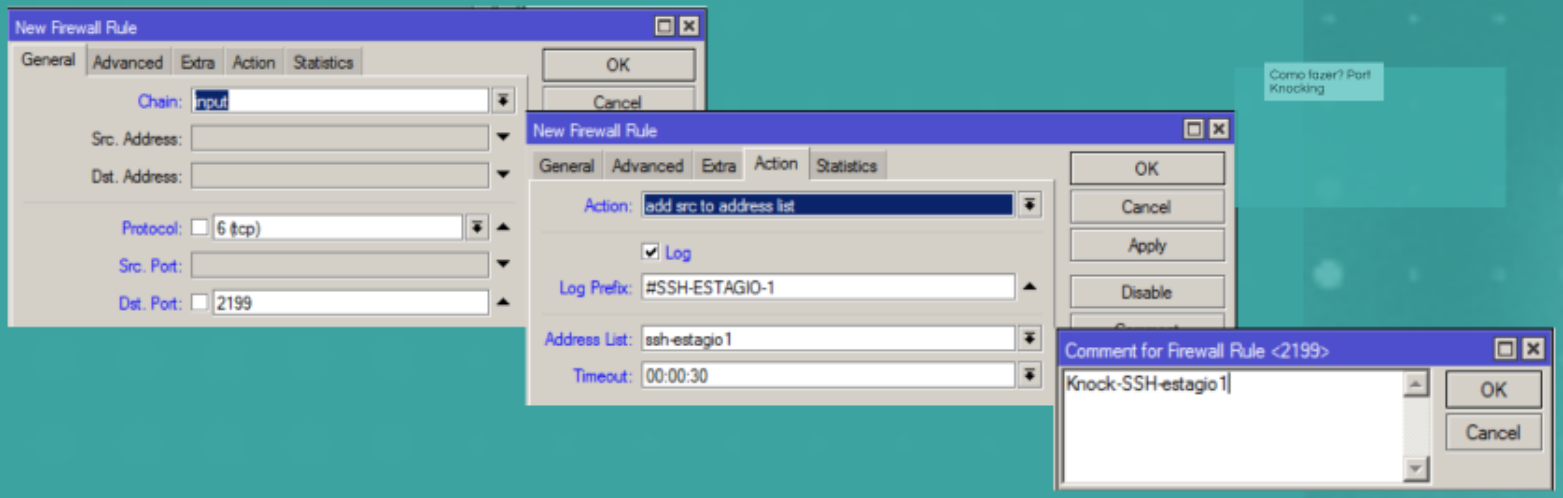
- Técnica muito útil em prover segurança;
- A Lógica é basicamente criar 1,2 ou mais estágios para se obter acesso a algum recurso;




pronetworks

# Como fazer? Port Knocking

## Regra #1:

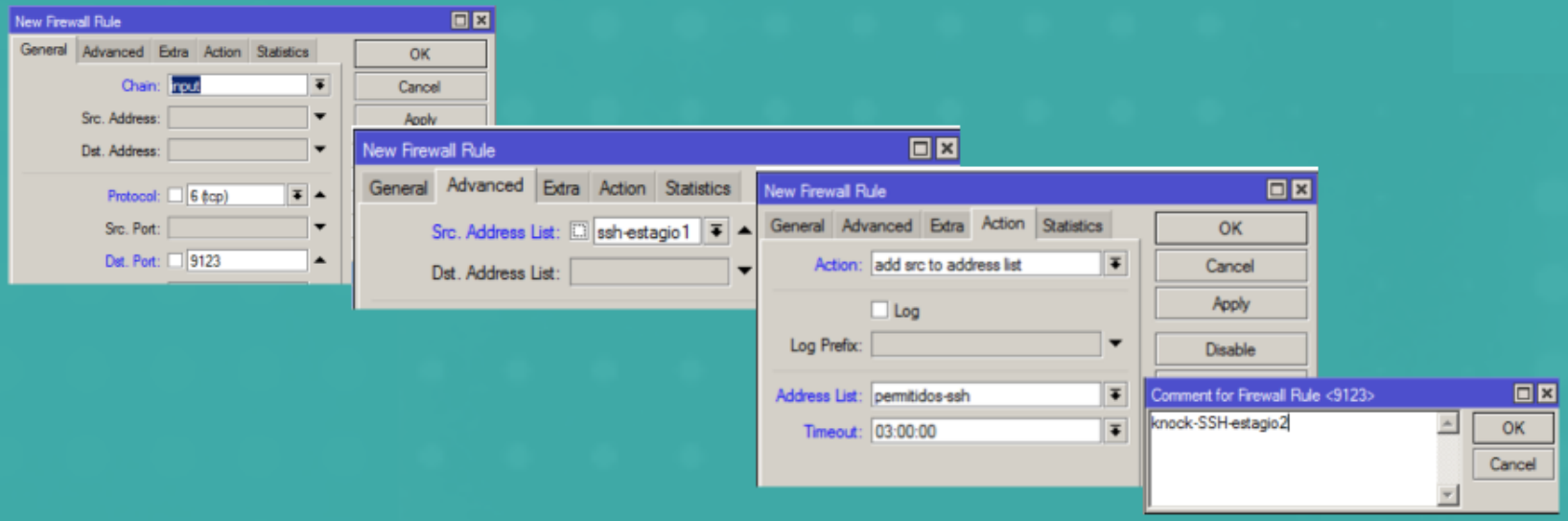



pronetworks

# Como fazer? Port Knocking

## Regra #2:



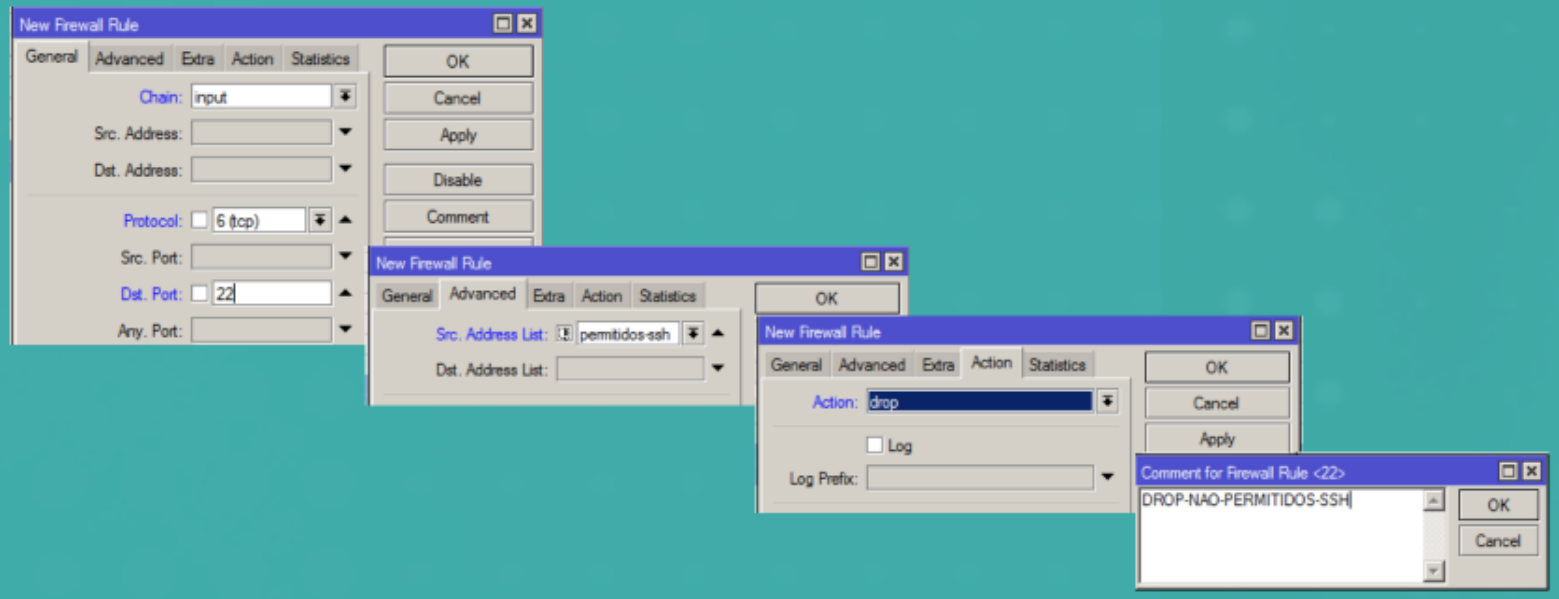



pronetworks

# Como fazer? Port Knocking

## Regra #3:

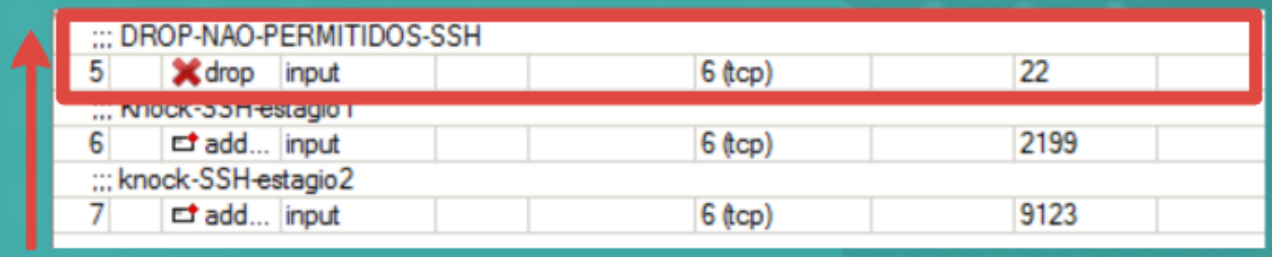





pronetworks

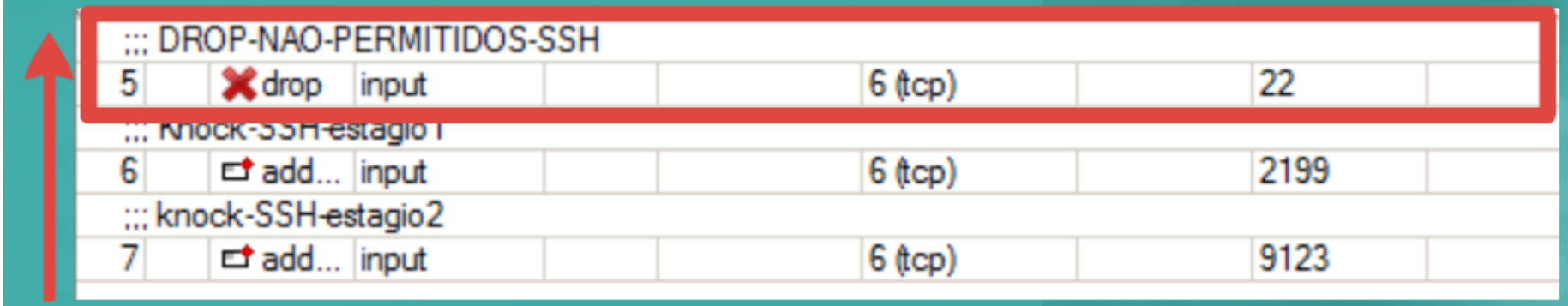
# Como fazer? Port Knocking

- Pode-se arrastar a regra para cima
- Assim o DROP poderá ser feito antes de ser processado pelas demais regras




pronetworks

ssim o DROP poderá ser feito antes de ser
rocessado pelas demais regras



# Logs Port Knocking

| | | | |
|---|---|---|---|
| Jun/03/2018 17:14:00 | memory | firewall, info | TENTATIVA-SSH input: in:bridge-lan(ether3-lan) out:(unknown 0), src-mac f4:6d:04:34:5e:93, proto TCP (SYN), 10.0.1.123:50318->10.0.1.1:22, len 52 |
| Jun/03/2018 17:14:06 | memory | firewall, info | TENTATIVA-SSH input: in:bridge-lan(ether3-lan) out:(unknown 0), src-mac f4:6d:04:34:5e:93, proto TCP (SYN), 10.0.1.123:50318->10.0.1.1:22, len 48 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ;;; DROP-NAO-PERMITIDOS-SSH | | | | | | | |
| 2 | drop | input | | | 6 (tcp) | | 22 |

| | | | |
|---|---|---|---|
| Jun/03/2018 17:15:23 | memory | firewall, info | #SSH-ESTAGIO-1 input: in:bridge-lan(ether3-lan) out:(unknown 0), src-mac f4:6d:04:34:5e:93, proto TCP (SYN), 10.0.1.123:50326->10.0.1.1:2199, len 52 |

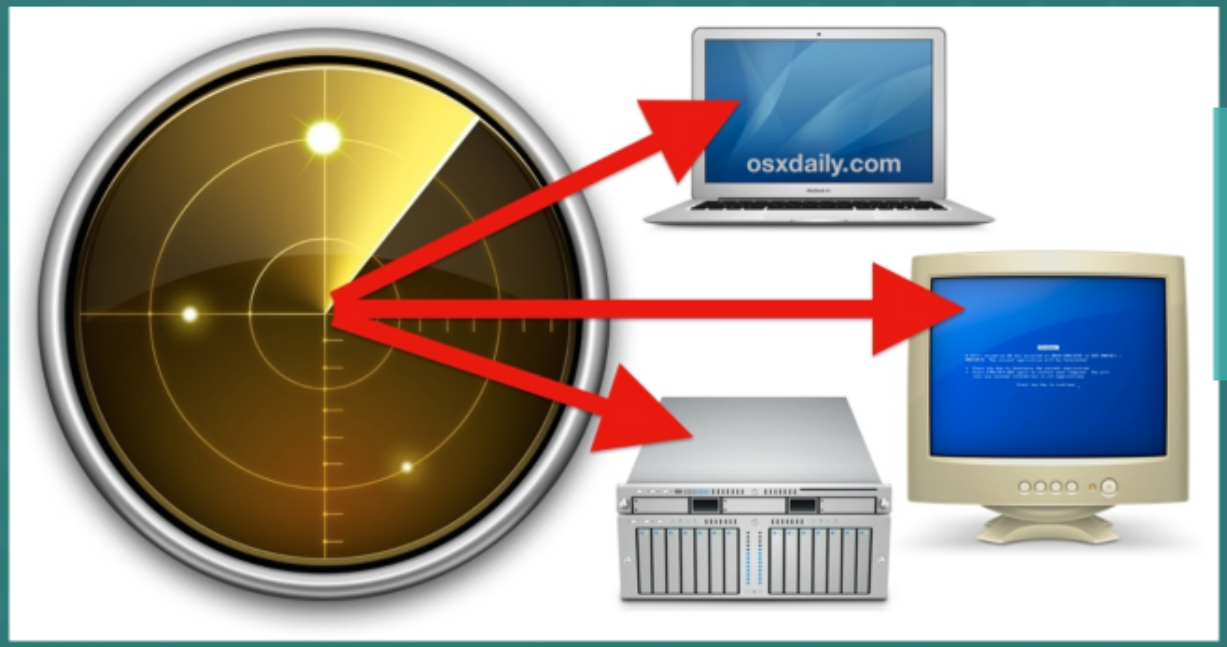
| | | | | | |
|---|---|---|---|---|---|
| D | ssh-estagio1 | 10.0.1.123 | | 00:00:25 | Jun/03/2018 17:... |

| | | | |
|---|---|---|---|
| Jun/03/2018 17:15:57 | memory | firewall, info | #SSH-ESTAGIO-2 input: in:bridge-lan(ether3-lan) out:(unknown 0), src-mac f4:6d:04:34:5e:93, proto TCP (SYN), 10.0.1.123:50333->10.0.1.1:9123, len 48 |

| | | | | | |
|---|---|---|---|---|---|
| D | permitidos-ssh | 10.0.1.123 | | 02:59:38 | Jun/03/2018 17:... |

pronetworks

# Port Scan




fonte: http://osxdaily.com/2014/05/20/port-scanner-mac-network-utility/

Protegendo-se

pronetworks

## Varredura padrão

```
Host is up (0.0025s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
2000/tcp open  cisco-sccp
8291/tcp open  unknown
MAC Address: CC:2D:E0:13:E3:D7 (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 18.39 seconds
```

Fonte: Autoria própria, 2018

pronetworks

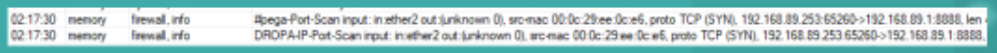
# Como evitar?

## Script

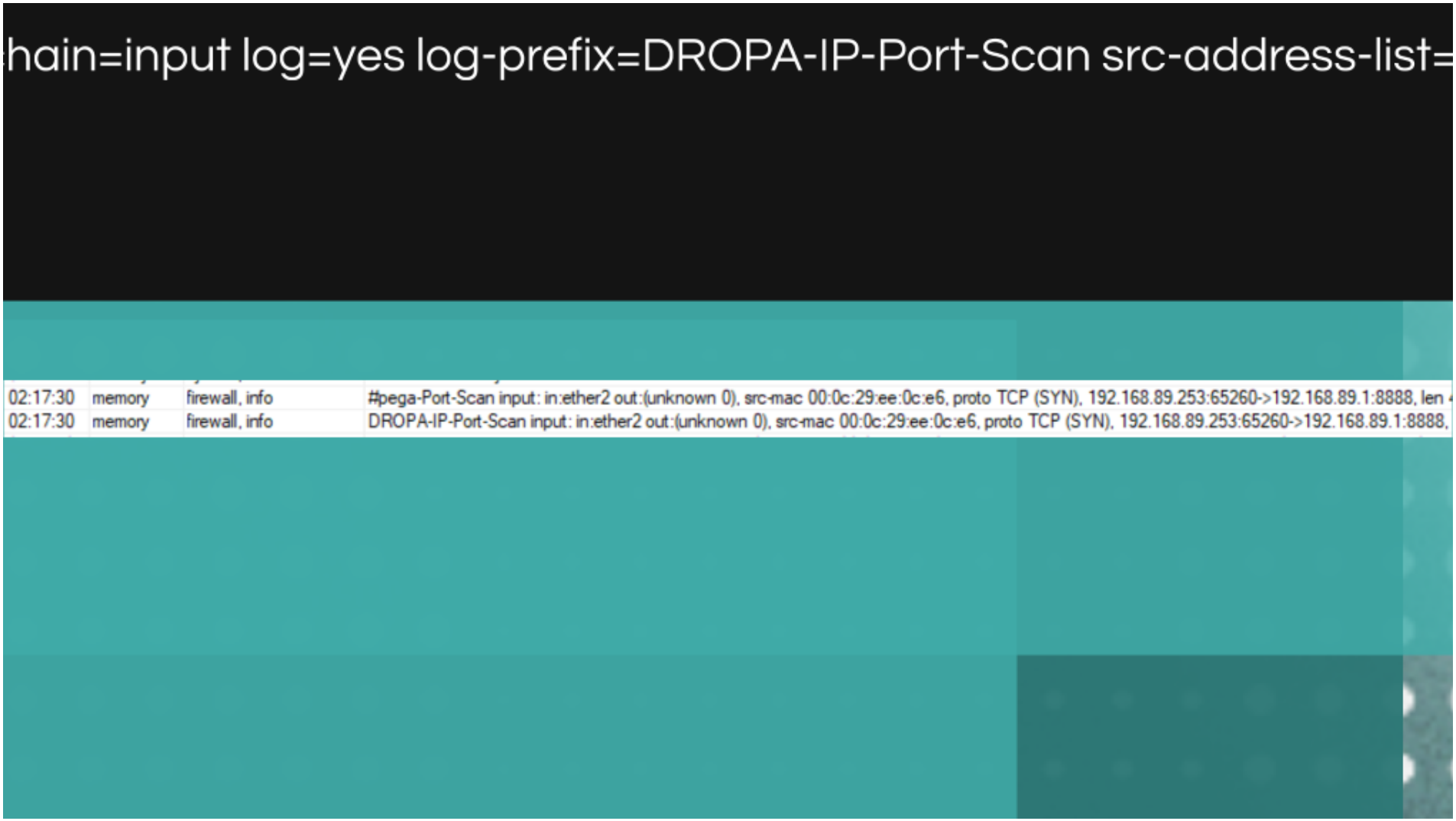
```
/ip firewall filter

 add action=add-src-to-address-list address-list=port-scan address-list-timeout=25w5d chain=input
comment="Pega a Origem - Port Scan" log=yes log-prefix=#pega-Port-Scan protocol=tcp psd=21,3s,3,1

 add action=drop chain=input log=yes log-prefix=DROPA-IP-Port-Scan src-address-list=port-scan
```

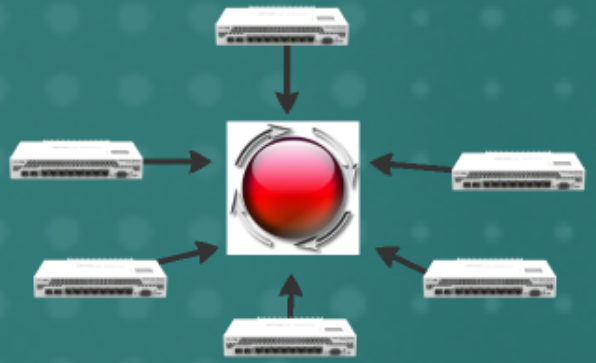



pronetworks

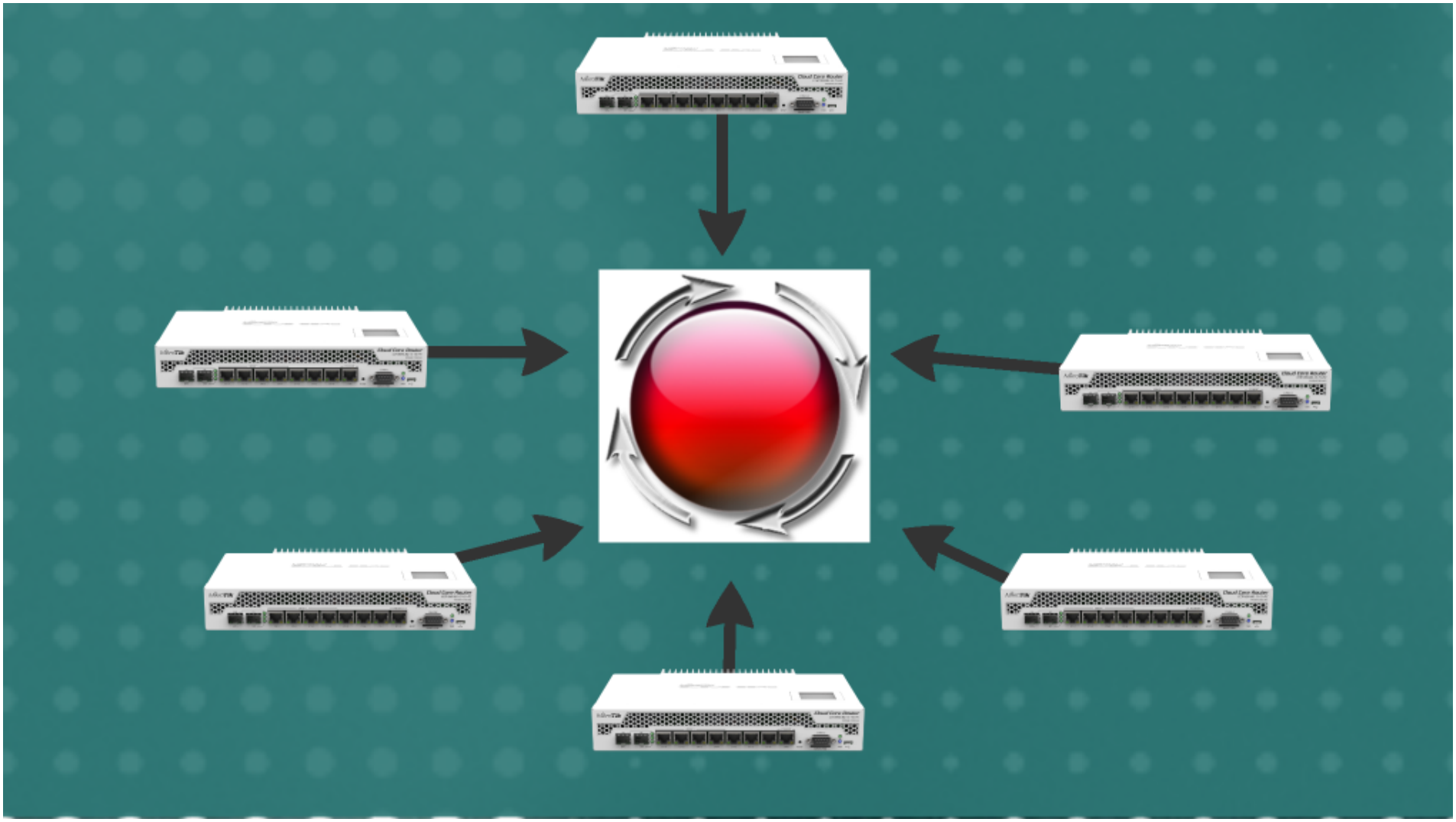

hain=input log=yes log-prefix=DROPA-IP-Port-Scan src-address-list=
02:17:30 memory firewall, info #pega-Port-Scan input: in:ether2 out:(unknown 0), src-mac 00:0c:29:ee:0c:e6, proto TCP (SYN), 192.168.89.253:65260->192.168.89.1:8888, len
02:17:30 memory firewall, info DROPA-IP-Port-Scan input: in:ether2 out:(unknown 0), src-mac 00:0c:29:ee:0c:e6, proto TCP (SYN), 192.168.89.253:65260->192.168.89.1:8888,

## Monitoramento de Logs

- Não é recomendado o armazenamento de logs críticos no dispositivo local;
- É recomendável o uso de um loghost centralizado, o "The Dude" tem essa função.
- Ao trabalhar com Syslog, verifique se o dispositivo está com datas e horas corretos;



pronetworks



| | | |
|---|---|---|
| Nov/09 22:28:09 | syslog | 220: system,info,account user Pooh logged in from 188.161.186.205 via winbox |
| Nov/09 22:28:28 | syslog | 220: system,info interface list member added by Pooh |
| Nov/09 22:28:28 | syslog | 220: system,info interface list member added by Pooh |
| Nov/09 22:28:28 | syslog | 220: system,info interface list added by Pooh |
| Nov/09 22:28:28 | syslog | 220: system,info interface list added by Pooh |
| Nov/09 22:29:02 | syslog | 220: system,info,account user Pooh logged out from 188.161.186.205 via winbox |

188.161.186.205

| Announced By | | |
|---|---|---|
| Origin AS | Announcement | Description |
| AS12975 | 188.161.0.0/16 | Palestine Telecommunications Company (PALTEL) |
| AS12975 | 188.161.128.0/17 | Palestine Telecommunications Company (PALTEL) |
| AS12975 | 188.161.128.0/18 | |
| AS12975 | 188.161.176.0/20 | Palestine Telecommunications Company (PALTEL) |

188.161.186.205

| Announced By | | |
|---|---|---|
| **Origin AS** | **Announcement** | **Description** |
| AS12975 | 188.161.0.0/16 ✅ | Palestine Telecommunications Company (PALTEL) |
| AS12975 | 188.161.128.0/17 ✅ | Palestine Telecommunications Company (PALTEL) |
| AS12975 | 188.161.128.0/18 ✅ | |
| AS12975 | 188.161.176.0/20 ✅ | Palestine Telecommunications Company (PALTEL) |

# Onde buscar mais informações?

https://blog.mikrotik.com/

https://wiki.mikrotik.com

https://www.cert.br/

https://bcp.nic.br/

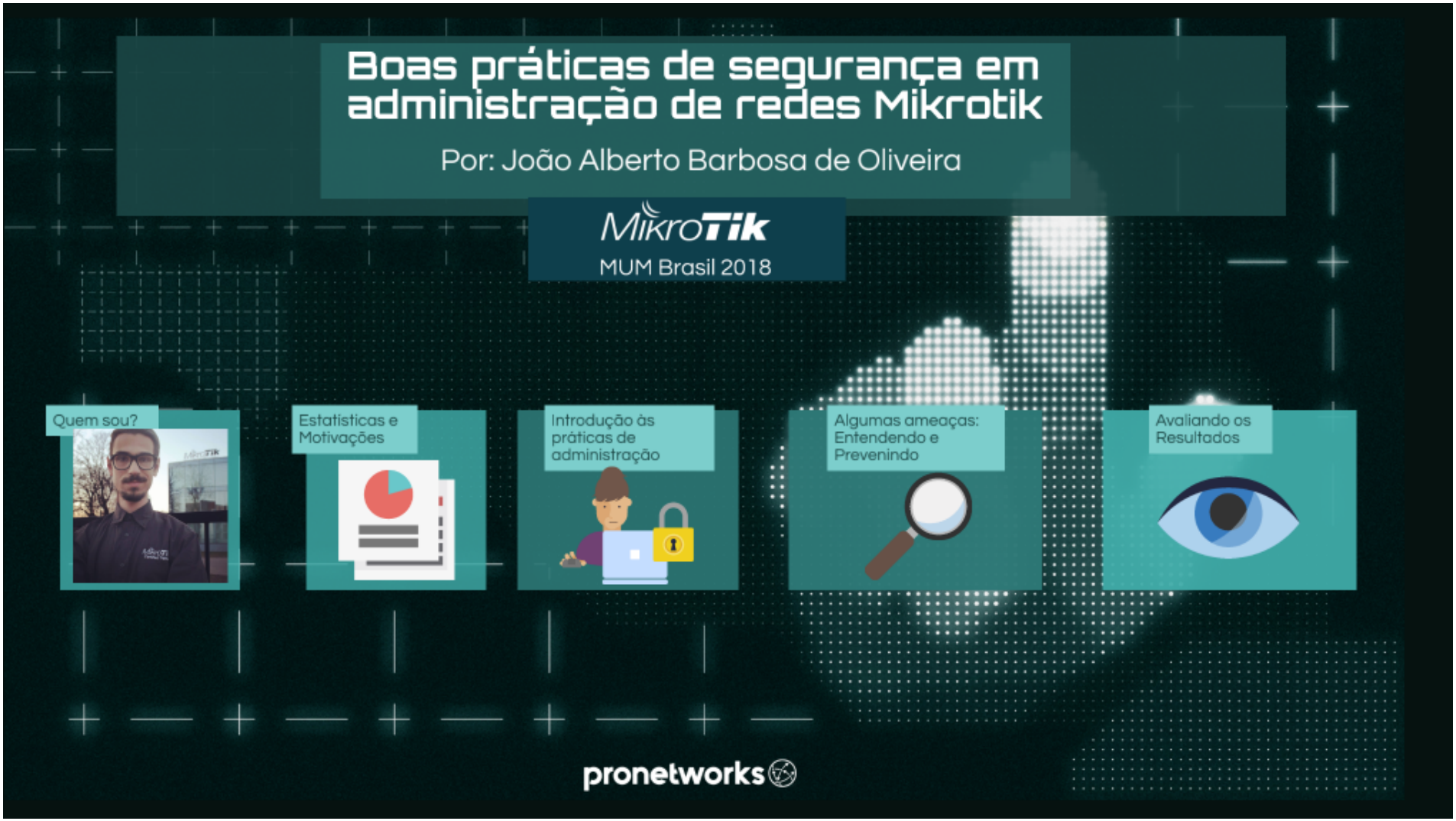
Dicas importantes!

pronetworks

## Observações importantes!

- Revise periodicamente suas configurações;
- Contextualize com as mudanças;
- Não se esqueça do IPv6!
- Cuidado com regras (principalmente forward)!

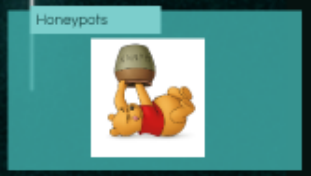
pronetworks


Boas práticas de segurança em administração de redes Mikrotik
Por: João Alberto Barbosa de Oliveira
MikroTik
MUM Brasil 2018
Quem sou?
Estatísticas e Motivações
Introdução às práticas de administração
Algumas ameaças: Entendendo e Prevenindo
Avaliando os Resultados
pronetworks

# Avaliando os Resultados

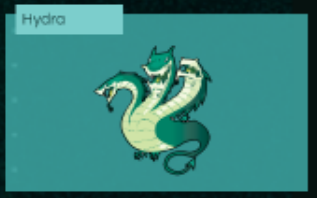
- As boas práticas devem ser levadas em consideração e aplicadas sempre que possivel e de acordo com o cenário.
- O resultado vem através do conjunto delas.

pronetworks









# Honeypots


Honeypots são uma excelente forma de testar / observar o comportamento de atacantes vulnerabilidades!

Pode-se, propositamente:

- Deixar informações "fake" visíveis
- Observar as etapas de um ataque
- Observar o comportamento anormal de pessoas da rede ou concorrentes

pronetworks

Honeypots são uma excelente forma de testar / observar o comportamento de atacantes vulnerabilidades!

# Pode-se, propositamente:

Deixar informações "fake" visíveis

Observar as etapas de um ataque

Observar o comportamento anormal de pessoas da rede ou concorrentes

pronetworks

| | |
|---|---|
| 21:45:00 | syslog: 177.10.232.222: script,info criando bkp |
| 21:41:23 | syslog: 177.10.232.220: system,info,account user Pooh logged out from 199.38.207.125 via winbox |
| 21:41:22 | syslog: 177.10.232.220: system,info socks config changed by Pooh |
| 21:41:22 | syslog: 177.10.232.220: system,info ip service changed by Pooh |
| 21:41:22 | syslog: 177.10.232.220: system,info socks acl entry added by Pooh |
| 21:41:21 | syslog: 177.10.232.220: system,info filter rule removed by Pooh |
| 21:41:21 | syslog: 177.10.232.220: system,info script removed by Pooh |
| 21:41:21 | syslog: 177.10.232.220: system,info filter rule removed by Pooh |
| 21:41:20 | syslog: 177.10.232.220: system,info,account user Pooh logged in from 199.38.207.125 via winbox |
| 21:41:20 | syslog: 177.10.232.220: system,info new script added by Pooh |
| 21:41:11 | syslog: 177.10.232.222: system,info,account user piglet logged out from 199.38.207.125 via winbox |
| 21:41:11 | syslog: 177.10.232.222: system,info ip service changed by piglet |
| 21:41:10 | syslog: 177.10.232.222: system,info socks acl entry added by piglet |
| 21:41:10 | syslog: 177.10.232.222: system,info socks config changed by piglet |
| 21:41:09 | syslog: 177.10.232.222: system,info new script added by piglet |
| 21:41:09 | syslog: 177.10.232.222: system,info script removed by piglet |
| 21:41:09 | syslog: 177.10.232.222: system,info filter rule removed by piglet |
| 21:41:09 | syslog: 177.10.232.222: system,info filter rule removed by piglet |
| 21:41:08 | syslog: 177.10.232.222: system,info,account user piglet logged in from 199.38.207.125 via winbox |
| 21:41:03 | syslog: 177.10.232.222: system,error,critical login failure for user piglet from 199.38.207.125 via winbox |
| 21:31:10 | syslog: 177.10.232.220: script,info deletando bkp |

Evento em: 13/11/2018
Fonte: Autoria Própria

# Pen Tests
# White Hat

- Estudar o funcionamento de protocolos e suas falhas e após isso, analisar em seu cenário;
- Avaliar periodicamente sua rede, com base em requisitos de seu cenário;
- Se informar sobre exploits para o seu fabricante;

Reflexões...

- Geralmente protegemos a rede apenas "de fora para dentro" mas a tentativa pode vir de dentro...
- "Se você não testar a sua rede, um dia alguém fará isso..." ;)

pronetworks

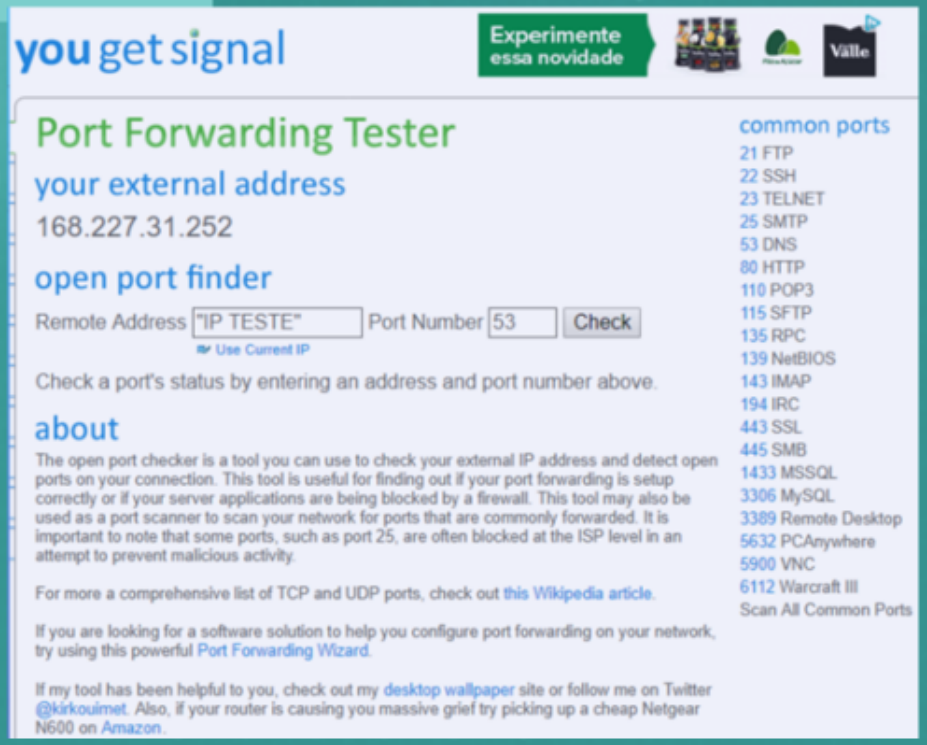
# Reflexões...

https://opiniaocentral.files.wordpress.com/2015/03/dsc02824.jpg?w=298&h=224

- Geralmente protegemos a rede apenas "de fora para dentro" mas a tentativa pode vir de dentro...
- "Se você não testar a sua rede, um dia alguém fará isso..." :)

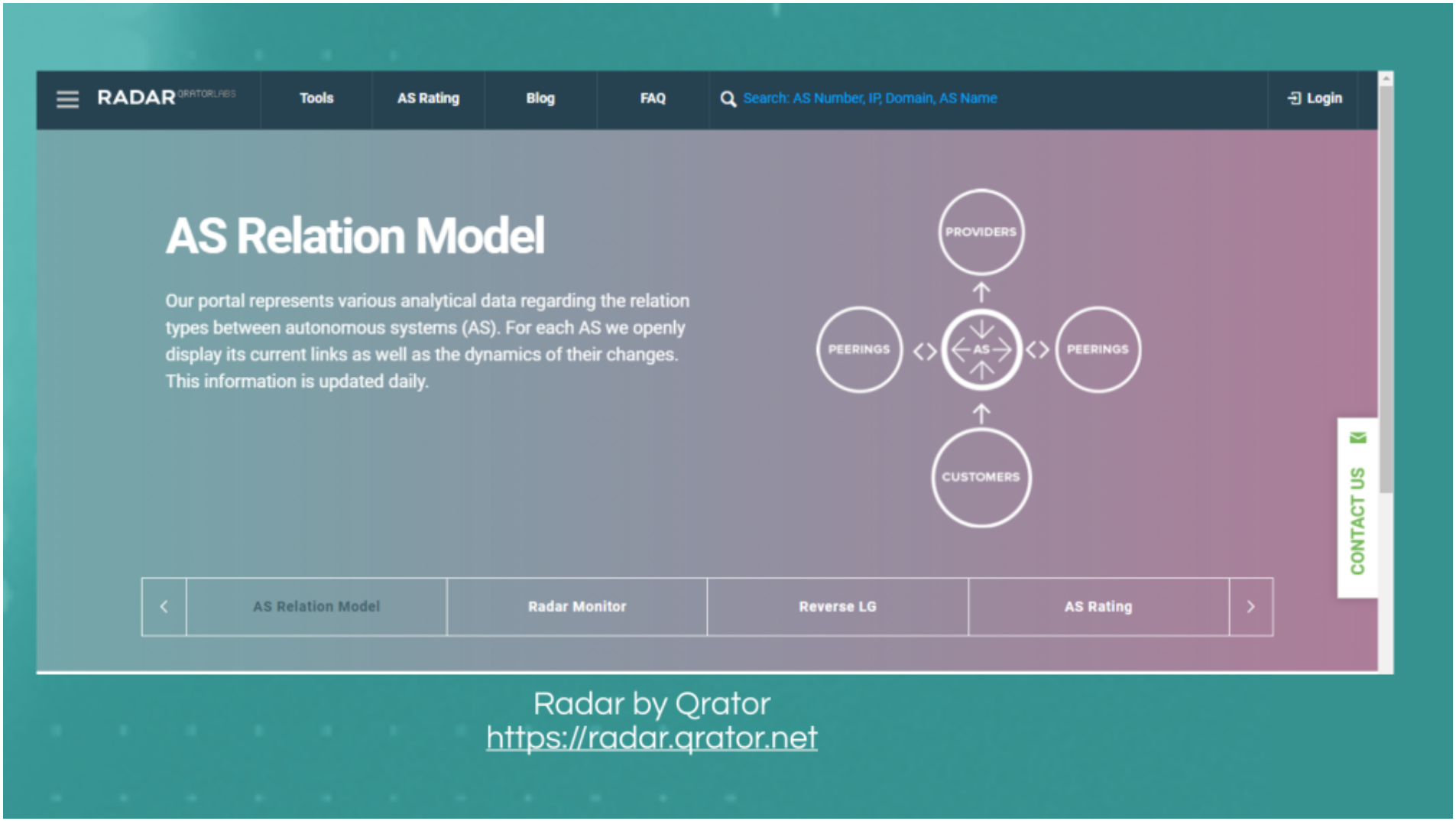
pronetworks

# Resultados
# Como testar?




acessivel em: https://www.yougetsignal.com/tools/open-ports/

pronetworks


RADAR QRATORLABS
Tools
AS Rating
Blog
FAQ
Search: AS Number, IP, Domain, AS Name
Login
AS Relation Model
Our portal represents various analytical data regarding the relation types between autonomous systems (AS). For each AS we openly display its current links as well as the dynamics of their changes. This information is updated daily.
PROVIDERS
PEERINGS
AS
PEERINGS
CUSTOMERS
CONTACT US
AS Relation Model
Radar Monitor
Reverse LG
AS Rating
Radar by Qrator
https://radar.qrator.net

# To manually test an IP address

```
dig +short test.openresolver.com TXT @1.2.3.4
```

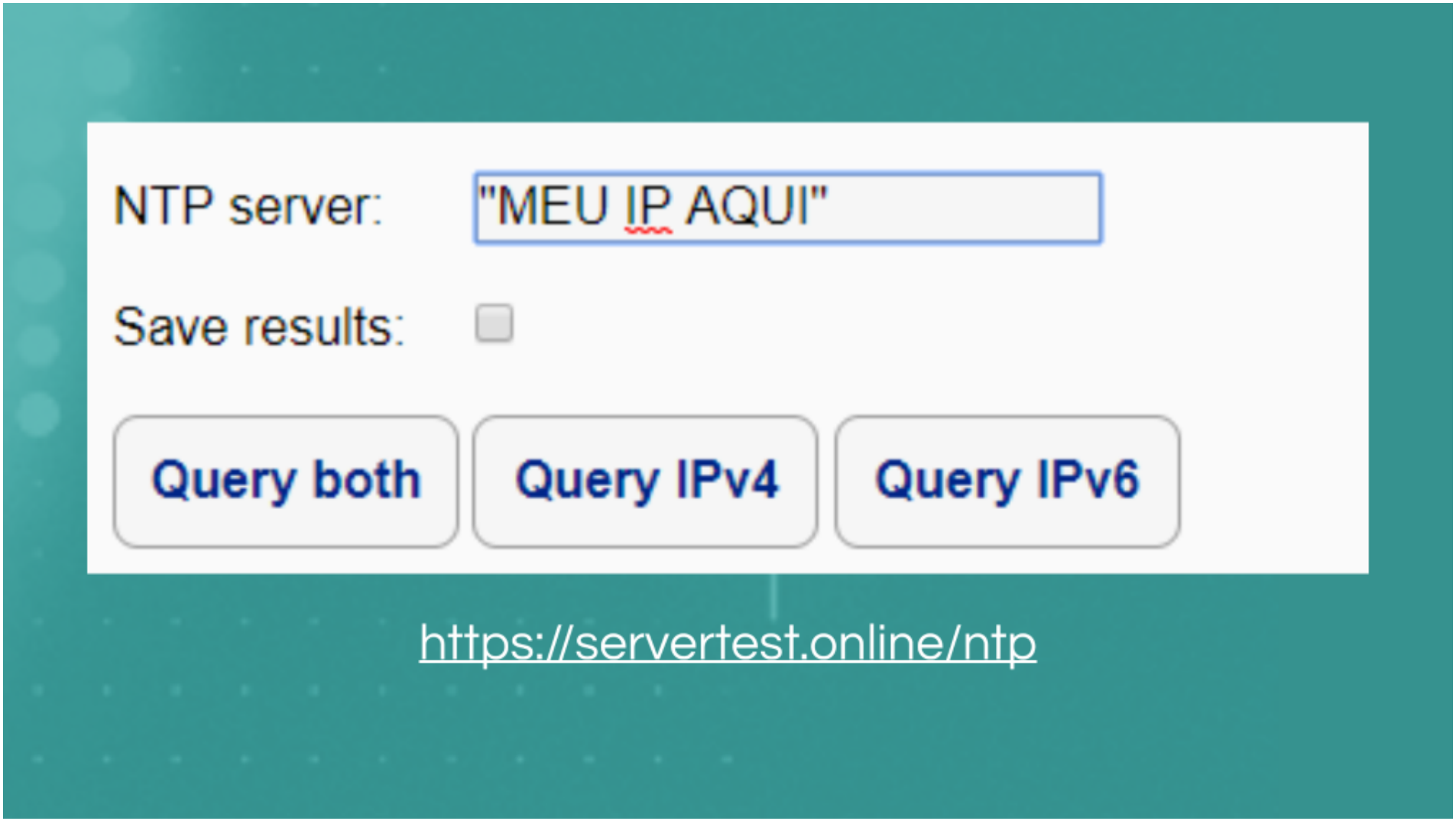
(replace 1.2.3.4 with the IP address or domain name of the DNS server you are testing)

If you get "open-resolver-detected" in response, then you have a problem :)

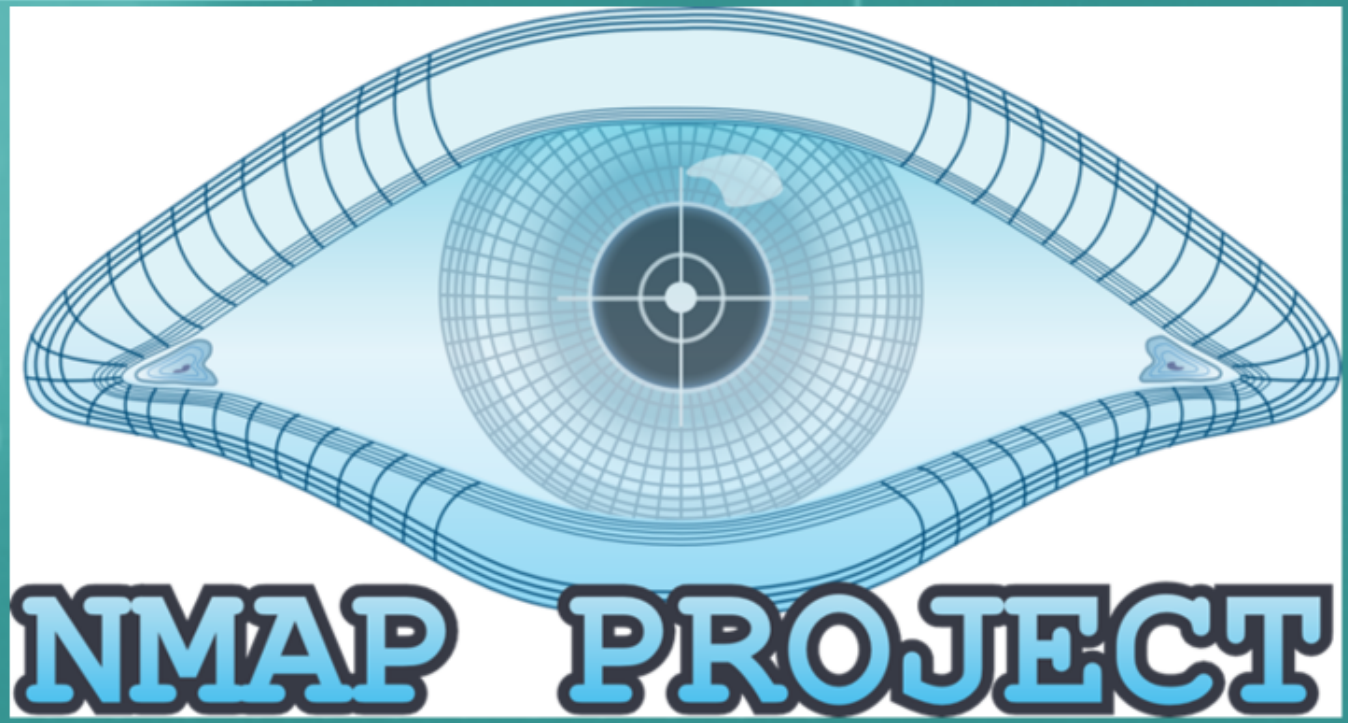
# Or, use a form:

"MEU IP AQUI" Test this IP

https://openresolver.com/


NTP server:
"MEU IP AQUI"
Save results:
Query both
Query IPv4
Query IPv6
https://servertest.online/ntp

## Nmap




acessivel em: https://nmap.org/

pronetworks

# Hydra


Incluso no Kali Linux: https://www.kali.org/

Referenc
Bibliogr

pronetworks

# Referencias Bibliográficas/ Links extras

https://wiki.mikrotik.com

http://nic.br/

https://cert.br

https://tools.ietf.org/html/bcp84

bcp.nic.br

http://www.team-cymru.com/

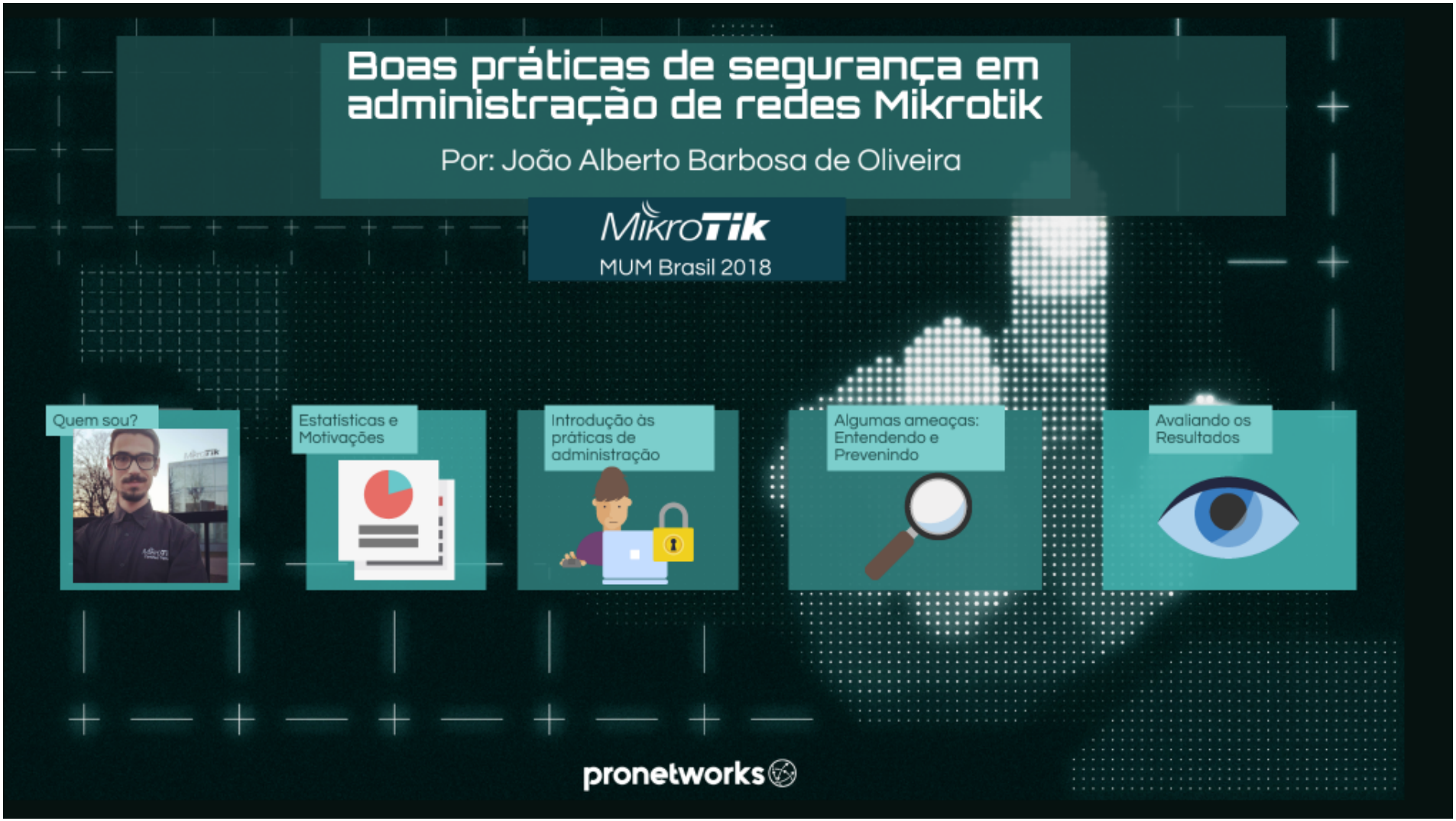
https://ostec.blog/padronizacao-seguranca/iso-27002-boas-praticas-gsi

Obrigado!

pronetworks

Obrigado!

Dúvidas??
Obrigado!


Boas práticas de segurança em administração de redes Mikrotik
Por: João Alberto Barbosa de Oliveira
MikroTik
MUM Brasil 2018
Quem sou?
Estatísticas e Motivações
Introdução às práticas de administração
Algumas ameaças: Entendendo e Prevenindo
Avaliando os Resultados
pronetworks