EMPRESAS

ATAQUES



Como Economizar Link, Aumentar a Banda dos Clientes e Limpar a Sua Rede.

Prof. Lacier Dias

MUM MIKROTIK USER MEETING

WG WALLED GARDEN

EMPRESAS

ATAQUES



Como Economizar Link, Aumentar a Banda dos Clientes e Limpar a Sua Rede.

Prof. Lacier Dias

MUM MIKROTIK USER MEETING

WG WALLED GARDEN

Como Economizar Link, Aumentar a Banda dos Clientes e Limpar a Sua Rede.

Prof. Lacier Dias



WALLED GARDEN



Prof. Lacier Dias

Formado em Segurança da Informação
Pós-Graduado em Segurança de Rede de Computadores
MBA em Gerenciamento de Projetos – FGV

Alguns dos Treinamentos e Certificações:
IPv6.br, MTCIPv6E e IPv6.br,
MikroTik Consultant, MTCNA, MTCWE, MTCTCE, MTCUME, MTCRE e MTCINE;
ITIL, Cobit, BSC;
ISO 27001 e 27002;
Motorola e UBNT;
Allied Telesis, Cisco e Juniper;
Hughes Networks.

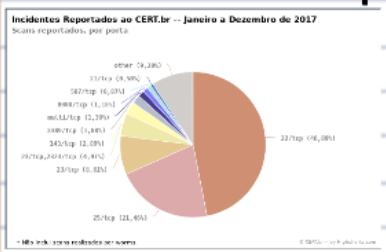
solintel MOGA Telecom VLSM

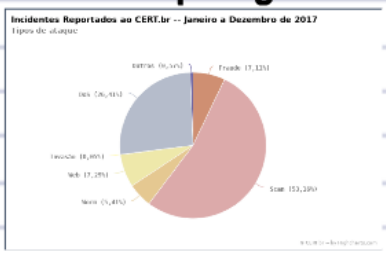




Infraestrutura

A infraestrutura do seu provedor está protegida?





DDoS

Ataques DDoS acima de 500 Gbps se intensificam após Rio 2016, aponta Embratel

Operadora responsável pela rede do evento avalia que os jogos adiantaram o alto volume desse tipo de ameaça.

Durante palestra realizada hoje (27/10) no Gartner Symposium/ITXPO 2016, Mario Rachid, diretor executivo de Soluções Digitais da Embratel, revelou que os jogos Olímpicos Rio 2016 mudou o padrão de ataques de negação de serviço (DDoS) no Brasil. Segundo dados da operadora, a média volumétrica dos ataques era de 30 Gbps entre janeiro e julho deste ano. Em agosto, quando começou o evento, a média passou para 500 Gbps, com a rede sendo atacada diariamente por volumes entre 500 e 600 Gbps.

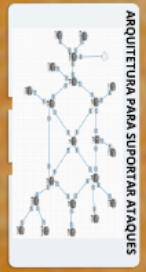


Rachid diz que os hackers já vinham se preparando para

https://ipnews.com.br/ataques-ddos-acima-de-500-gbps-se-intensificam-apos-rio-2016-aponta-embratel/

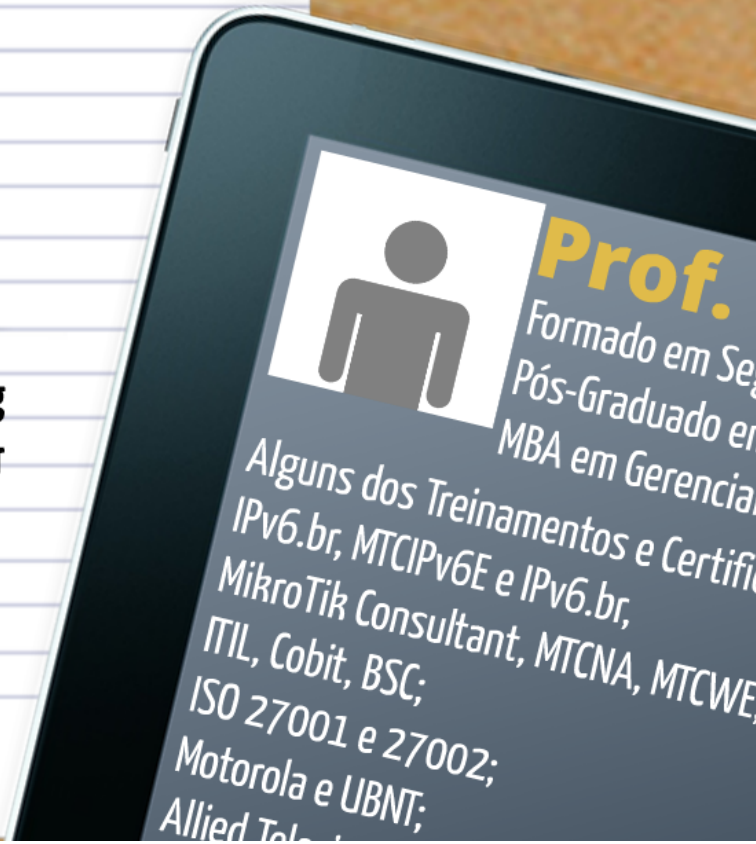
O Brasil atualmente está em 8° lugar no ranking de países vulneráveis com um potencial de gerar ataques DDoS da ordem de 144 Tbit/S:

Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	Open CLDAP/LDAP	DDOS Potential Tbit/sec	DDOS Rank
United States	3,047,504	1,945,745	409,036	120,040	6,455	1,188	1
China	3,026,790	1,494,500	159,037	129,836	3,512	1,033	2
Italy	229,295	769,506	104,012	47,151	5,536	143	3
Russian Federation	329,190	529,279	108,142	248,762	13,71	135	4
South Korea	220,662	362,975	388,726	116,127	12,089	126	5
Germany	215,448	331,305	24,271	7,916	1,067	105	6
France	167,626	104,520	50,646	4,424	473	87	7
Brazil	220,064	93,147	107,434	51,001	760	84	8
United Kingdom	208,428	214,857	41,242	5,717	455	79	9
Netherland	22,772	224,454	18,525	1,787	106	68	10
Japan	130,487	182,884	42,639	42,638	598	59	11



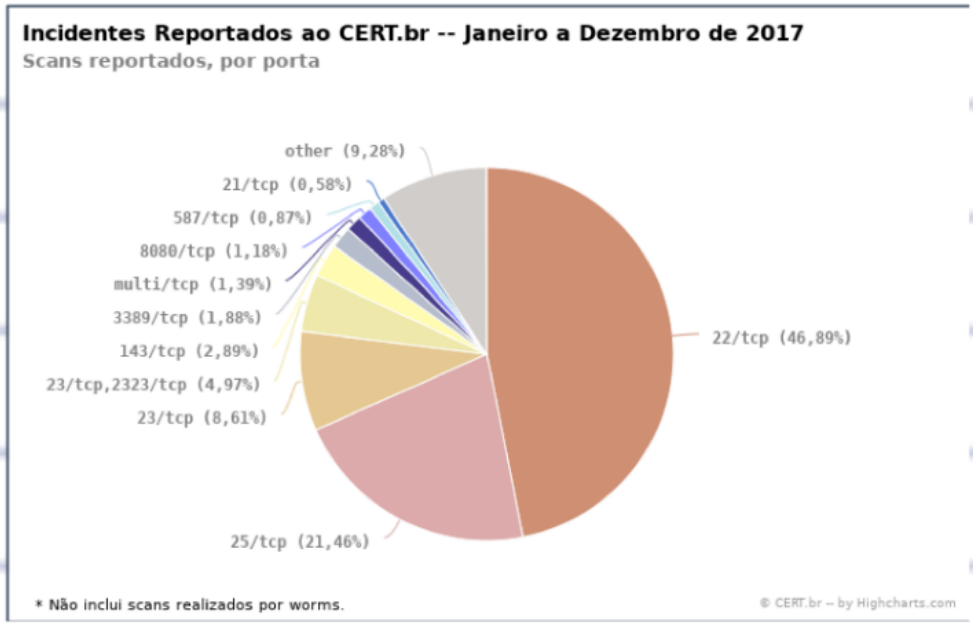


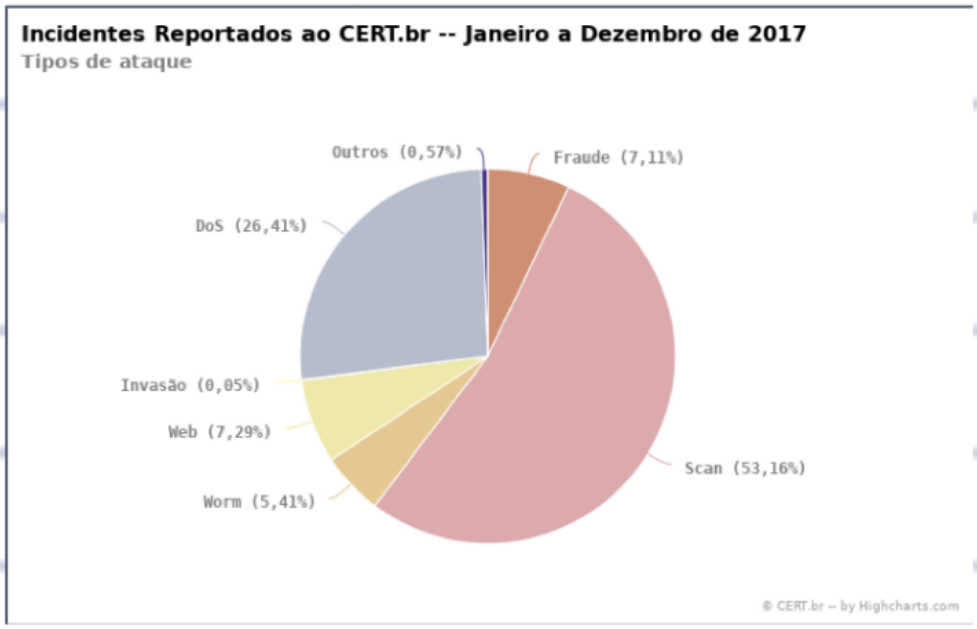




Infraestrutura

A infraestrutura do seu provedor está protegida?





DDoS

Ataques DDoS acima de 500 Gbps se intensificam após Rio 2016, aponta Embratel

* Não inclui scans realizados por worms.

© CERT.br -- by Highcharts.com

DDoS

Ataques DDoS acima de 500 Gbps se intensificam após Rio 2016, aponta Embratel

João Monteiro 27/10/2016 ataque volumétrico, DDoS, Embratel, Jogos Olímpicos, Mario Rachid, negação de serviço, olimpíada, Rio 2016, Segurança

Operadora responsável pela rede do evento avalia que os Jogos adiantaram o alto volume desse tipo de ameaça.



Durante palestra realizada hoje (27/10) no Gartner Symposium/ITXPO 2016, Mario Rachid, diretor executivo de Soluções Digitais da Embratel, revelou que os Jogos Olímpicos Rio 2016 mudou o padrão de ataques de negação de serviço (DDoS) no Brasil. Segundo dados da operadora, a média volumétrica dos ataques era de 30 Gbps entre janeiro e julho deste ano. Em agosto, quando começou o evento, a média passou para 500 Gbps, com a rede sendo atacada diariamente por volumes entre 500 e 600 Gbps.

Rachid diz que os hackers já vinham se preparando para

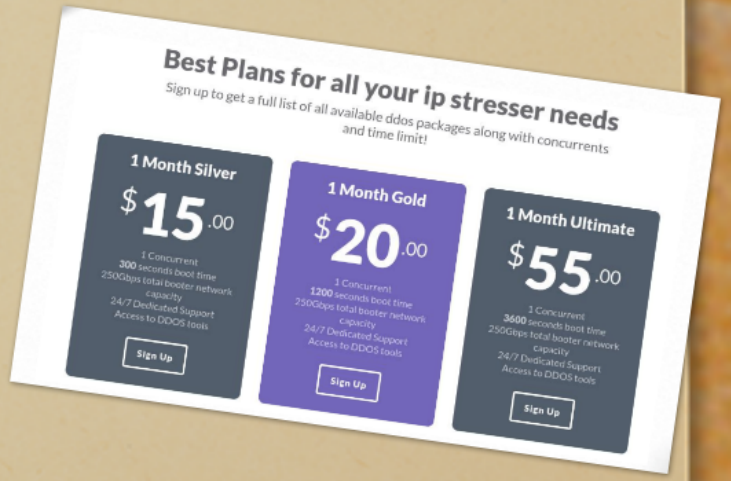
https://ipnews.com.br/ataques-ddos-acima-de-500-gbps-se-intensificam-apos-rio-2016-aponta-embratel/

O Brasil atualmente está em 8° lugar no ranking de países vulneráveis com um potencial de gerar ataques DDoS da ordem de 144 Tbit/S:

Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	Open CHARGEN	DDOS Potential TBit/sec	DDOS Rank
United States	2,067,384	1,965,745	409,086	130,840	6,455	1,188	1
China	2,031,792	1,694,503	152,883	129,936	2,512	1,033	2
Italy	229,295	769,505	136,312	47,151	6,538	443	3
Russian Federation	329,190	525,279	103,142	248,762	1,171	315	4
South Korea	210,552	352,973	388,736	116,139	12,083	216	5
Germany	215,440	351,103	24,271	7,910	1,057	205	6
France	267,626	314,330	50,646	4,624	473	187	7
Brazil	220,384	231,867	587,689	51,081	780	144	8
United Kingdom	202,428	214,937	41,242	3,717	455	129	9
Switzerland	22,772	227,454	18,526	1,739	104	128	10
Japan	130,487	182,881	42,699	42,538	598	109	11

NOVO NOME PARA ATAQUES







Teste de Stress

TRIAL

$4

120 second Stress Tests

1 attack(s) at once

5-10Gbps Stress Tests

Unlimited Stress Tests per day

PURCHASE

BEGINNER

$10

monthly

300 second Stress Tests

1 attack(s) at once

5-10Gbps Stress Tests

Unlimited Stress Tests per day

PURCHASE

STANDARD

$15

monthly

700 second Stress Tests

2 attack(s) at once

5-10Gbps Stress Tests

Unlimited Stress Tests per day

PURCHASE

PLUS

$30

monthly

3600 second Stress Tests

2 attack(s) at once

10+ Gbps Stress Tests

Unlimited Stress Tests per day

PURCHASE

Best Plans for all your ip stresser needs

Sign up to get a full list of all available ddos packages along with concurrents and time limit!

1 Month Silver

$15.00

1 Concurrent
300 seconds boot time
250Gbps total booter network capacity
24/7 Dedicated Support
Access to DDOS tools

Sign Up

1 Month Gold

$20.00

1 Concurrent
1200 seconds boot time
250Gbps total booter network capacity
24/7 Dedicated Support
Access to DDOS tools

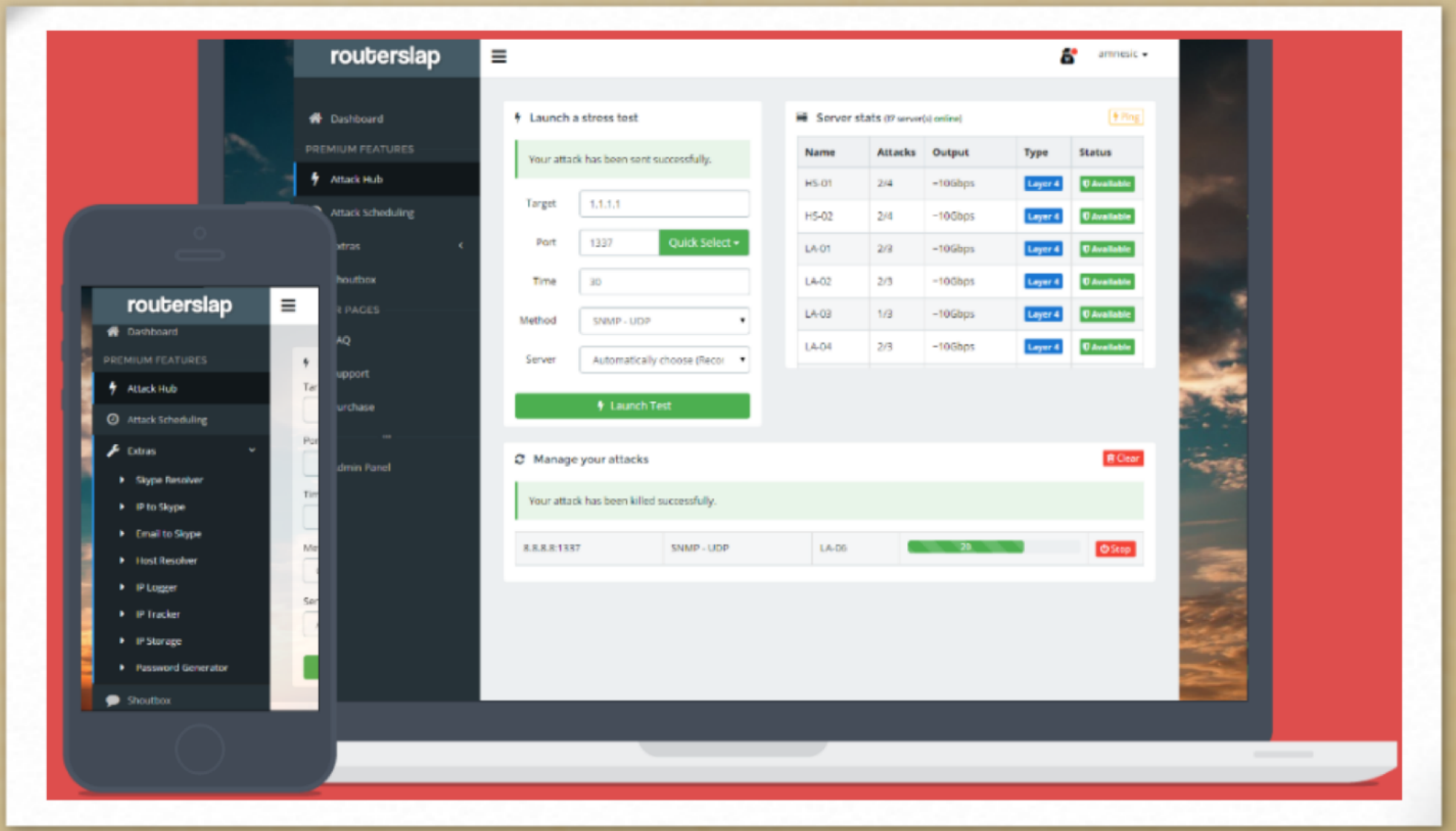
Sign Up

1 Month Ultimate

$55.00

1 Concurrent
3600 seconds boot time
250Gbps total booter network capacity
24/7 Dedicated Support
Access to DDOS tools

Sign Up


routerslap
Dashboard
PREMIUM FEATURES
Attack Hub
Attack Scheduling
Launch a stress test
Your attack has been sent successfully.
Target
1.1.1.1
Port
1337
Quick Select
Time
30
Method
SNMP - UDP
Server
Launch Test
Server stats
Name
Attacks
Output
Type
Status
Manage your attacks
Clear
Your attack has been killed successfully.
Stop
Extras
Skype Resolver
IP to Skype
Email to Skype
Host Resolver
IP Logger
IP Tracker
IP Storage
Password Generator
Shoutbox

Com o que eles atacam?
Equipamentos contaminados:









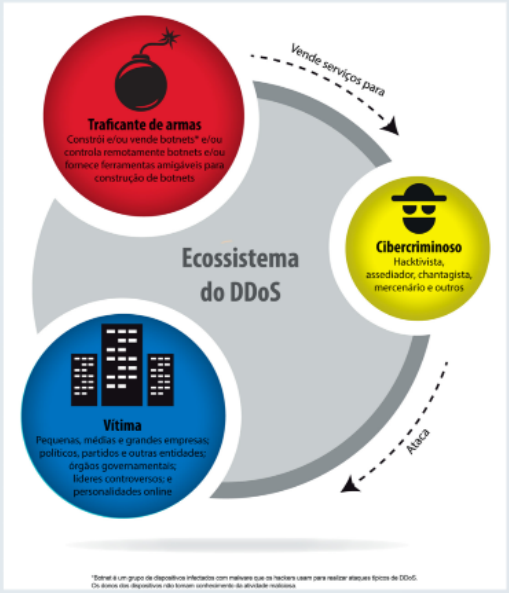


https://www.tecmundo.com.br/malware/114996-smartphones-vendidos-android-contaminado-malware.htm

Seu Android pode não ser ele mesmo. Android são vendidos já contaminado por malware.

- Samsung Galaxy Note 2
- Samsung Galaxy Note 3
- Samsung Galaxy Note 4
- Samsung Galaxy Note 5
- Samsung Galaxy Note 8
- Samsung Galaxy Note Edge
- Samsung Galaxy S4
- Samsung Galaxy S7
- Samsung Galaxy A5
- Samsung Galaxy Tab S2
- Samsung Galaxy Tab 2
- LG G4
- Xiaomi Mi 4i
- ZTE x500
- Google Nexus 5
- Google Nexus 5X
- Oppo N3
- Vivo X6 plus
- ASUS Zenfone 2
- Lenovo S90
- OppoR7 plus
- Xiaomi Redmi
- Lenovo A850

COMO FUNCIONA O DINHEIRO





Traficante de armas

Constrói e/ou vende botnets* e/ou controla remotamente botnets e/ou fornece ferramentas amigáveis para construção de botnets


Cibercriminoso
Hacktivista,
assediador, chantagista,
mercenário e outros


Vítima
Pequenas, médias e grandes empresas;
políticos, partidos e outras entidades;
órgãos governamentais;
líderes controversos; e
personalidades online

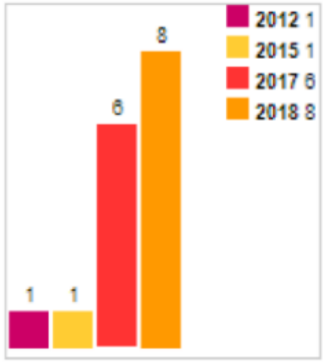
Você acredita que sua infraestrutura está realmente segura?



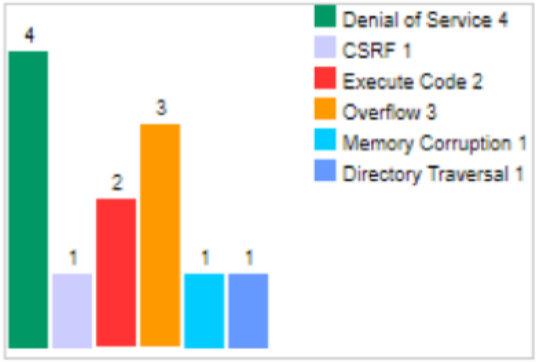
Roteadores



Vulnerabilities By Year



Vulnerabilities By Type



MikroTik

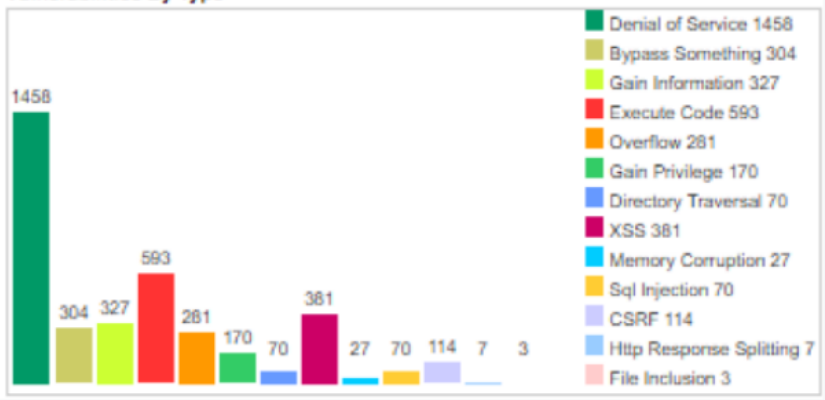
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2012	1	1													1
2015	1												1		
2017	6	3													
2018	8		2	3	1			1							
Total	16	4	2	3	1			1					1		1
% Of All		25.0	12.5	18.8	6.3	0.0	0.0	6.3	0.0	0.0	0.0	0.0	6.3	0.0	

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	21	3								2	2				
2000	16	6	4	3						3	1	1			
2001	55	24	2					1		7	2	3			
2002	65	34	6	8			1	1		2	3	3			
2003	27	14	4	4						1	3	7			
2004	36	24	2	2	1					1		1			
2005	54	33	4	4	1		1			11	3	3			
2006	69	17	10	6			6			10	3	5			
2007	111	51	16	13	1	1	7			9	10	12			1
2008	90	58	15	8	2	1	3			6	7	2	1		
2009	109	62	12	8	1		12	5		8	9	2	5		3
2010	155	82	13	7	1	3	8	3	1	15	10	5	1		4
2011	167	92	37	12	2	4	5	4		13	7	6	2		9
2012	160	93	31	29	3	2	6	1	2	6	8	2	3		
2013	433	185	47	50	7	8	49	14		26	35	30	17		4
2014	368	146	37	20	6	12	38	9		22	43	14	11		
2015	490	188	47	8		14	59	4	2	47	57	17	34	2	
2016	353	118	46	28	2	9	46	7		40	32	12	8		
2017	491	107	103	48		10	78	13	1	39	62	17	10	1	
2018	424	121	153	23		6	57	8	1	36	30	28	22		
2019	5		4				5								
Total	3699	1458	593	281	27	70	381	70	7	304	327	170	114	3	21
% Of All		39.4	16.0	7.6	0.7	1.9	10.3	1.9	0.2	8.2	8.8	4.6	3.1	0.1	

CISCO™

Vulnerabilities By Type

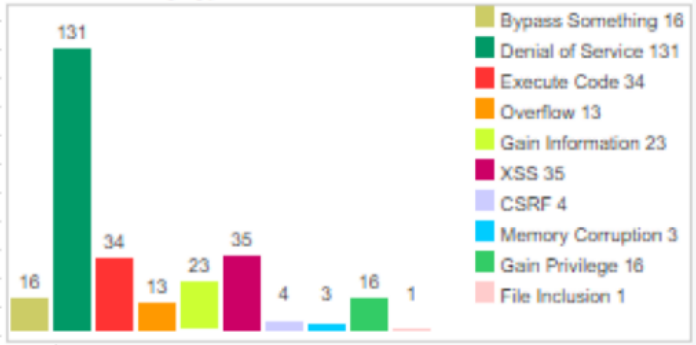


Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2001	1									1					
2002	4	3	1	1											
2003	1	1													
2004	5	4									1				
2005	3	2	1								1				
2006	4	1	1	1			1								
2007	2	1	1	1											
2008	4	1					1			1	1				
2009	4						4								
2010	3		1	1			1								
2011	1						1								
2013	27	8	3	2			7			2	3		1		
2014	47	22	2	1	1		6			1	2	4			
2015	32	16	3	2			1			3	1	3			
2016	21	13	1							1	2	4			
2017	86	33	14	4			9			3	8	3	3		
2018	53	25	6		2		4			4	4	2		1	
2019	1	1													
Total	299	131	34	13	3		35			16	23	16	4	1	1
% Of All		43.8	11.4	4.3	1.0	0.0	11.7	0.0	0.0	5.4	7.7	5.4	1.3	0.3	

Juniper® NETWORKS

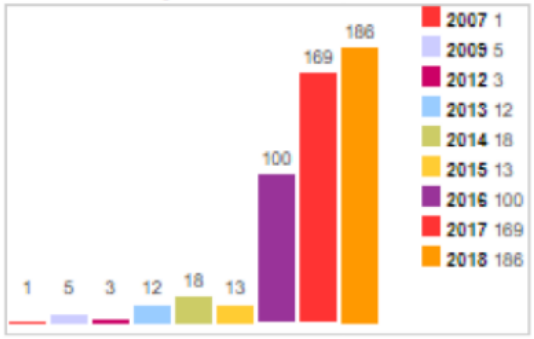
Vulnerabilities By Type



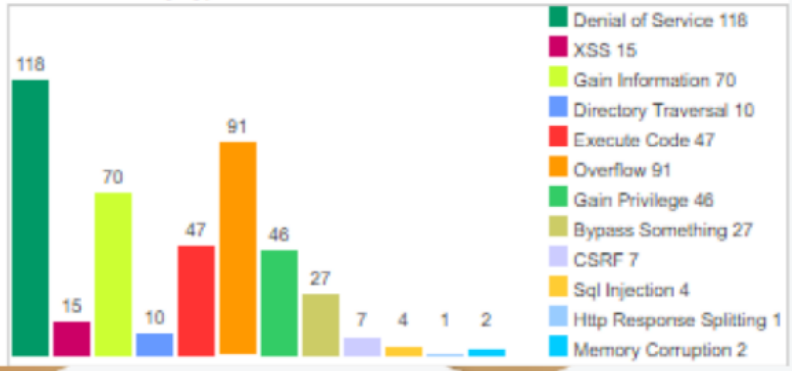
Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2007	1	1													
2009	5						1				2				2
2012	3	1						1			1				
2013	12	2	3	5							2	2			2
2014	18	6	3	4			3			2	1		3		
2015	13	6		1			1	2		1	2	1			
2016	100	53	14	18		1	5	1	1	3	14	21	1		
2017	169	26	17	19	2	2	4	4		8	27	22	3		
2018	186	23	10	44		1	1	2		13	21				
Total	507	118	47	91	2	4	15	10	1	27	70	46	7		4
% Of All		23.3	9.3	17.9	0.4	0.8	3.0	2.0	0.2	5.3	13.8	9.1	1.4	0.0	

Vulnerabilities By Year



Vulnerabilities By Type



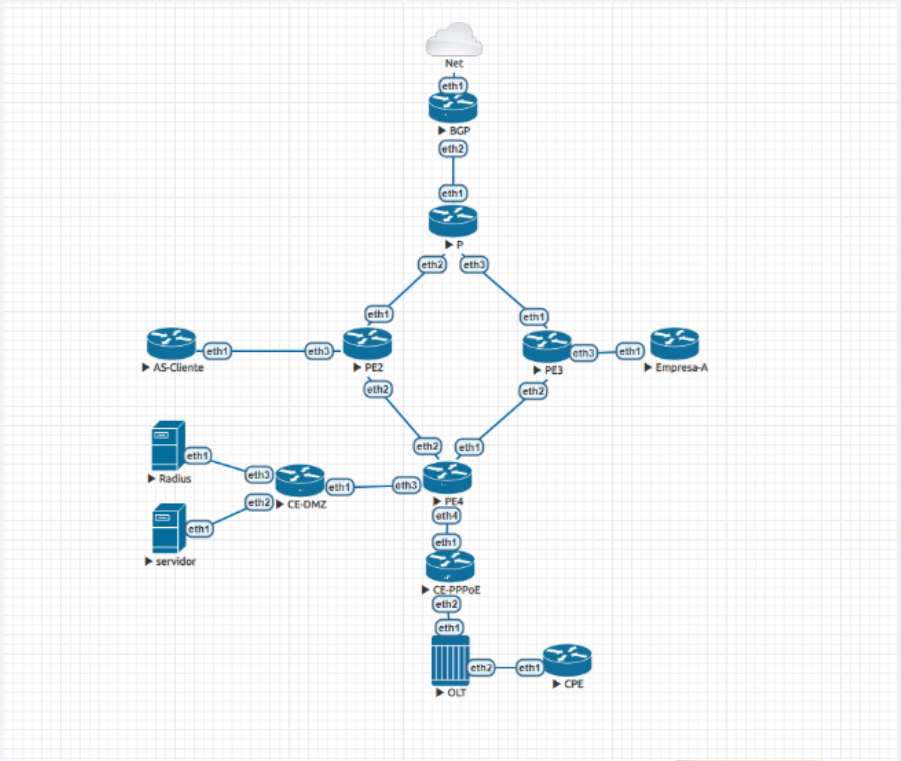
HUAWEI

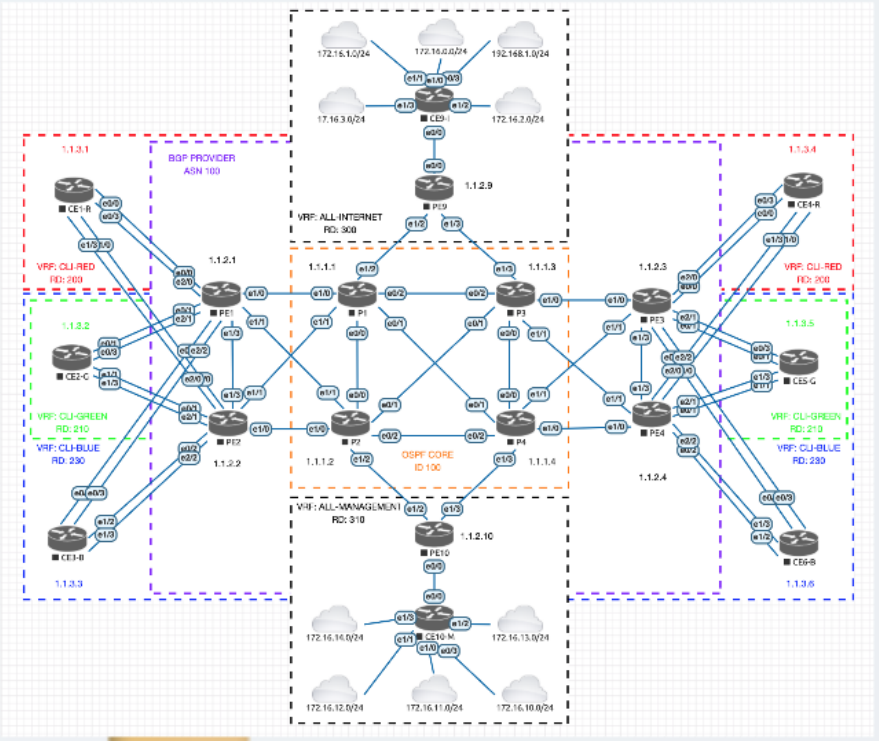
SE OS PRINCIPAIS ROTEADORES DO MERCADO TEM BUGS COMO SE PROTEGER?



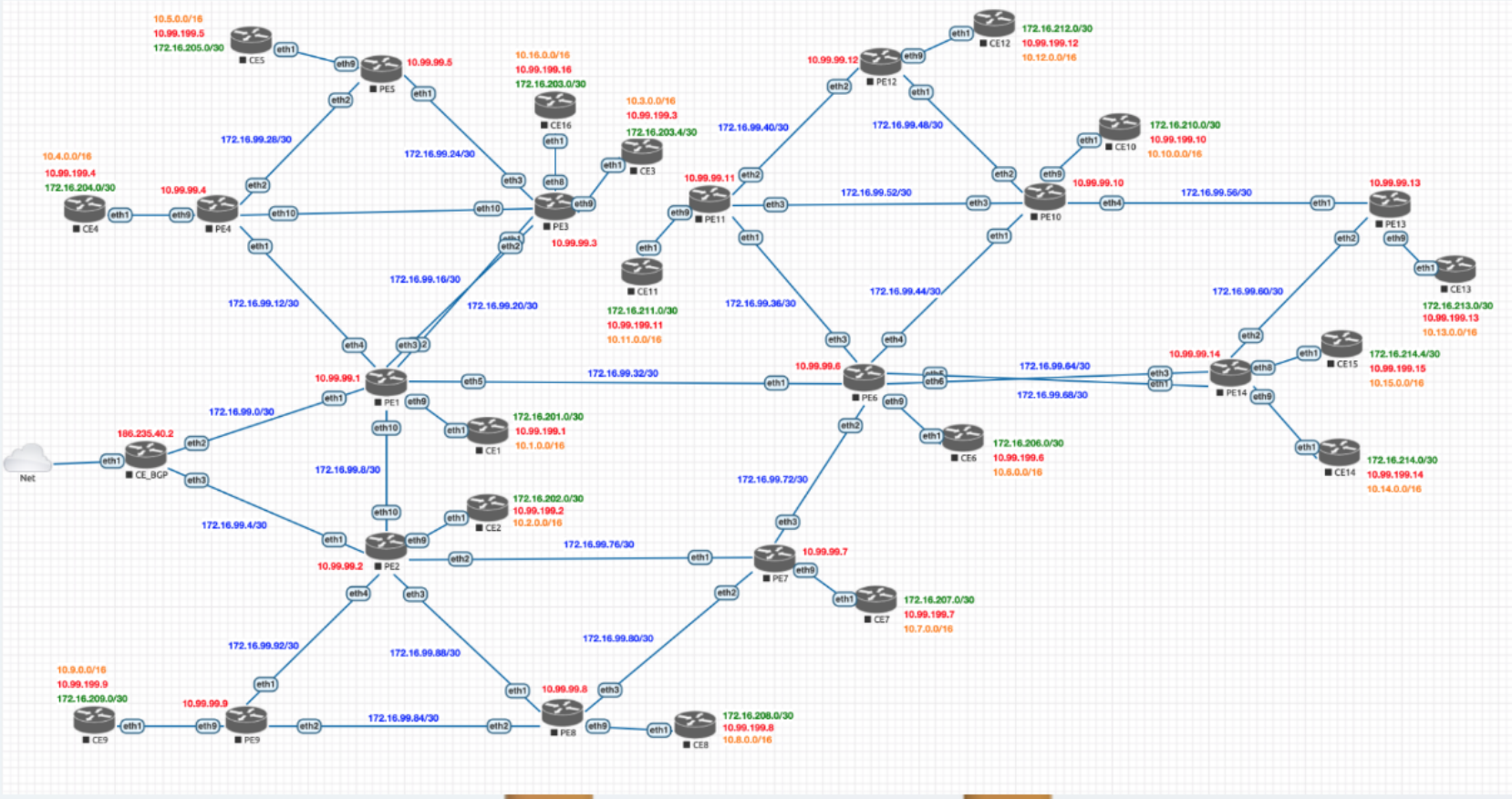

ARQUITETURA
DE
REDE

ARQUITETURA PARA SUPORTAR ATAQUES

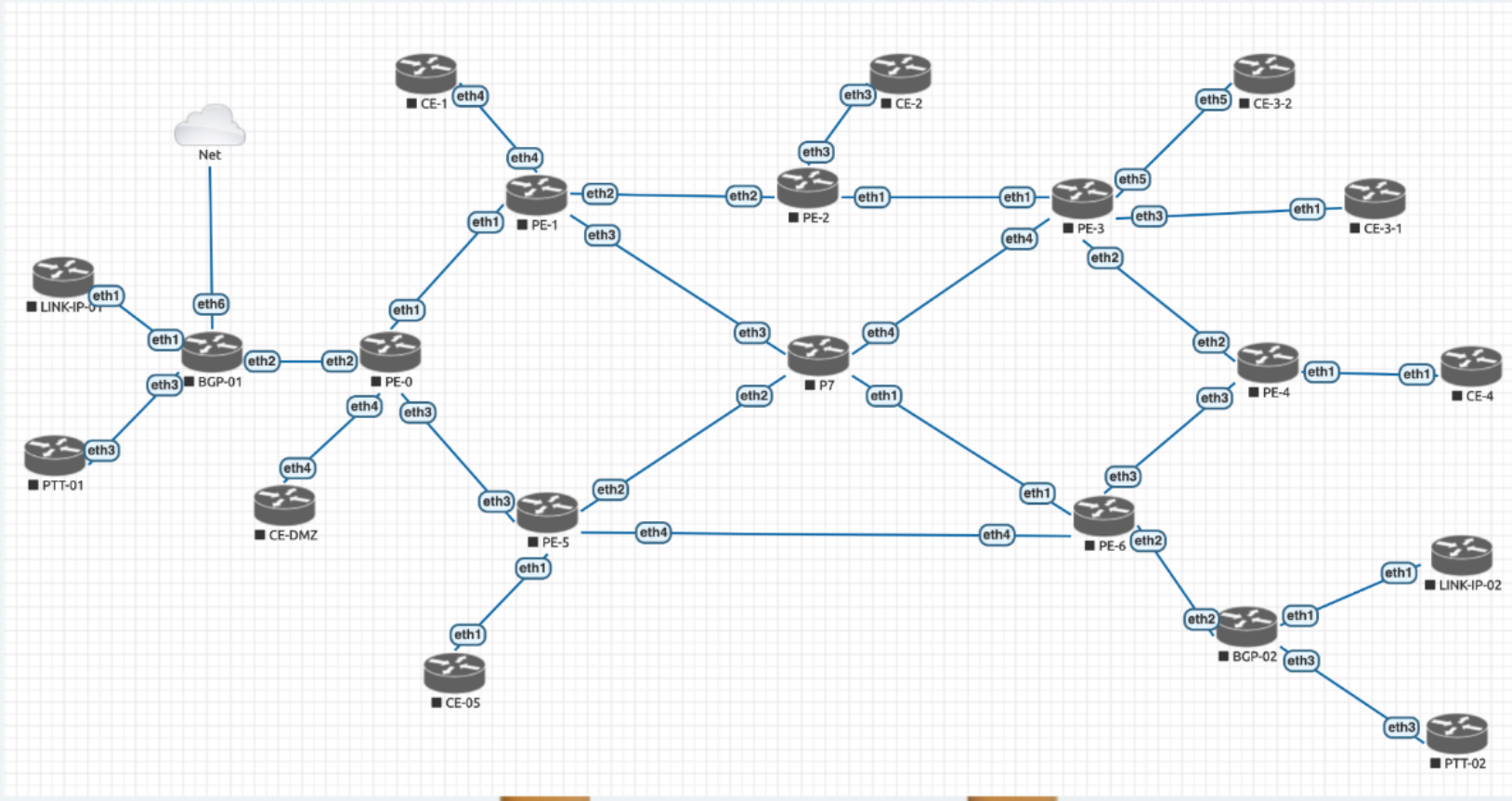


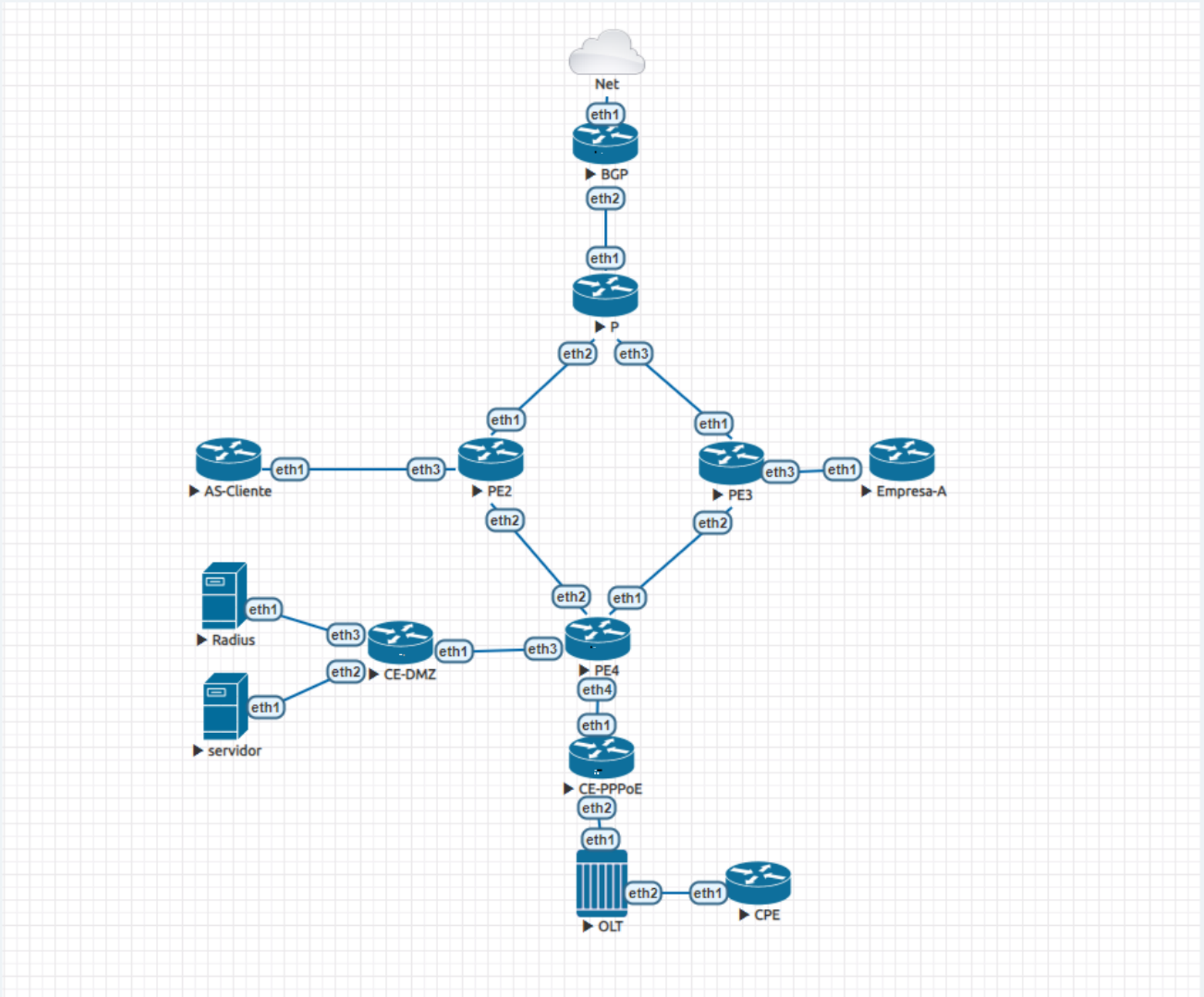


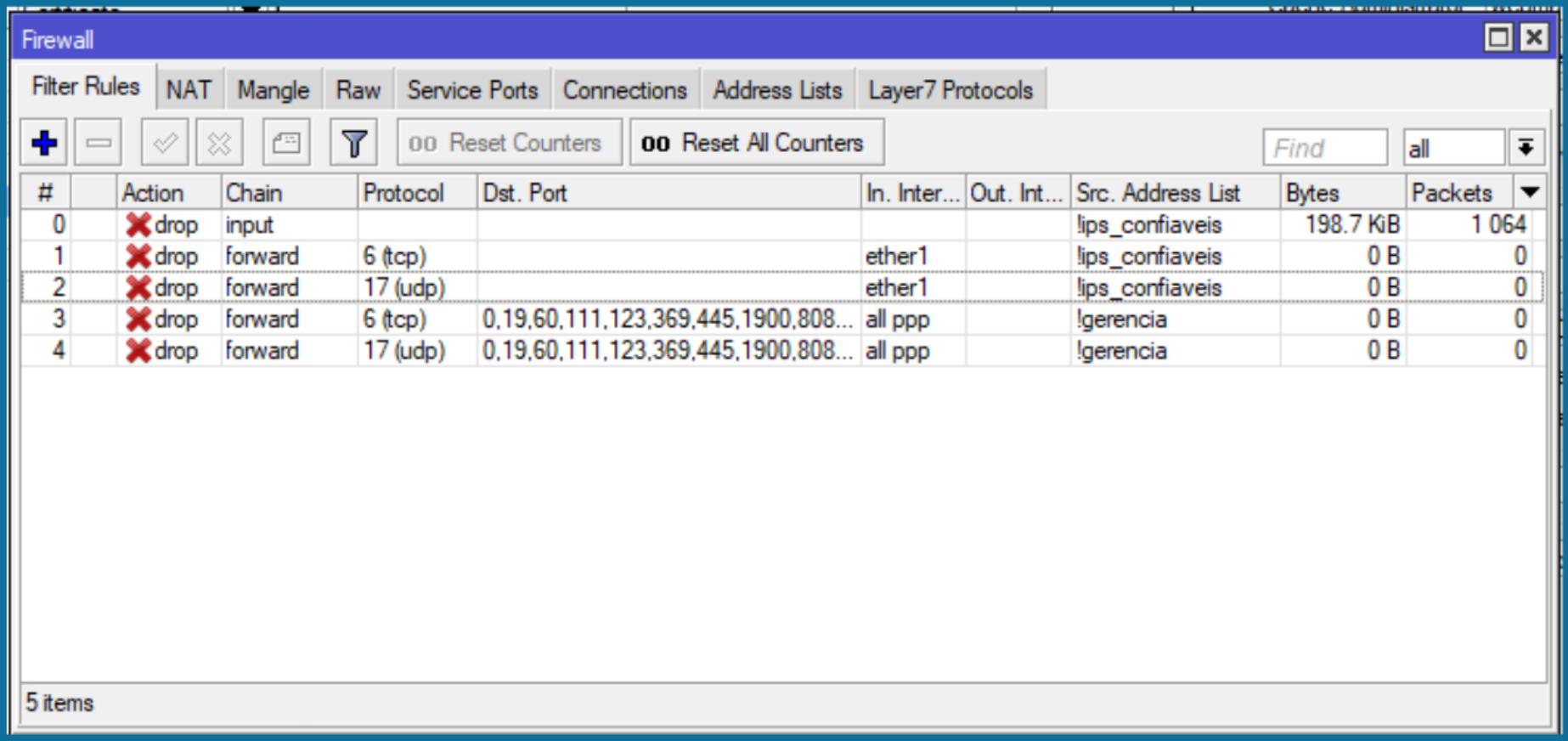
ARQUITETURA PARA SUPORTAR ATAQUES

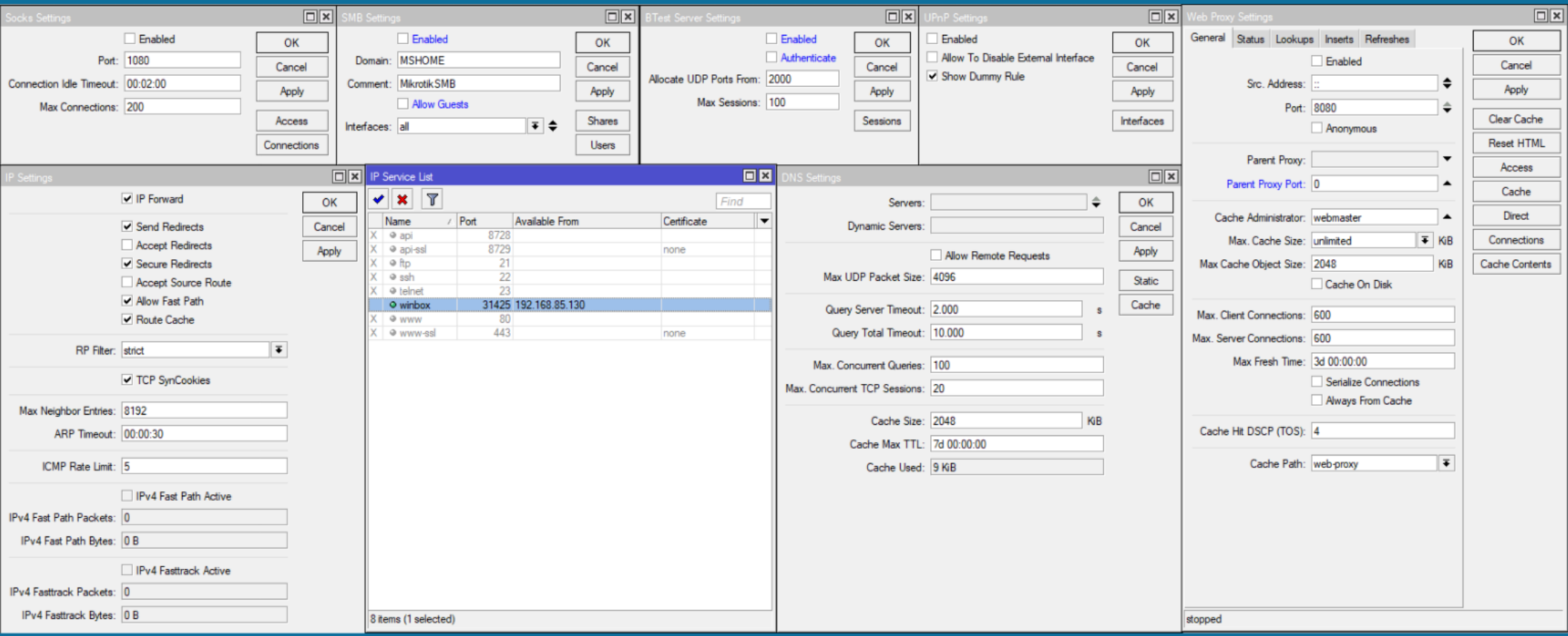


ARQUITETURA PARA SUPORTAR ATAQUES

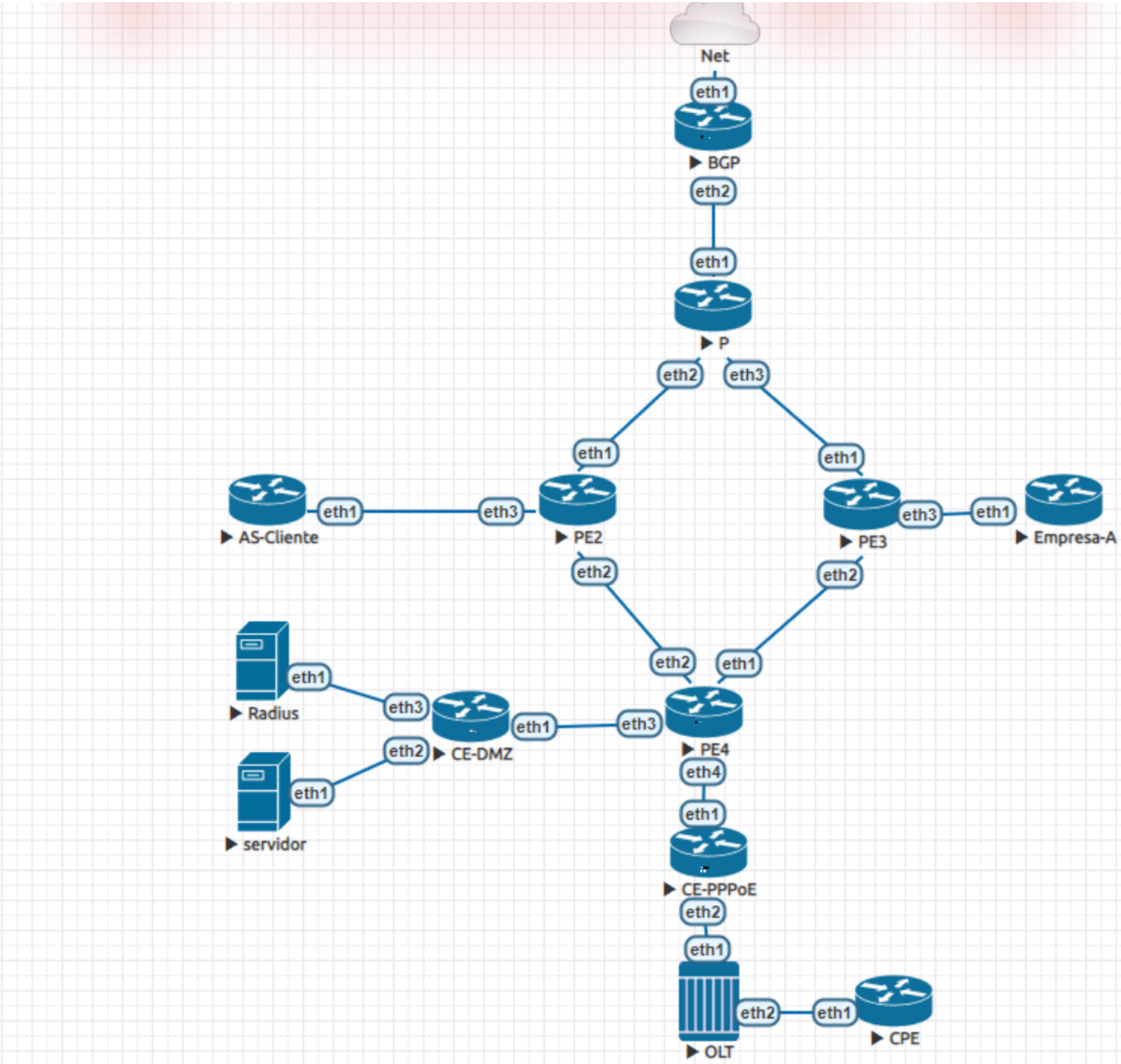


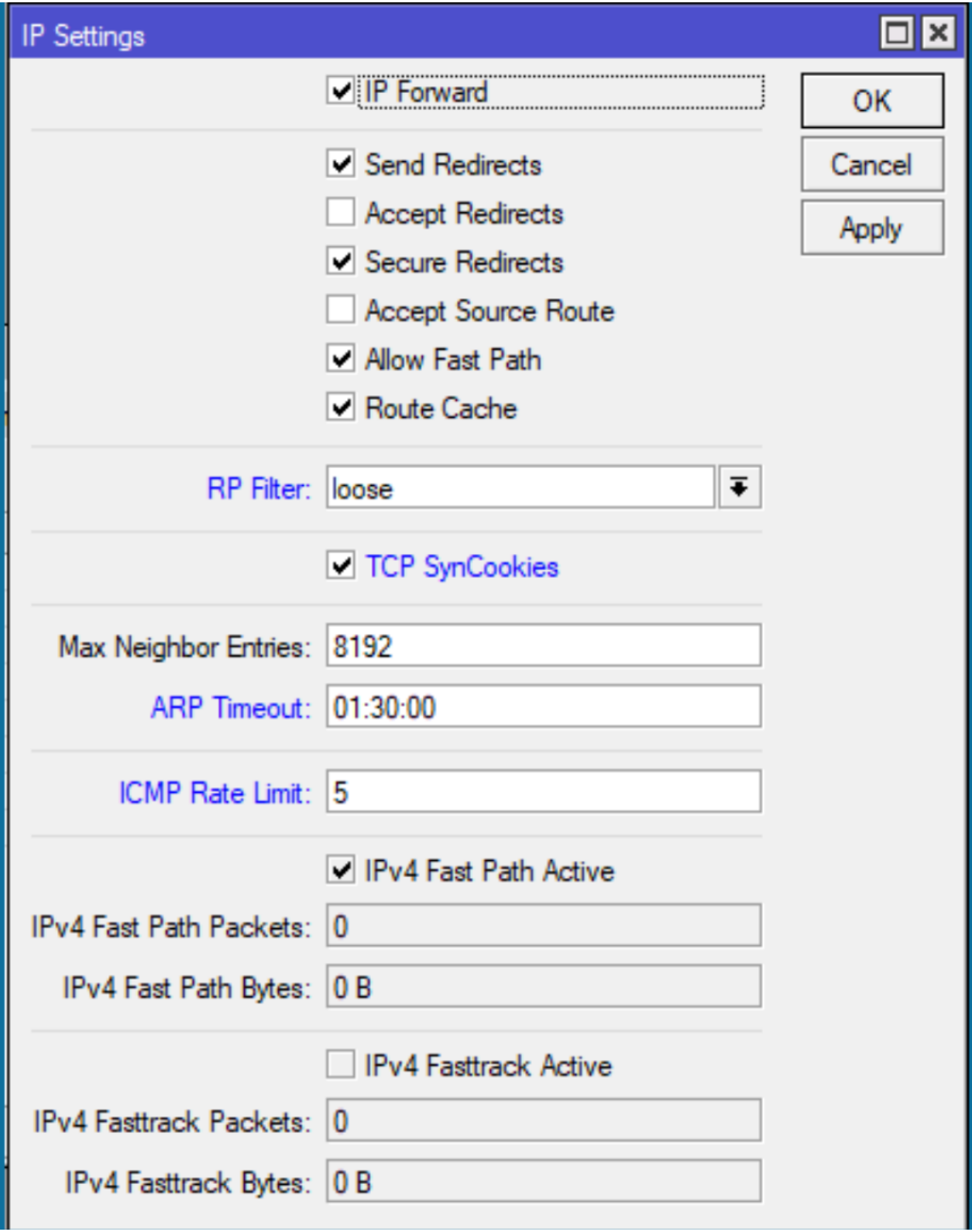

Net
eth1
BGP
eth2
eth1
P
eth2
eth3
eth1
eth1
AS-Cliente
eth1
eth3
PE2
eth3
eth1
PE3
Empresa-A
eth2
eth2
eth2
eth1
Radius
eth1
eth3
CE-DMZ
eth1
eth3
PE4
eth2
eth4
servidor
eth1
eth1
CE-PPPoE
eth2
eth1
eth2
eth1
OLT
CPE

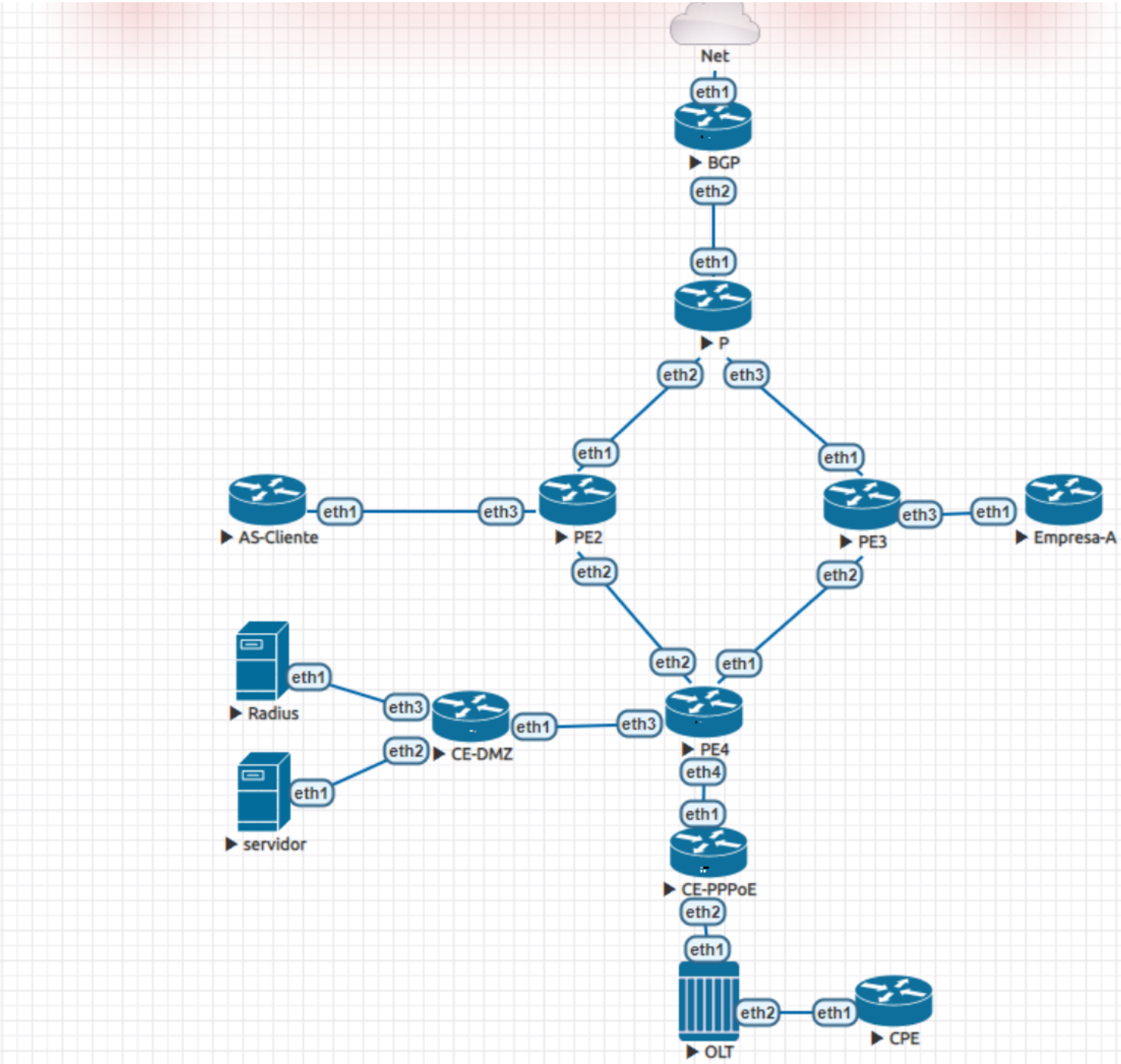

Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
00 Reset Counters
00 Reset All Counters
Find
all
Action Chain Protocol Dst. Port In. Inter... Out. Int... Src. Address List Bytes Packets
0 drop input !ips_confiaveis 198.7 KiB 1 064
1 drop forward 6 (tcp) ether1 !ips_confiaveis 0 B 0
2 drop forward 17 (udp) ether1 !ips_confiaveis 0 B 0
3 drop forward 6 (tcp) 0,19,60,111,123,369,445,1900,808... all ppp !gerencia 0 B 0
4 drop forward 17 (udp) 0,19,60,111,123,369,445,1900,808... all ppp !gerencia 0 B 0
5 items

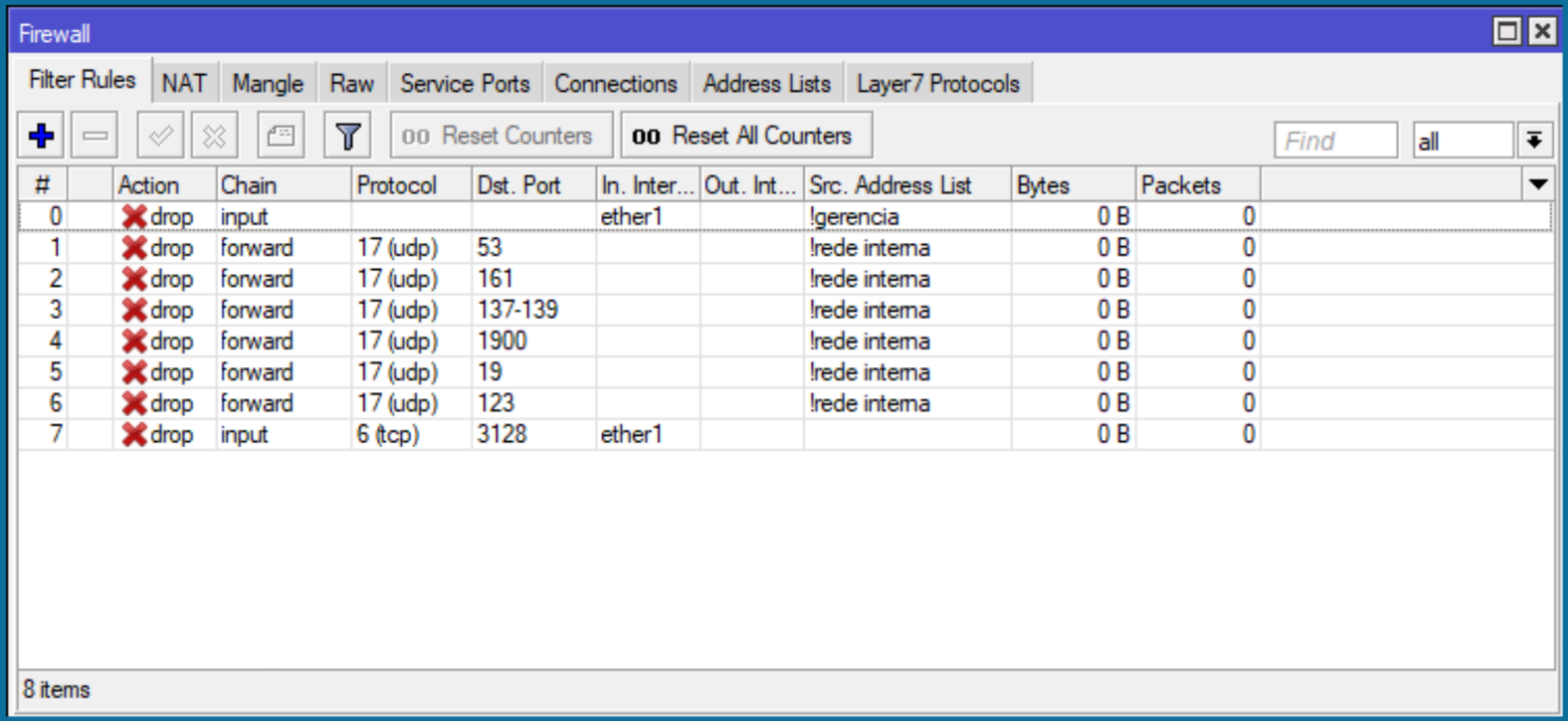


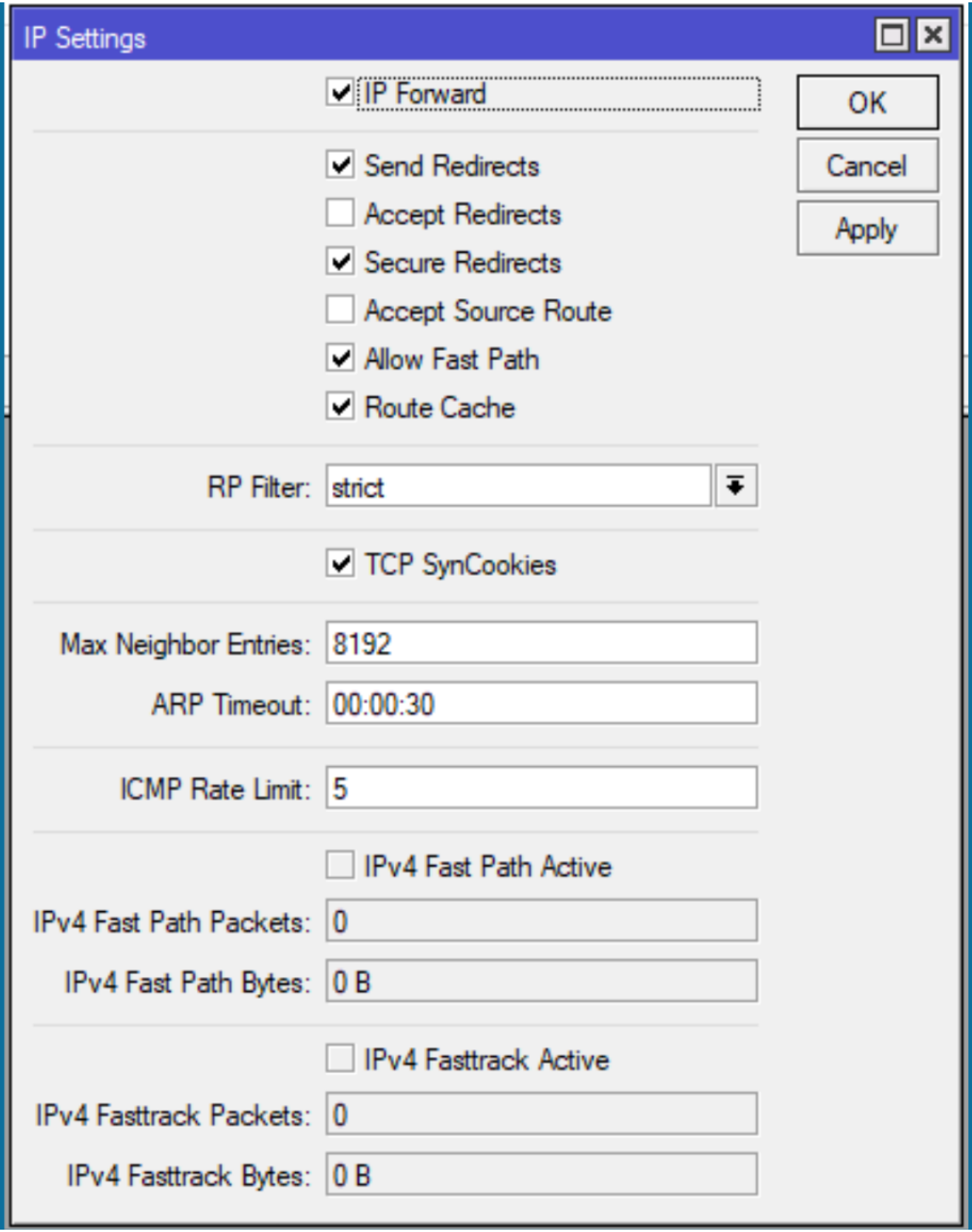

```
traffic classifier bloqueios-pppoe-in operator or
```

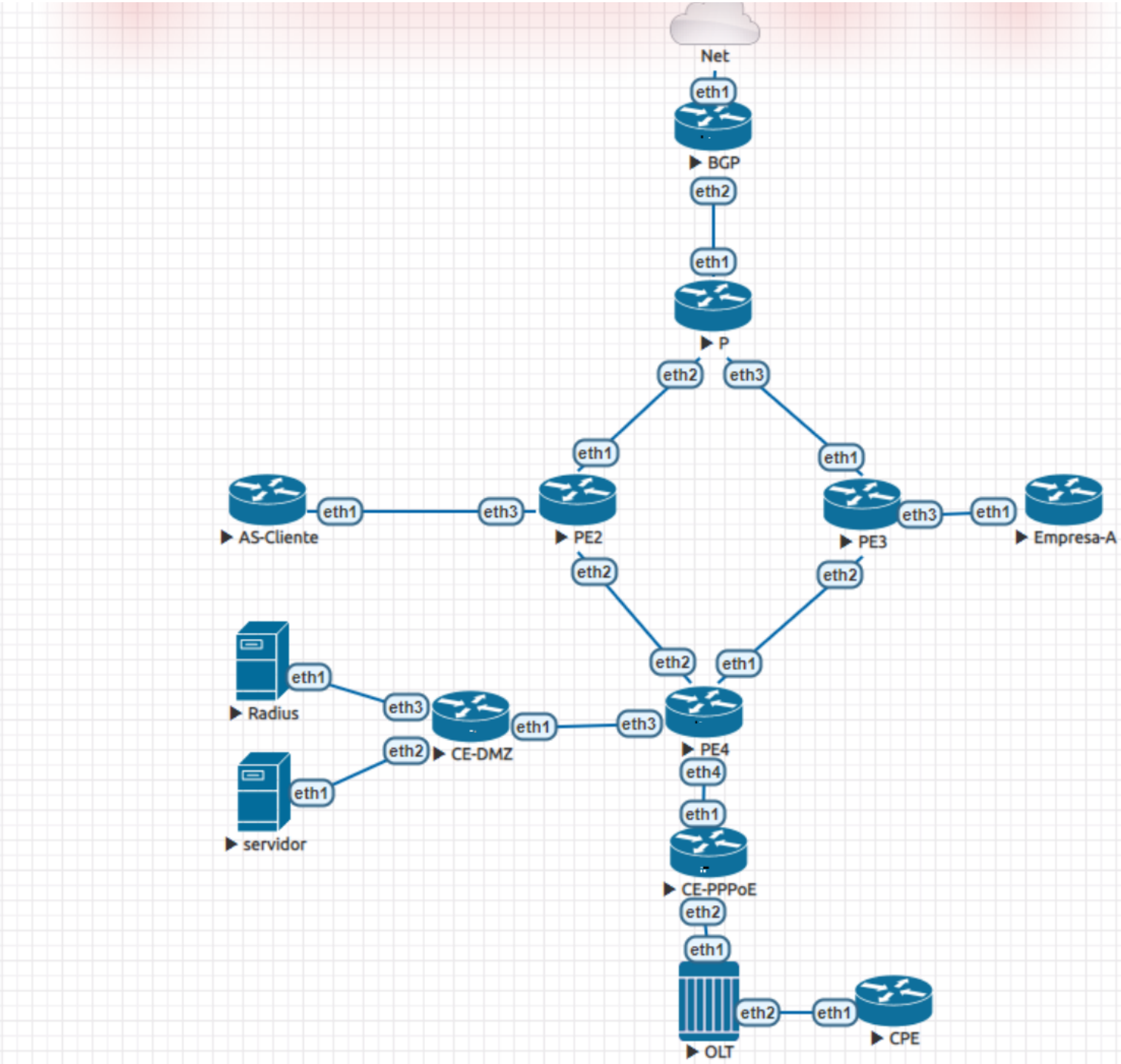

Net
eth1
BGP
eth2
eth1
P
eth2
eth3
eth1
eth1
AS-Cliente
eth1
eth3
PE2
eth3
eth1
PE3
eth1
Empresa-A
eth2
eth2
eth2
eth1
Radius
eth1
eth3
CE-DMZ
eth1
eth3
PE4
eth2
eth4
eth1
servidor
eth1
CE-PPPoE
eth2
eth1
eth2
eth1
OLT
CPE

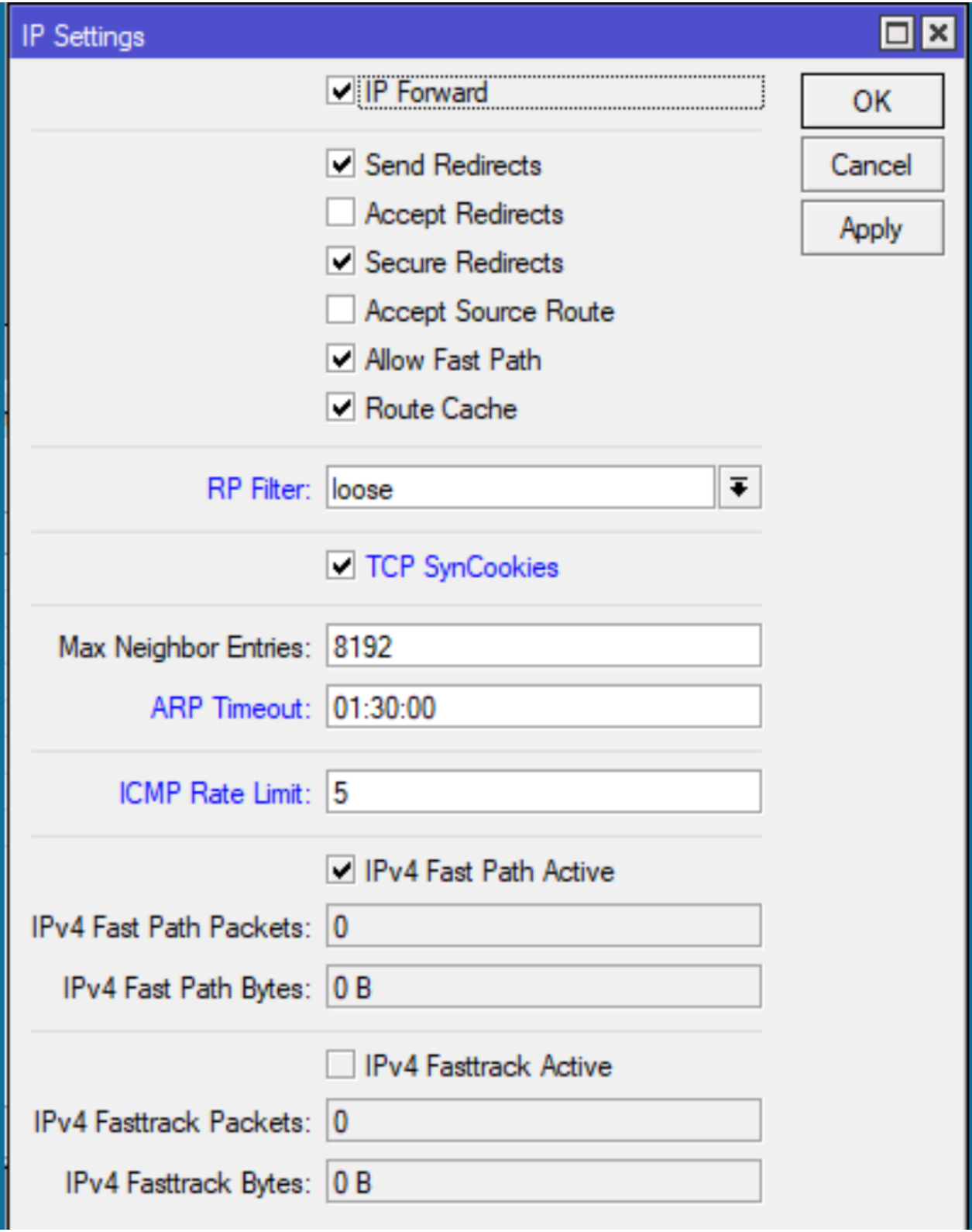

IP Settings
IP Forward
OK
Cancel
Apply
Send Redirects
Accept Redirects
Secure Redirects
Accept Source Route
Allow Fast Path
Route Cache
RP Filter:
loose
TCP SynCookies
Max Neighbor Entries:
8192
ARP Timeout:
01:30:00
ICMP Rate Limit:
5
IPv4 Fast Path Active
IPv4 Fast Path Packets:
0
IPv4 Fast Path Bytes:
0 B
IPv4 Fasttrack Active
IPv4 Fasttrack Packets:
0
IPv4 Fasttrack Bytes:
0 B


Net
eth1
BGP
eth2
eth1
P
eth2
eth3
eth1
eth1
AS-Cliente
eth1
eth3
PE2
eth3
eth1
PE3
eth1
Empresa-A
eth2
eth2
eth2
eth1
Radius
eth1
eth3
CE-DMZ
eth1
eth3
PE4
eth2
eth4
eth1
servidor
eth1
CE-PPPoE
eth2
eth1
eth2
eth1
OLT
CPE


Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Protocol Dst. Port In. Inter... Out. Int... Src. Address List Bytes Packets
0 drop input ether1 !gerencia 0 B 0
1 drop forward 17 (udp) 53 !rede interna 0 B 0
2 drop forward 17 (udp) 161 !rede interna 0 B 0
3 drop forward 17 (udp) 137-139 !rede interna 0 B 0
4 drop forward 17 (udp) 1900 !rede interna 0 B 0
5 drop forward 17 (udp) 19 !rede interna 0 B 0
6 drop forward 17 (udp) 123 !rede interna 0 B 0
7 drop input 6 (tcp) 3128 ether1 0 B 0
8 items


IP Settings
IP Forward
OK
Cancel
Apply
Send Redirects
Accept Redirects
Secure Redirects
Accept Source Route
Allow Fast Path
Route Cache
RP Filter:
strict
TCP SynCookies
Max Neighbor Entries:
8192
ARP Timeout:
00:00:30
ICMP Rate Limit:
5
IPv4 Fast Path Active
IPv4 Fast Path Packets:
0
IPv4 Fast Path Bytes:
0 B
IPv4 Fasttrack Active
IPv4 Fasttrack Packets:
0
IPv4 Fasttrack Bytes:
0 B


Net
eth1
BGP
eth2
eth1
P
eth2
eth3
eth1
eth1
AS-Cliente
eth1
eth3
PE2
eth3
eth1
PE3
eth1
Empresa-A
eth2
eth2
eth2
eth1
Radius
eth1
eth3
CE-DMZ
eth1
eth3
PE4
eth2
eth4
eth1
servidor
eth1
CE-PPPoE
eth2
eth1
eth2
eth1
OLT
CPE


IP Settings
IP Forward
Send Redirects
Accept Redirects
Secure Redirects
Accept Source Route
Allow Fast Path
Route Cache
RP Filter:
loose
TCP SynCookies
Max Neighbor Entries:
8192
ARP Timeout:
01:30:00
ICMP Rate Limit:
5
IPv4 Fast Path Active
IPv4 Fast Path Packets:
0
IPv4 Fast Path Bytes:
0 B
IPv4 Fasttrack Active
IPv4 Fasttrack Packets:
0
IPv4 Fasttrack Bytes:
0 B
OK
Cancel
Apply





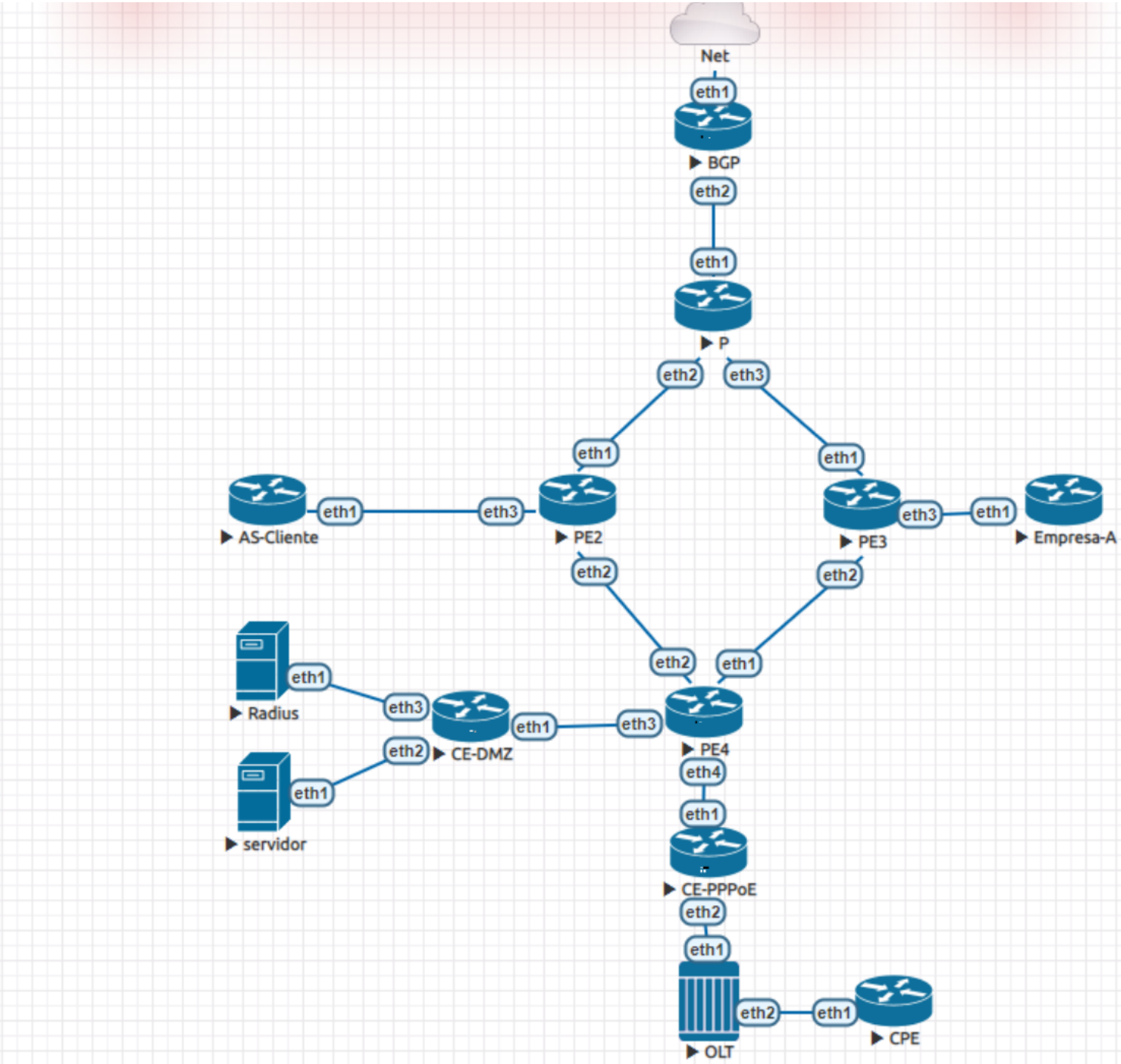
MANRS

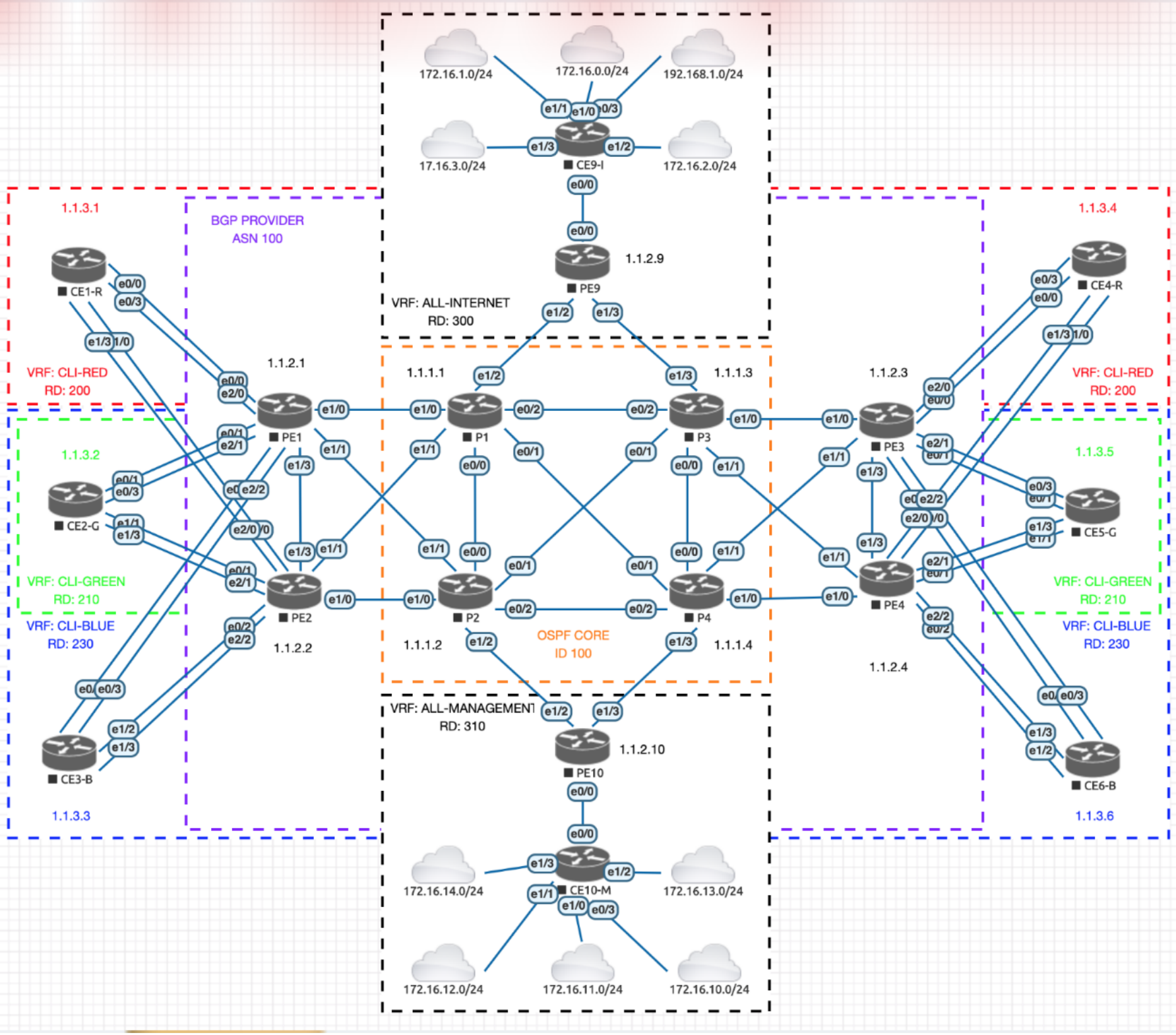




BGPmon




Net
eth1
BGP
eth2
eth1
P
eth2
eth3
eth1
eth1
AS-Cliente
eth1
eth3
PE2
eth3
eth1
PE3
eth1
Empresa-A
eth2
eth2
eth2
eth1
Radius
eth1
eth3
CE-DMZ
eth1
eth3
PE4
eth2
eth4
eth1
servidor
eth1
CE-PPPoE
eth2
eth1
eth2
eth1
OLT
CPE


172.16.1.0/24
172.16.0.0/24
192.168.1.0/24
17.16.3.0/24
CE9-I
172.16.2.0/24
1.1.2.9
PE9
VRF: ALL-INTERNET
RD: 300
1.1.3.1
BGP PROVIDER
ASN 100
1.1.3.4
CE1-R
CE4-R
VRF: CLI-RED
RD: 200
1.1.2.1
1.1.1.1
1.1.1.3
1.1.2.3
PE1
P1
P3
PE3
1.1.3.2
1.1.3.5
CE2-G
CE5-G
VRF: CLI-GREEN
RD: 210
VRF: CLI-BLUE
RD: 230
PE2
P2
P4
PE4
1.1.2.2
1.1.1.2
OSPF CORE
ID 100
1.1.1.4
1.1.2.4
CE3-B
CE6-B
1.1.3.3
1.1.3.6
VRF: ALL-MANAGEMENT
RD: 310
1.1.2.10
PE10
CE10-M
172.16.14.0/24
172.16.13.0/24
172.16.12.0/24
172.16.11.0/24
172.16.10.0/24

Se arquitetura é uma peça do quebra cabeça o que mais podemos fazer?



Como está a saúde da sua infraestrutura?




Existem empresas trabalhando para ajudar com estes problemas.
ICANN | ISPCP
Internet Service Providers & Connectivity Providers
WALLED GARDEN
TEAM CYMRU
MOGA

Existem empresas trabalhando para ajudar com estes problemas.

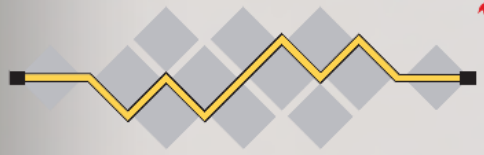


ICANN | ISPCP

Internet Service Providers & Connectivity Providers



WALLED GARDEN











IETF®



MOGA telecom









MANRS









#internet24hs



Normas de Acordo Mútuo para Segurança de Roteamento
https://www.manrs.org/
Objetivos

1. Aumentar a conscientização e incentivar ações, pela demonstração do compromisso crescente do grupo de apoiadores.

2. Promover a cultura de responsabilidade coletiva para a resiliência e segurança do sistema de roteamento global da Internet.

3. Demonstrar a capacidade do setor para abordar questões de resiliência e segurança do sistema de roteamento global da Internet com o espírito da responsabilidade coletiva.

4. Fornecer uma estrutura para que os provedores de acesso à Internet (ISPs) compreendam melhor e ajudem a solucionar problemas relacionados à resiliência e à segurança do sistema de roteamento global da Internet.

Existem empresas trabalhando para ajudar com estes problemas.

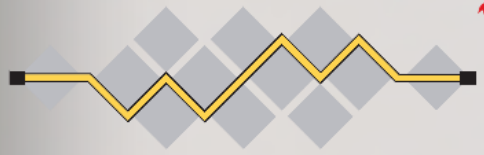


ICANN | ISPCP

Internet Service Providers & Connectivity Providers



WALLED GARDEN











IETF®



MOGA telecom









MANRS









#internet24hs



TEAM CYMRU

Our Insight | Our Initiatives | Dragon News | Who We Are

HOW DO I OBTAIN A PEERING SESSION?

To peer with the bogon route servers, contact bogonrs@cymru.com. When requesting a peering session, please include the following information in your e-mail:

1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4 fullbogons, and/or IPv6 fullbogons)
2. Your AS number
3. The IP address(es) you want us to peer with
4. Does your equipment support MD5 passwords for BGP sessions?
5. Optional: your GPG/PGP public key

We will typically provide multiple peering sessions (at least 2) per remote peer for redundancy. If you would like more or less than 2 sessions please note that in your request. We try to respond to new peering requests within one to two business days, but, again, can provide no guarantees for this free service.

Remember that you must be able to accommodate up to 100 prefixes for traditional bogons, and up to 50,000 prefixes for fullbogons, and be capable of multihop peering with a private ASN. If you improperly configure your peering and route all packets destined for bogon addresses to the bogon route-servers, your peering session will be dropped.

http://www.team-cymru.org/bogon-reference.html

Existem empresas trabalhando para ajudar com estes problemas.

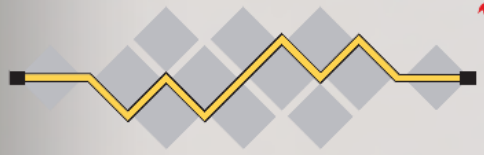


ICANN | ISPCP

Internet Service Providers & Connectivity Providers



WALLED GARDEN











IETF®



MOGA telecom









MANRS









#internet24hs




WALLED GARDEN
WWW.WALLEDGARDEN.GLOBAL
SOBRE A SOLUÇÃO COMO FUNCIONA CONTATO PT EN ES
E-Mail
Nome
Cadastrar
ENTRAR
33 ATAQUES POR SEGUNDO
117.572 POR HORA
84.652.096 POR MÊS
Estes ataques foram registrados na América Latina durante os primeiros oito meses de 2018. Proteja sua rede e seus clientes. Cadastre-se.
CONSULTE SEU NÍVEL DE SEGURANÇA
Digite seu ASN
Ok
INSTITUIÇÃO:
NIVEL DE SEGURANÇA:
WWW.WALLEDGARDEN.GLOBAL


CONSULTE SEU NÍVEL DE SEGURANÇA
Digite seu ASN
Ok
INSTITUIÇÃO:
NIVEL DE SEGURANÇA:
WWW.WALLEDGARDEN.GLOBAL

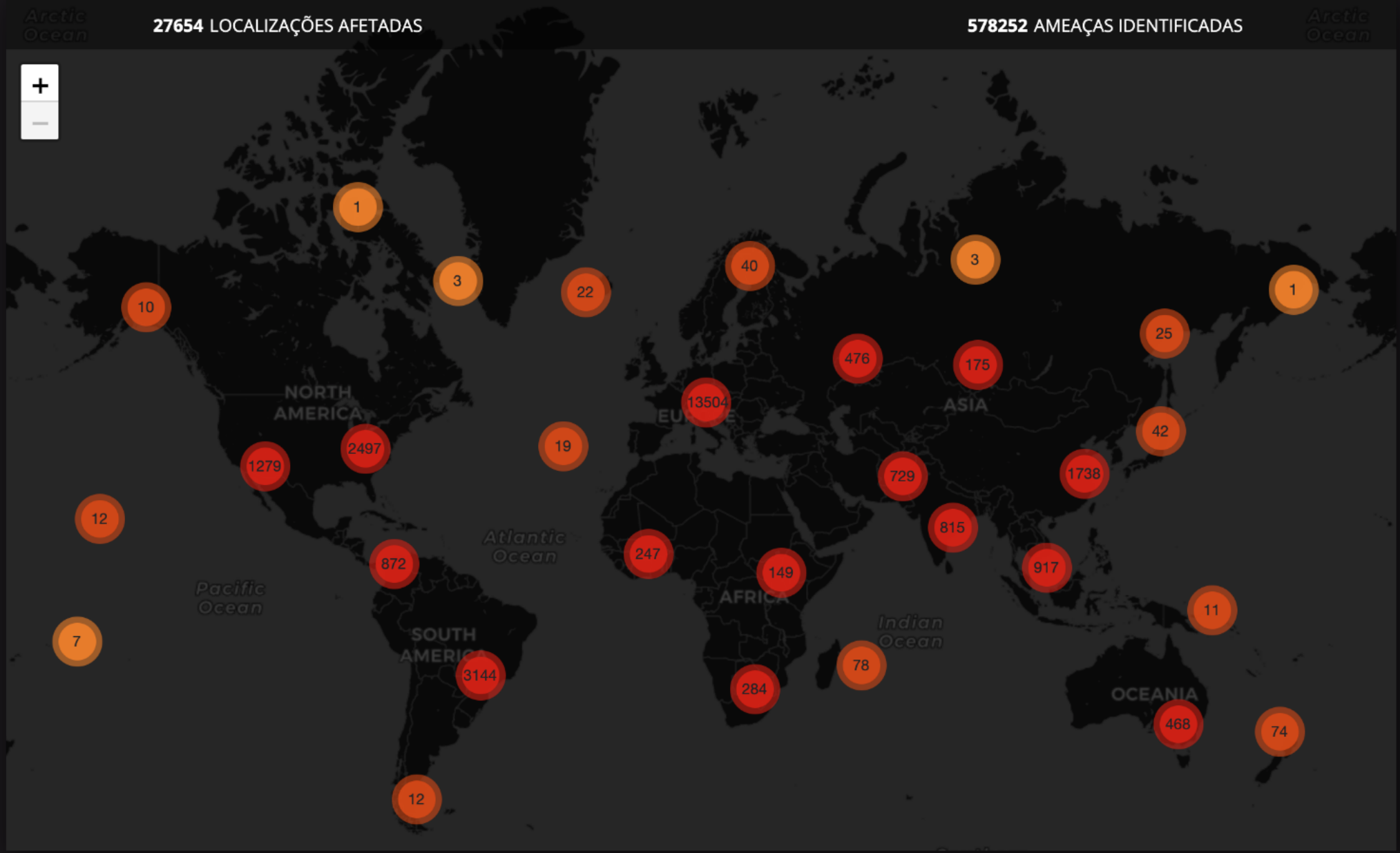
MAPA DE AMEAÇAS

WWW.WALLEDGARDEN.GLOBAL

WALLED GARDEN

27654 LOCALIZAÇÕES AFETADAS

578252 AMEAÇAS IDENTIFICADAS



QUEM SOMOS

WWW.WALLEDGARDEN.GLOBAL

WALLED GARDEN

A Walled Garden é uma ferramenta que agrega diversas estratégias de segurança para proteger sua rede contra milhares de ameaças que a internet possui e que prejudicam a disponibilidade, performance e a confiabilidade do seu serviço.

DE QUAIS AMEAÇAS TE PROTEGEMOS



ROUTE HIJACKING

Um ataque projetado para derrubar uma sessão, ou ainda, mudar rotas usadas pelo peer, a fim de facilitar a espionagem ou a análise de tráfego, causando interrupções graves incluindo perda completa de conectividade.



PHISHING

Captura de informações e dados pessoais importantes através de mensagens falsas. Com isso, é possível conseguir nomes de usuários, senhas, dados de contas bancárias e cartões de crédito.



ROUTE LEAKS

Envolvem anúncios ilegítimos de prefixos de IP que se propagam pela rede e levam a um roteamento comprometido. São, geralmente, inadvertidos e acontecem devido à configurações incorretas do filtro.



IP ADDRESS SPOOFING

Mascarar o endereço de origem permite que vários computadores enviem pacotes fazendo-se passar por um determinado endereço de origem, o que representa uma séria ameaça para os sistemas baseados em autenticação pelo endereço IP.



DDOS

Os Ataques Distribuídos de Negação de Serviços são realizados por um computador mestre que direciona um ataque em massa usando um exército de máquinas infectadas. Este ataque visa tornar um servidor, serviço ou infraestrutura indisponível.



BACKDOOR

Usado para controlar remotamente softwares maliciosos infiltrados nos computadores, celulares e diversos IOTs que serão usados como zumbis para amplificarem a potência dos ataques.

COMO ATUAMOS

WWW.WALLEDGARDEN.GLOBAL

WALLED GARDEN

Walled Garden realiza a validação de diversas fontes confiáveis na qual o sistema está conectado, envia as instruções de roteamento em tempo real via BGP para prevenir que ameaças globais ataquem ou usem para atacar sua rede e seus clientes, oferecendo, ainda, filtragem, bloqueio de vírus, backdoor, worms, spyware, spam, com Atendimento Técnico 24 horas.



SURGE UMA
AMEAÇA NA INTERNET

São muitas as ameaças presentes na internet que trazem risco aos usuários. Vírus, backdoor, worms, spyware, pedofilia, spam, bugs de sistemas, minerador de bitcoin...dentre outros milhares de lixos que são distribuídos via internet



A FONTE DA AMEAÇA
É DETECTADA

Existem diversas entidades, empresas e equipamentos espalhados pelo mundo dedicados de forma séria a higienizar e proteger a internet. Eles detectam esse tráfego malicioso e alimentam a base de dados compartilhada com o Walled Garden.



PROCESSANDO
AS INFORMAÇÕES

O sistema do Walled Garden analisa os dados coletados pelas entidades, empresas e equipamentos espalhados pelo mundo, valida e constrói uma base com alto nível de confiabilidade, composta por milhares de "lixos" que trafegam na internet em tempo real



NEUTRALIZANDO
A AMEAÇA

Ao mesmo tempo, todos os participantes são comunicados via BGP e instantaneamente protegidos contra as ameaças, tornando a ferramenta altamente eficaz, fazendo com que a propagação das ameaças perca forças, sem afetar sua rede e seus clientes.

COMO VOCÊ PODE COLABORAR

Ainda assim existem ataques únicos a sistemas e equipamentos com vulnerabilidades especificas. Caso isso ocorra você não está sozinho: além do suporte 24 horas o participante pode informar através de uma communities especifica seus IPv4 /32 e IPv6 /64 para os roteadores do Walled Garden, que vão informar a toda estrutura de segurança que o Walled Garden faz parte, e conter o encaminhamento do tráfego para este IP, mitigando assim até 95% da potência dos ataques.

Existem empresas trabalhando para ajudar com estes problemas.

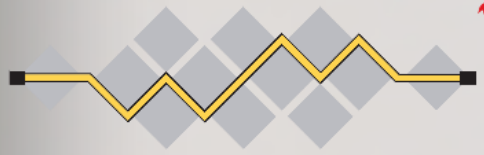


ICANN | ISPCP

Internet Service Providers & Connectivity Providers



WALLED GARDEN











IETF®



MOGA telecom









MANRS









#internet24hs



A segurança da internet é um desafio de todos e ações coletivas tendem a ser mais eficientes em mitigar e resolver problemas.

Contamos com todos para obtermos uma internet cada vez mais limpa.

solintel

MOGA Telecom

VLSM CONSULTORIA E TREINAMENTO

WG WALLED GARDEN

Perguntas?



Obrigado.

Prof. Lacier Dias

lacier@vlsm.com.br

lacier@solintel.com.br

@lacierdias

(43) 99185-5550

lacierdias

@lacierdias

EMPRESAS

ATAQUES



Como Economizar Link, Aumentar a Banda dos Clientes e Limpar a Sua Rede.

Prof. Lacier Dias

MUM MIKROTIK USER MEETING

WG WALLED GARDEN