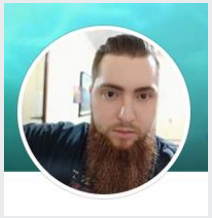
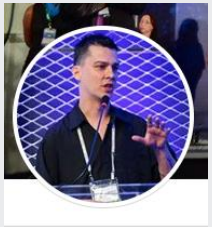
Dever de Casa e o Impacto da Negligência Técnica e Administrativa de Participantes do IX-BR

Quem somos?



Vagner Zanoni

Profissional do ramo de consultoria há mais de 8 anos,
atualmente é consultor-chefe na NextHop Solutions, atuando a frente de desenvolvimento de projetos e produtos.
É também, bacharel em Sistemas da Informação pela Faculdade ESUCRI de Santa Catarina.



Elizandro Pacheco

Profissional do ramo de consultoria para provedores de internet há mais de 15 anos no mercado, estudou engenharia em sistemas digitais na universidade estadual do rio grande do sul e atualmente cursa gestão em tecnologia da informação no senac/sp.
É autor do livro Docker Para Provedores, um dos fundadores da Network Education e CEO da NextHop Solutions, empresa especializada em consultoria para provedores.

nic.br cgi.br

NETWORK EDUCATION

NEXTHOP SOLUTIONS

Por que este tema?

- ✓ Alta frequência de vulnerabilidades nos últimos anos,

Por que este tema?

- ✓ Alta frequência de vulnerabilidades nos últimos anos,
- ✓ Divulgação de exploits variados,

Por que este tema?

- ✓ Alta frequência de vulnerabilidades nos últimos anos,
- ✓ Divulgação de exploits variados,
- ✓ Quantidade de dispositivos responsáveis por conexões entre sistemas autônomos vulneráveis, desprotegidos e negligenciados.

Por que este tema?

- ✓ Alta frequência de vulnerabilidades nos últimos anos,
- ✓ Divulgação de exploits variados,
- ✓ Quantidade de dispositivos responsáveis por conexões entre sistemas autônomos vulneráveis, desprotegidos e negligenciados.
- ✓ Falta de orientação completa e efetiva sobre alternativas simples e eficientes para se proteger.

Por que este tema?

- ✓ Alta frequência de vulnerabilidades nos últimos anos,
- ✓ Divulgação de exploits variados,
- ✓ Quantidade de dispositivos responsáveis por conexões entre sistemas autônomos vulneráveis, desprotegidos e negligenciados.
- ✓ Falta de orientação completa e efetiva sobre alternativas simples e eficientes para se proteger.

Mikrotik » Routeros : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

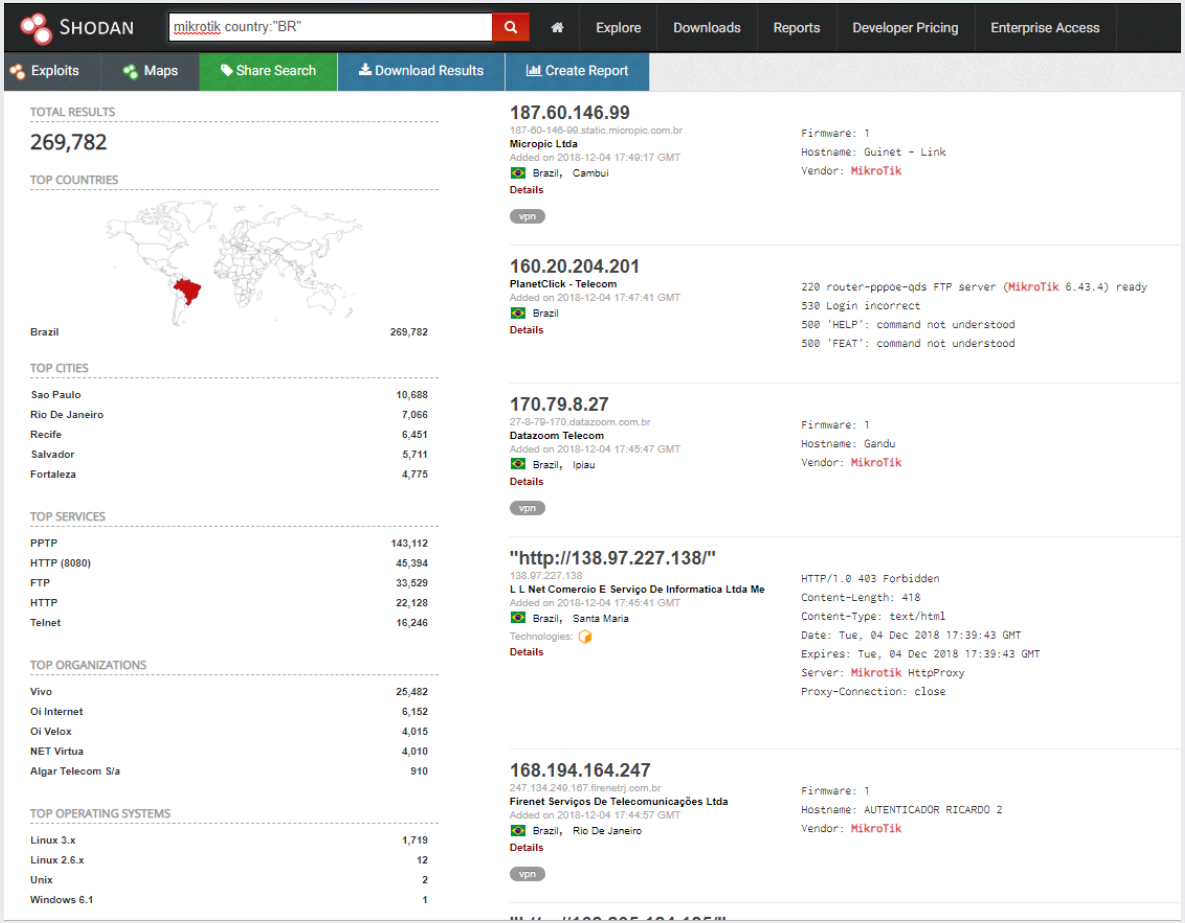
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-14847	287		Dir. Trav.	2018-08-02	2018-11-16	5.0	None	Remote	Low	Not required	Partial	None	None
MikroTik RouterOS through 6.42 allows unauthenticated remote attackers to read arbitrary files and remote authenticated attackers to write arbitrary files due to a directory traversal vulnerability in the WinBox interface.														
2	CVE-2018-7445	119		Exec Code Overflow	2018-03-19	2018-04-24	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
A buffer overflow was found in the MikroTik RouterOS SMB service when processing NetBIOS session request messages. Remote attackers with access to the service can exploit this vulnerability and gain code execution on the system. The overflow occurs before authentication takes place, so it is possible for an unauthenticated remote attacker to exploit it. All architectures and all devices running RouterOS before versions 6.41.3/6.42rc27 are vulnerable.														
3	CVE-2018-1159	119		Overflow Mem. Corr.	2018-08-23	2018-10-12	4.0	None	Remote	Low	Single system	None	None	Partial
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory corruption vulnerability. An authenticated remote attacker can crash the HTTP server by rapidly authenticating and disconnecting.														
4	CVE-2018-1158	400			2018-08-23	2018-10-12	4.0	None	Remote	Low	Single system	None	None	Partial
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a stack exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server via recursive parsing of JSON.														
5	CVE-2018-1157	400			2018-08-23	2018-11-23	6.8	None	Remote	Low	Single system	None	None	Complete
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server and in some circumstances reboot the system via a crafted HTTP POST request.														
6	CVE-2018-1156	119		Exec Code Overflow	2018-08-23	2018-11-23	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to stack buffer overflow through the license upgrade interface. This vulnerability could theoretically allow a remote authenticated attacker execute arbitrary code on the system.														
7	CVE-2017-8338	399			2017-05-18	2017-06-01	7.8	None	Remote	Low	Not required	None	None	Complete
A vulnerability in MikroTik Version 6.38.5 could allow an unauthenticated remote attacker to exhaust all available CPU via a flood of UDP packets on port 500 (used for L2TP over IPsec), preventing the affected router from accepting new connections; all devices will be disconnected from the router and all logs removed automatically.														
8	CVE-2017-7285	400			2017-03-29	2017-04-10	7.8	None	Remote	Low	Not required	None	None	Complete
A vulnerability in the network stack of MikroTik Version 6.38.5 released 2017-03-09 could allow an unauthenticated remote attacker to exhaust all available CPU via a flood of TCP RST packets, preventing the affected router from accepting new TCP connections.														
9	CVE-2017-6297	254			2017-02-27	2017-03-15	4.3	None	Remote	Medium	Not required	Partial	None	None
The L2TP Client in MikroTik RouterOS versions 6.83.3 and 6.37.4 does not enable IPsec encryption after a reboot, which allows man-in-the-middle attackers to view transmitted data unencrypted and gain access to networks on the L2TP server by monitoring the packets for the transmitted data and obtaining the L2TP secret.														
10	CVE-2015-2350	352		CSRF	2015-03-19	2015-09-24	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Cross-site request forgery (CSRF) vulnerability in MikroTik RouterOS 5.0 and earlier allows remote attackers to hijack the authentication of administrators for requests that change the administrator password via a request in the status page to /cfg.														
11	CVE-2012-6050	16	1	DoS	2012-11-26	2017-08-28	6.4	None	Remote	Low	Not required	Partial	None	Partial
The winbox service in MikroTik RouterOS 5.15 and earlier allows remote attackers to cause a denial of service (CPU consumption), read the router version, and possibly have other impacts via a request to download the router's DLLs or plugins, as demonstrated by roteros.dll.														

Total number of vulnerabilities : 11 Page : 1 (This Page)

Shodan: Mikrotik Brasil



nic.br cgi.br

NEXTHOP SOLUTIONS

Shodan: RouterOS Brasil

SHODAN routeros country:"BR" Explore Downloads Reports Developer Pricing Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS

74,493

TOP COUNTRIES

Brazil	74,493

TOP CITIES

Rio De Janeiro	5,150
Sao Paulo	4,745
Recife	1,959
Salvador	1,810
Ribeirao Das Neves	758

TOP SERVICES

SNMP	60,035
8081	5,716
Splunk	2,477
8083	1,615
HTTP (8181)	757

TOP ORGANIZATIONS

Vivo	6,132
Mundivox LTDA	4,975
RB7 TELECOM	1,617
Netprimus Tecnologia Ltda	1,543
Oi Internet	1,221

TOP OPERATING SYSTEMS

Linux 3.x	41

TOP PRODUCTS

MikroTik router ftpd	105

177.73.107.114
Fatima Video Eletronica Ltda Me
Added on 2018-12-04 17:47:43 GMT
Brazil, Dourados
Details

RouterOS RB1100

186.229.55.101
186-229-55-101.ded.intelignet.com.br
Tim Celular S.A.
Added on 2018-12-04 17:47:30 GMT
Brazil, Rio De Janeiro
Details

RouterOS RB1100AHx2

201.55.113.18
static-201-55-113-18.optitel.net.br
Itake Telecom
Added on 2018-12-04 17:46:17 GMT
Brazil, Jacutinga
Details

RouterOS RB750

177.87.218.209
GPSNet Provedor de Acesso a Redes de Comunicação
Added on 2018-12-04 17:45:30 GMT
Brazil, Sao Borja
Details
scanner

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Length: 7025
Content-Type: text/html
Date: Mon, 03 Dec 2018 20:23:11 GMT
Expires: 0

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
<html xmlns="http://www.w3.org/1999...
```

201.76.167.104
mvx-201-76-167-104.mundivox.com
Mundivox LTDA
Added on 2018-12-04 17:43:50 GMT
Brazil, Rio De Janeiro
Details

RouterOS RB750r2

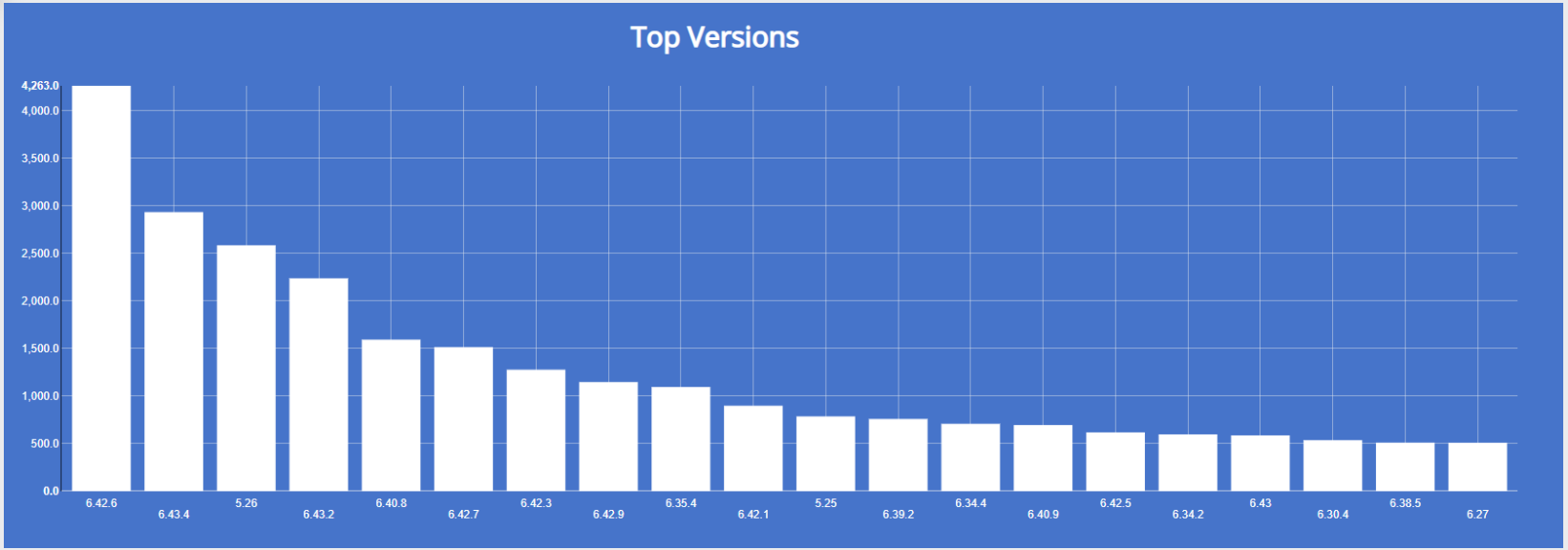
177.105.64.70
Netprimus Tecnologia Ltda
Added on 2018-12-04 17:42:29 GMT
Brazil, Recife
Details

RouterOS CCR1009-8G-1S-1S+

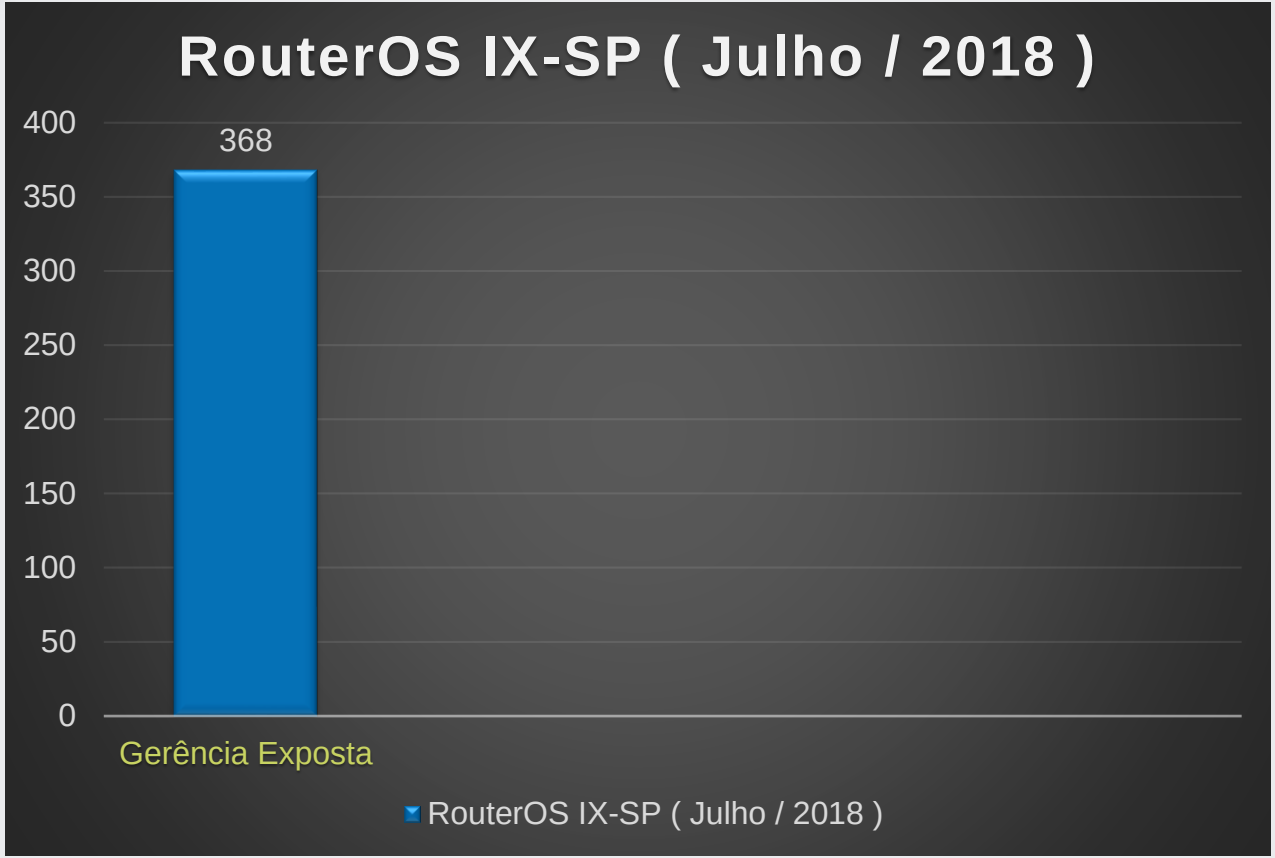
nic.br cgi.br

NEXTHOP SOLUTIONS

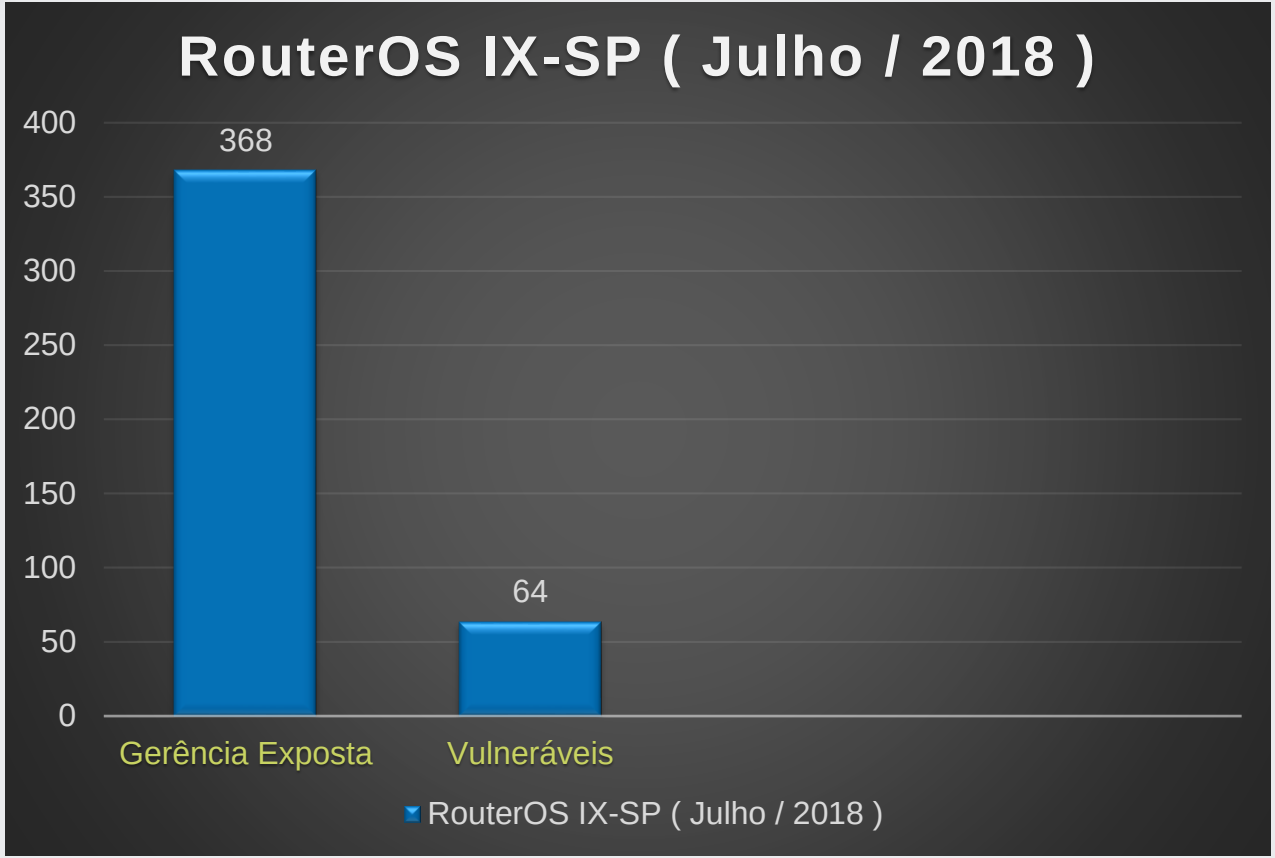
Shodan: Mikrotik Brasil



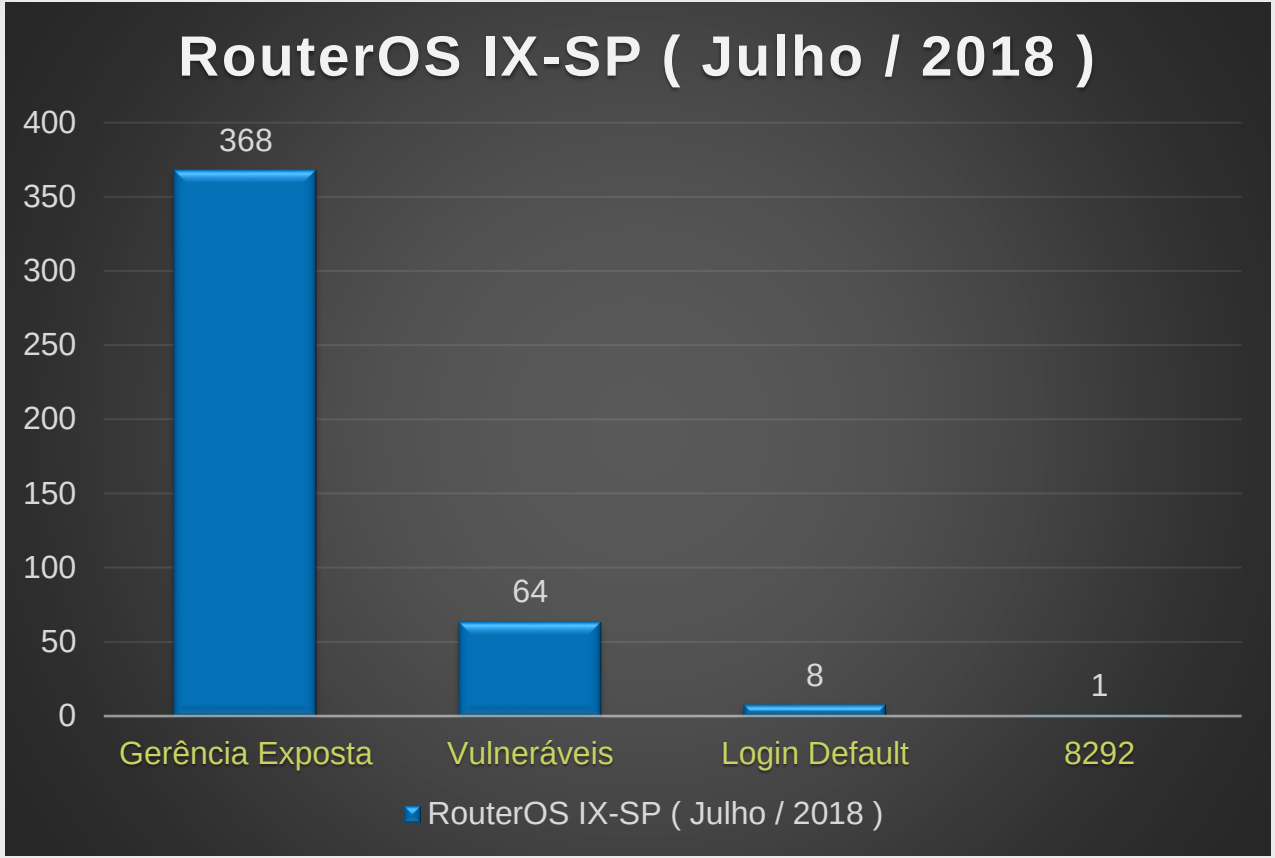
Análise IX-SP



Análise IX-SP



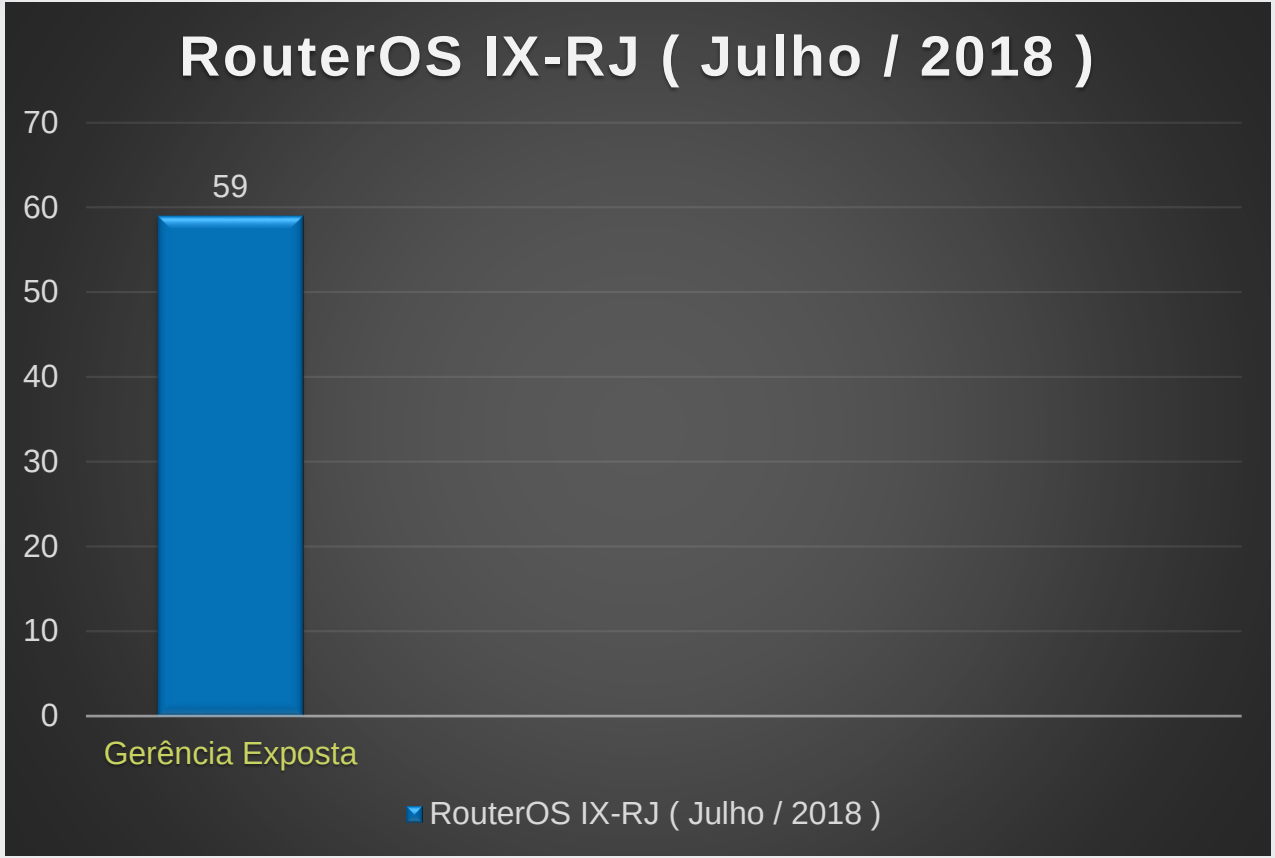
Análise IX-SP



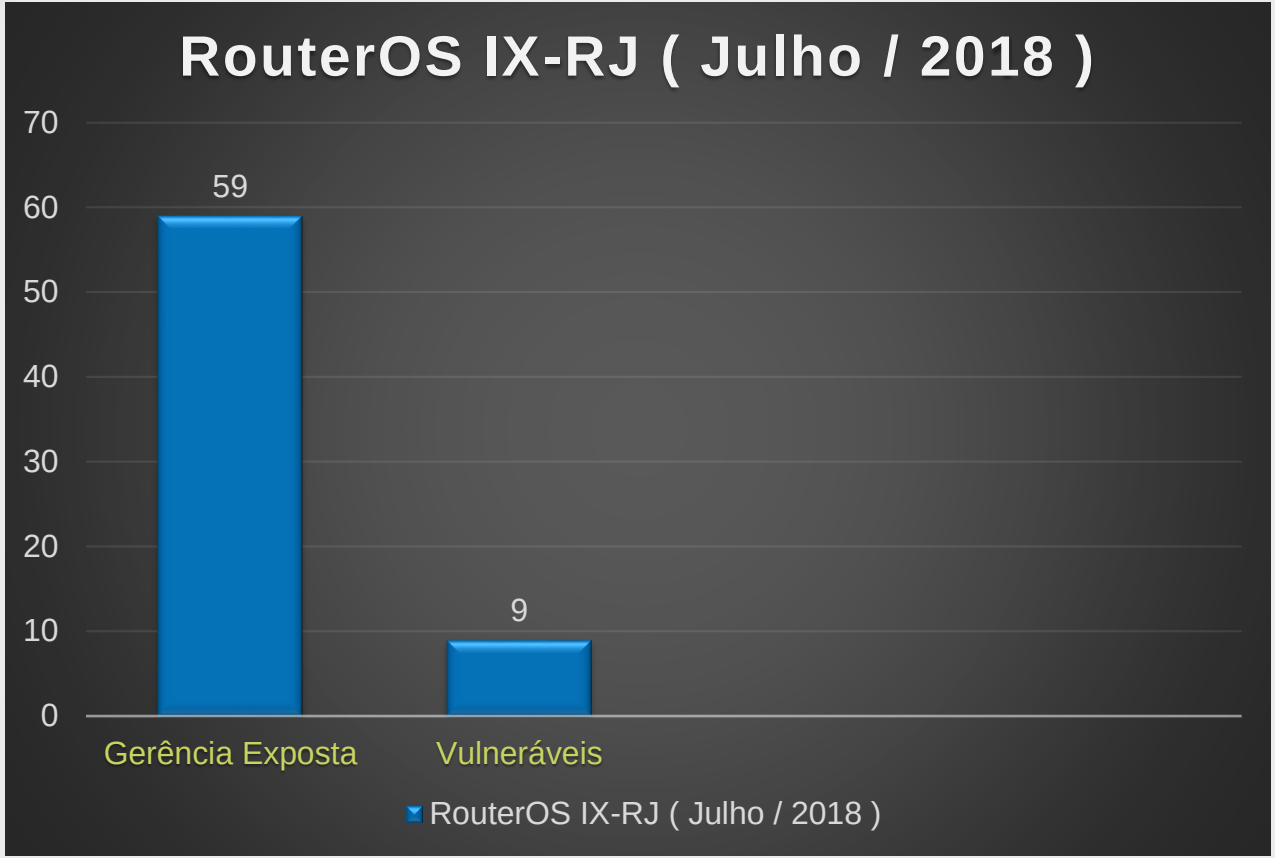
nic.br cgi.br

NEXTHOP SOLUTIONS

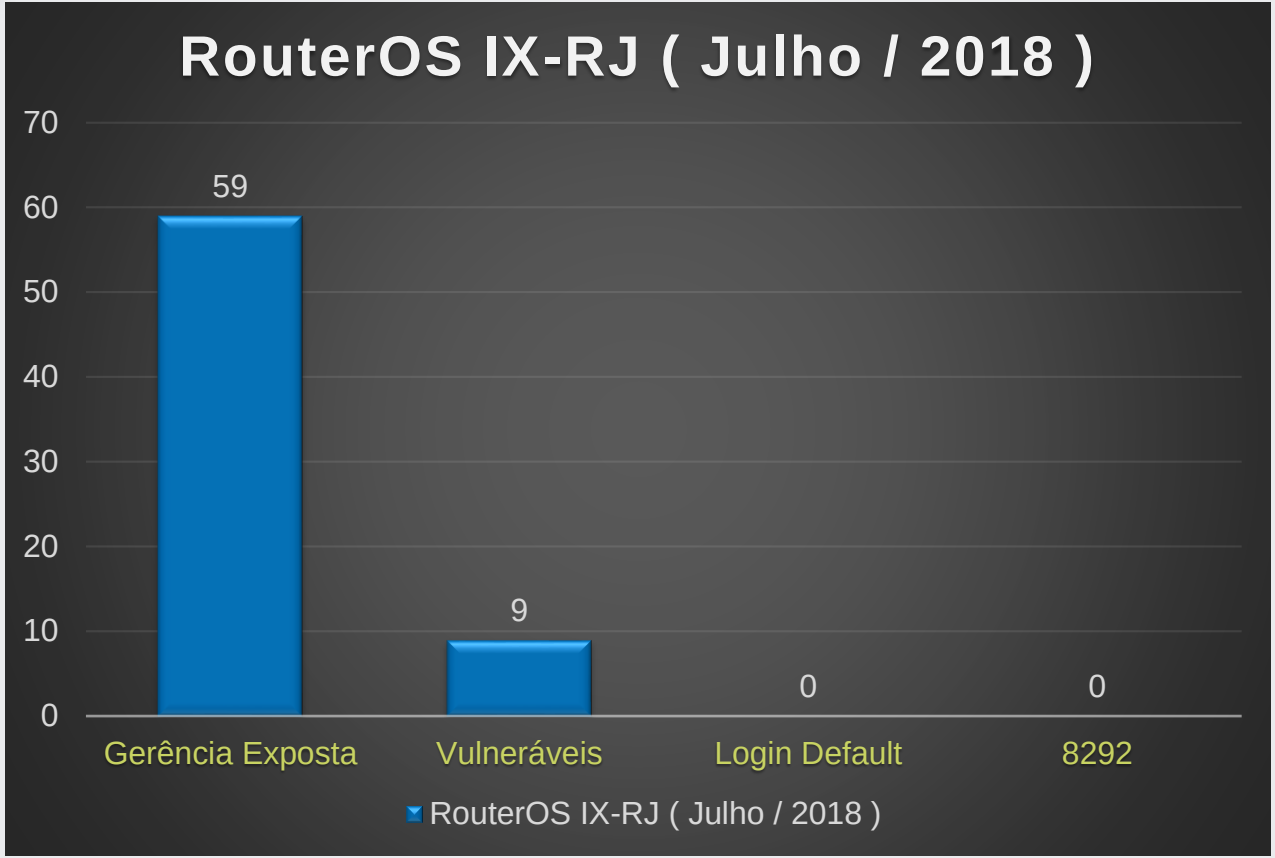
Análise IX-RJ



Análise IX-RJ



Análise IX-RJ



Como melhorar a situação?

Como melhorar a situação - RouterOS

- ✓ Proteger a gerência do dispositivo.

Como melhorar a situação - RouterOS

- ✓ Proteger a gerência do dispositivo.
- ✓ Técnica de Port Knocking.

Técnica de Port Knocking

- ✓ O port knocking é um técnica de firewall onde o cliente envia uma sequência de pacotes em portas diferentes, que estão fechadas no host destinatário.
- ✓ Apesar da porta do host destinatário estar protegida no firewall, este fica escutando os pacotes que chegam.
- ✓ Caso a sequência de pacotes enviada pelo cliente estiver correta (for a determinada pelas políticas do firewall do destinatário)
- ✓ Este cliente ganha acessos privilegiados temporariamente.

Técnica de Port Knocking – Exemplo 1

- ✓ Exemplo básico em RouterOS:

- ✓ Ao “bater” na porta 1000, o ip de origem da conexão é Adicionado a uma lista chamada port:9000 com um timeout de 1 m.

Técnica de Port Knocking – Exemplo 1

- ✓ Exemplo básico em RouterOS:

- ✓ Ao "bater" na porta 1000, o ip de origem da conexão é Adicionado a uma lista chamada port:1000 com um timeout de 1 m.

- ✓ Se dentro deste minuto, houver outra conexão com destino a porta 3000 e o ip de origem já estiver na address-list port:1000, o ip então é adicionado a uma segunda lista (secure), Que por sua vez, será a lista utilizada nas liberações de input.

Técnica de Port Knocking – Exemplo 1

- ✓ Exemplo básico em RouterOS:

```
/ip firewall filter
add action=add-src-to-address-list address-list=port:1000 address-list-timeout=1m \
        chain=input dst-port=1000 protocol=tcp

add action=add-src-to-address-list address-list=secure address-list-timeout=1m \
        chain=input dst-port=3000 protocol=tcp src-address-list=port:1000


add action=accept chain=input src-address-list=secure

add action=drop disable=yes chain=input
```

Exemplo 1 – Análise

- ✓ Baixo nível de segurança
- ✓ Apenas 2 portas para bater
- ✓ Sequência crescente de portas
- ✓ Timeout muito alto nas listas

Técnica de Port Knocking – Exemplo 2

- ✓ Exemplo RouterOS, maior segurança.
- ✓ Ao “bater” na porta 54389, o ip de origem da conexão é Adicionado a uma lista chamada port: 54389 com um timeout de 10s.

Técnica de Port Knocking – Exemplo 1

- ✓ Exemplo RouterOS, maior segurança.
- ✓ Ao "bater" na porta 54389, o ip de origem da conexão é Adicionado a uma lista chamada port: 54389 com um timeout de 10s.
- ✓ Se dentro destes 10s, houver outra conexão com destino a porta 1763 e o ip de origem já estiver na address-list port: 54389, o ip então é adicionado a uma segunda lista: port:1763 com timeout também de 10s.

Técnica de Port Knocking – Exemplo 2

- ✓ Exemplo RouterOS, maior segurança.
- ✓ Ao "bater" na porta 54389, o ip de origem da conexão é Adicionado a uma lista chamada port: 54389 com um timeout de 10s.
- ✓ Se dentro destes 10s, houver outra conexão com destino a porta 1763 e o ip de origem já estiver na address-list port: 54389, o ip então é adicionado a uma segunda lista: port:1763 com timeout também de 10s.
- ✓ Se dentro dos próximos 10s, houver outra conexão com destino a porta 34576 e o ip de origem já estiver na address-list port:1763 , o ip então é adicionado a uma terceira lista: secure, com timeout de 1h.

Técnica de Port Knocking – Exemplo 2

- ✓ Exemplo RouterOS, maior segurança.
- ✓ Ao "bater" na porta 54389, o ip de origem da conexão é Adicionado a uma lista chamada port: 54389 com um timeout de 10s.
- ✓ Se dentro destes 10s, houver outra conexão com destino a porta 1763 e o ip de origem já estiver na address-list port: 54389, o ip então é adicionado a uma segunda lista: port:1763 com timeout também de 10s.
- ✓ Se dentro dos próximos 10s, houver outra conexão com destino a porta 34576 e o ip de origem já estiver na address-list port:1763
- ✓ , o ip então é adicionado a uma terceira lista: secure, com timeout de 1h.
- ✓ Que por sua vez, será a lista utilizada nas liberações de input.

Técnica de Port Knocking – Exemplo 2

✓ Exemplo RouterOS, maior segurança

```
/ip firewall filter
add action=add-src-to-address-list address-list=port:54389 address-list-timeout=10s chain=\
   input dst-port=54389 protocol=tcp

add action=add-src-to-address-list address-list=port:1763 address-list-timeout=10s chain=\
   input dst-port=1763 protocol=tcp src-address-list=port:54389

add action=add-src-to-address-list address-list=secure address-list-timeout=1h chain=input \
   dst-port=34576 protocol=tcp src-address-list=port:1763

add action=accept chain=input src-address-list=secure

add action=drop disable=yes chain=input
```

Exemplo 2 – Análise

- ✓ Maior nível de segurança
- ✓ 3 portas para bater
- ✓ Portas fora de sequência
- ✓ Timeout de 10s

Técnica de Port Knocking – Exemplo 3

- ✓ Exemplo RouterOS, liberar apenas VPN IPSec.
- ✓ Ao "bater" na porta 54389, o ip de origem da conexão é Adicionado a uma lista chamada port: 54389 com um timeout de 10s.

Técnica de Port Knocking – Exemplo 3

- ✓ Exemplo RouterOS, liberar apenas VPN IPSec.
- ✓ Ao "bater" na porta 54389, o ip de origem da conexão é Adicionado a uma lista chamada port: 54389 com um timeout de 10s.
- ✓ Se dentro destes 10s, houver outra conexão com destino a porta 1763 e o ip de origem já estiver na address-list port: 54389, o ip então é adicionado a uma segunda lista: port:1763 com timeout também de 10s.

Técnica de Port Knocking – Exemplo 3

- ✓ Exemplo RouterOS, liberar apenas VPN IPSec.
- ✓ Ao "bater" na porta 54389, o ip de origem da conexão é Adicionado a uma lista chamada port: 54389 com um timeout de 10s.
- ✓ Se dentro destes 10s, houver outra conexão com destino a porta 1763 e o ip de origem já estiver na address-list port: 54389, o ip então é adicionado a uma segunda lista: port:1763 com timeout também de 10s.
- ✓ Se dentro dos próximos 10s, houver outra conexão com destino a porta 34576 e o ip de origem já estiver na address-list port:176 , o ip então é adicionado a uma terceira lista: secure, com timeout de 1h.

Técnica de Port Knocking – Exemplo 3

- ✓ Exemplo RouterOS, liberar apenas VPN IPSec.
- ✓ Ao "bater" na porta 54389, o ip de origem da conexão é Adicionado a uma lista chamada port: 54389 com um timeout de 10s.
- ✓ Se dentro destes 10s, houver outra conexão com destino a porta 1763 e o ip de origem já estiver na address-list port: 54389, o ip então é adicionado a uma segunda lista: port:1763 com timeout também de 10s.
- ✓ Se dentro dos próximos 10s, houver outra conexão com destino a porta 34576 e o ip de origem já estiver na address-list port:176 , o ip então é adicionado a uma terceira lista: secure, com timeout de 1h.
- ✓ Que por sua vez, será a lista utilizada nas liberação das portas utilizadas para estabelecer a VPN.

Técnica de Port Knocking – Exemplo 3

- ✓ Utilizando o port knocking dessa maneira, será necessário que a rede que o cliente receba, quando conectado na VPN, esteja em uma address list utilizada na liberação de input.

Técnica de Port Knocking – Exemplo 3

✓ Exemplo RouterOS, VPN L2TP IPSec

```
/ip firewall filter
add action=add-src-to-address-list address-list=port:54389 address-list-timeout=10s chain=\
   input dst-port=54389 protocol=tcp

add action=add-src-to-address-list address-list=port:1763 address-list-timeout=10s chain=\
   input dst-port=1763 protocol=tcp src-address-list=port:54389

add action=add-src-to-address-list address-list=secure address-list-timeout=1h chain=input \
   dst-port=34576 protocol=tcp src-address-list=port:1763

add action=accept chain=input dst-port=500,1701,4500 protocol=udp src-address-list=secure
add action=accept chain=input protocol=ipsec-esp src-address-list=secure
add action=accept chain=input src-address-list=management_network
add action=drop disable=yes chain=input
```

Técnica de Port Knocking – Exemplo 3

✓ Exemplo RouterOS, VPN L2TP IPSec

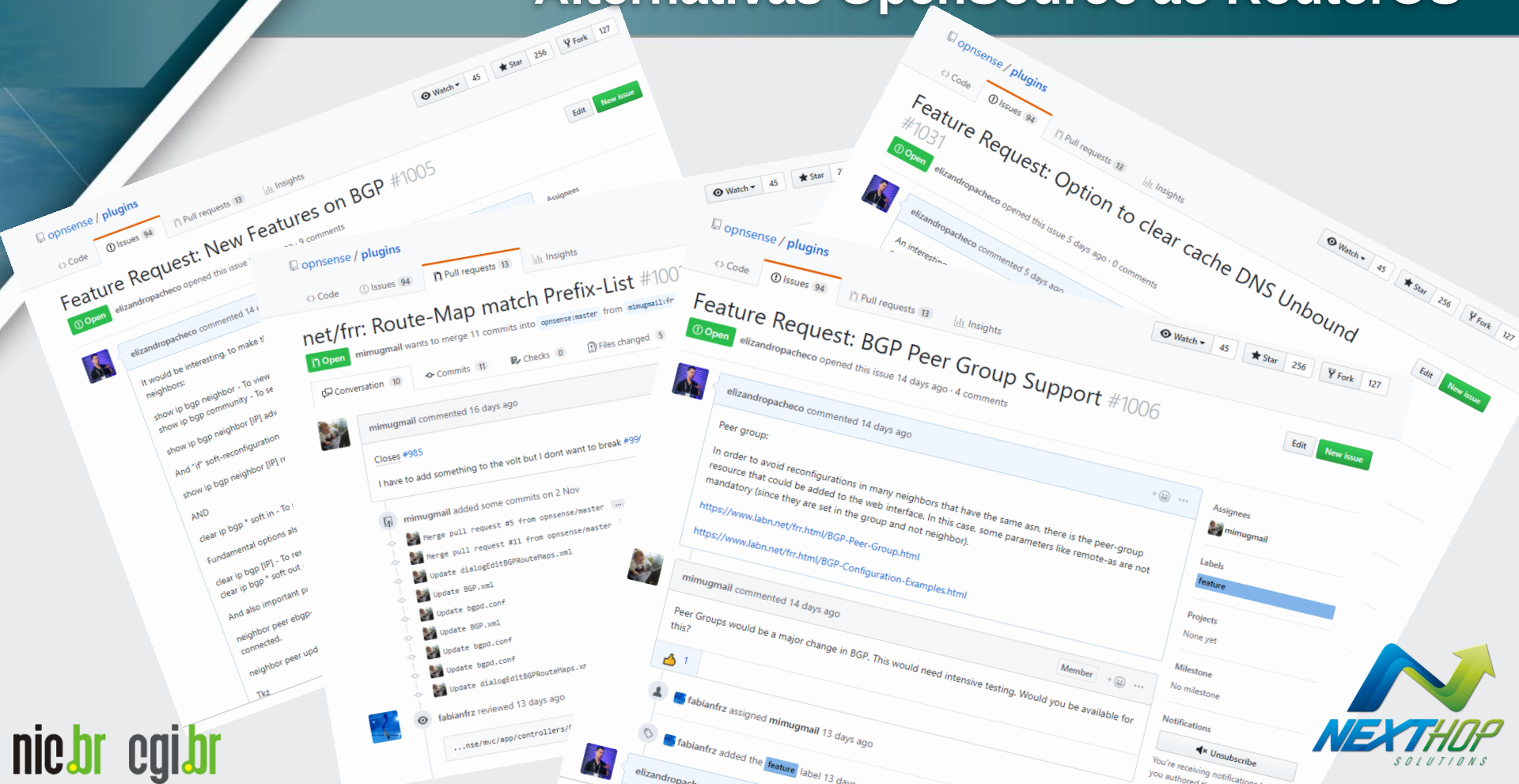
```
/ip firewall address-list
add address=100.70.1.0/24 list=management_network

/ip pool
add name=pool_vpn ranges=100.70.1.1-100.70.1.254

/ppp profile
add change-tcp-mss=yes local-address=100.80.1.1 name=profile_vpn remote-address=pool_vpn use-encryption=yes

/interface l2tp-server server
set authentication=mschap2 default-profile=profile_vpn enabled=yes ipsec-secret=Z3719Q use-ipsec=yes
```

Exemplo 3 - Análise

- ✓ Ainda mais restritivo
- ✓ 3 portas para bater
- ✓ Portas fora de sequência
- ✓ Timeout de 10s
- ✓ Libera apenas a possibilidade de estabelecer a VPN

Alternativas OpenSource ao RouterOS

Alternativas OpenSource ao RouterOS

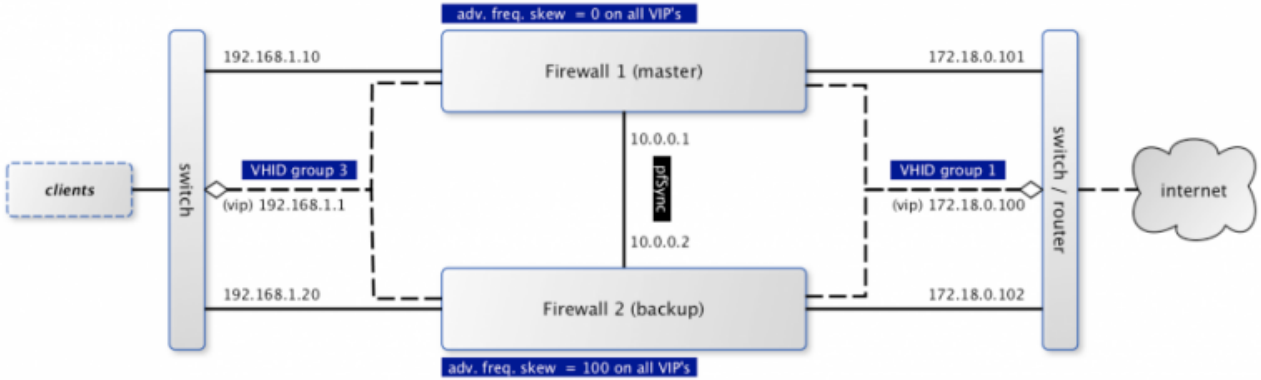


nic.br cgi.br

NEXTHOP SOLUTIONS

High Availability / Hardware Failover

The Common Address Redundancy Protocol or CARP allows for hardware failover. Two or more firewalls can be configured as a failover group. If one interface fails on the primary or the primary goes offline entirely, the secondary becomes active.



Alternativas OpenSource ao RouterOS

https://opnsense.org/

Agradecimentos

Agradecemos, mais uma vez, a oportunidade em compartilharmos um pouco de nosso conhecimento em prol da melhora da Internet no Brasil.

Em especial, ao amigo Rubens Kuhl!

Contatos:
elizandro@nexthop.solutions
vagner@nexthop.solutions
Fone: +55 48 3181-0071

nic.br cgi.br

NEXTHOP SOLUTIONS