# WTR X Workshop de Tecnologias de Redes do POP-BA

***Ações de otimização e Boas Práticas para um sistema autônomo***
***Roadmap ITS***

# *Francisco José Badaró Valente Neto*

## Quem Sou ?

- **Mestrando em Sistemas e Computação (*Strictu Sensu*)**
- **MBA em Gestão Política, Planejamento Estratégico e Inteligência Estratégica . MBA em Sistemas e Telecomunicações**
- **Especialista (*Lato Sensu*) em Sistemas e Computação, Especialista (*Lato Sensu*) em Redes e Telecomunicações.**
- **Bacharel em Ciências da Computação**
- **Tecnólogo em Análise e Desenvolvimento de Sistemas**
- **Diversas certificações de diversos fabricantes.**

***- Pesquisador Ativo e Publicador (Redes, Telecomunicações (Otimização e Roteamento)) e Blockchain. Professor UniRuy/Wyden-DeVry e Caelis/São Salvador.***
***- Gerente de Telecomunicações e Treinamento - ITS Brasil***

**https://www.linkedin.com/in/franciscobadaro/en**

**http://lattes.cnpq.br/0008999030113038**

**https://www.researchgate.net/profile/Francisco_Neto24**

# Quem Somos ?

# QUEM SOMOS

Somos a ITS Brasil Telecomunicações, com mais de 15 anos atuando no mercado corporativo, buscamos a qualidade com obstinação, provendo soluções em internet para o mercado corporativo.

Possuímos uma rede de Fibra Óptica DWDM em Anel na sua maior parte, com mais de 1.100 KM, com ampla cobertura.

# QUEM SOMOS

Sistema autônomo (ASN: 28186) de infraestrutura de rede Tier-2 na internet, com plano de otimização contínua focado na melhoria do QoE do assinante.

Alta capacidade de borda, escalar, com interconexões às principais operadoras do mercado nacional, com provimento de transito nacional e internacional. Interconectado (plano contínuo de otimização) com **11 IXs (23/09/2019), sendo o AS com mais interconexões no ESTADO DA BAHIA (excluindo as grandes telco em ação no estado)**

# QUEM SOMOS

Vanguarda em PNI: PNI com Google, Facebook, Verizon/Edgecast.

Conexão direta e privativa com Globo, Netflix e outros grandes players e CDNs através de vlan direta bilateral ou peer direto em IXs.

**AS com maior participação em IXs no estado da Bahia ! E um dos maiores do Brasil neste aspecto/contexto**.

# QUEM SOMOS

Hosting de Servidor Raiz de DNS (K-ROOT.SERVER.ORG) do RIPE, otimizando não só a nossa mas TODA a infraestrutura de internet do Brasil.

**Diversas ações de apoio e participação comunitária em prol do desenvolvimento da internet.**

# O que fazemos ?

# O QUE FAZEMOS ?

Atendemos ao mercado corporativo de empresas de pequeno, médio e grande porte. ISP/Provedores de internet de todos os portes. Operadoras de telecomunicações (Tier-1 e Tier-2). Governo e diversas instituições que necessitam de soluções em telecomunicações com alta disponibilidade, confiável e seguro, com SLA.

# Acesso Dedicado Internet

→ ASN próprio (Autonomous System) amplamente interconectado;

→ 99,7% de disponibilidade anual última milha;

→ SLA

→ Atendimento de suporte N1, N2, N3 com equipe **PRÓPRIA QUALIFICADA (Suporte N1, N2, Engenharia e monitoramento)** ;

→ Tempo médio de reparo | Status do link

**4 horas | indisponível;**

**8 horas | parcialmente**

# Interligação de Matriz x Filiais

→Acesso em tempo real, sistemas, aplicações, documentos, backups e entre outros;

→Uniformidade nas informações para todas as filiais;

→Melhor controle sobre o fluxo de dados na rede;

# Transporte L2L para Operadores

→ Soluções de Transporte Lan-to-Lan , Ethernet carrier grade para ISPs/Operadores;

→SLA diferenciado e monitoramento pró-ativo;

→Equipe própria de monitoramento pró-ativo e suporte reativo, além de equipe de engenharia de rede e projetos própria.

→Soluções elásticas para o mercado Telco/EILD.

# Colocation

- Estrutura de padrão mundial, com redundância em todos os sistemas;
- Sistemas de monitoramento pró-ativo e reativo, sistemas de extinção de incêndio (Agente 3M™ Novec™ 1230);
- Controle de acesso/CFTV;
- Centro de soluções formado por profissionais certificados e altamente qualificados.

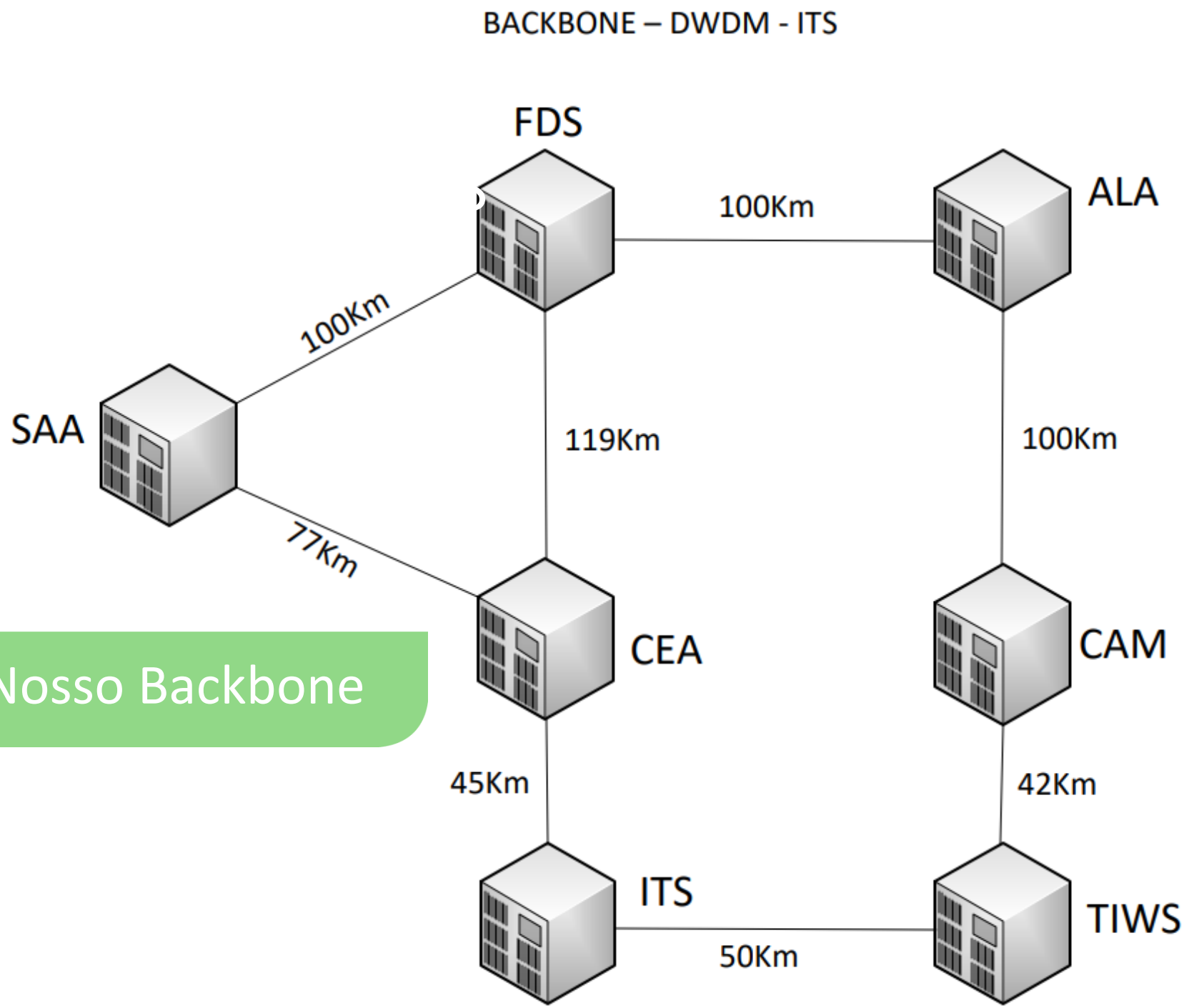
# Internet Satélite

- ❑ Banda KA
- ❑ Velocidades assíncronas até 40mbps.
- ❑ Alta Disponibilidade
- ❑ Ideal para locais remotos, total cobertura nacional

# São nossos clientes (alguns)

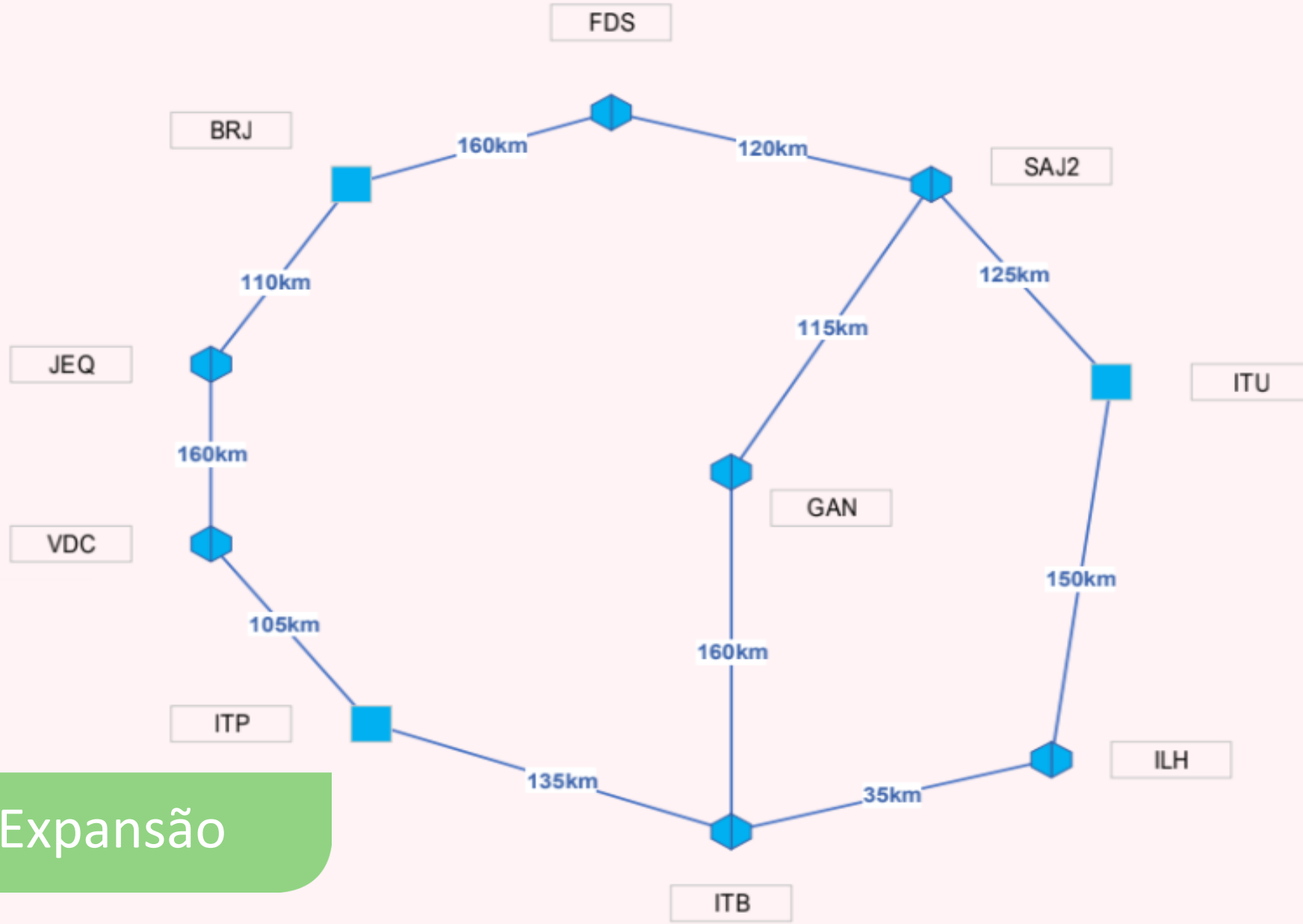

- **Mais de 1300 clientes corporativos.**
- **Mais de 400 clientes ISPs (Transito IPV4/IPv6, Link Dedicado, L2L)**
- **E algumas operadoras de telecomunicações (Com L2L)**

# Nosso Backbone

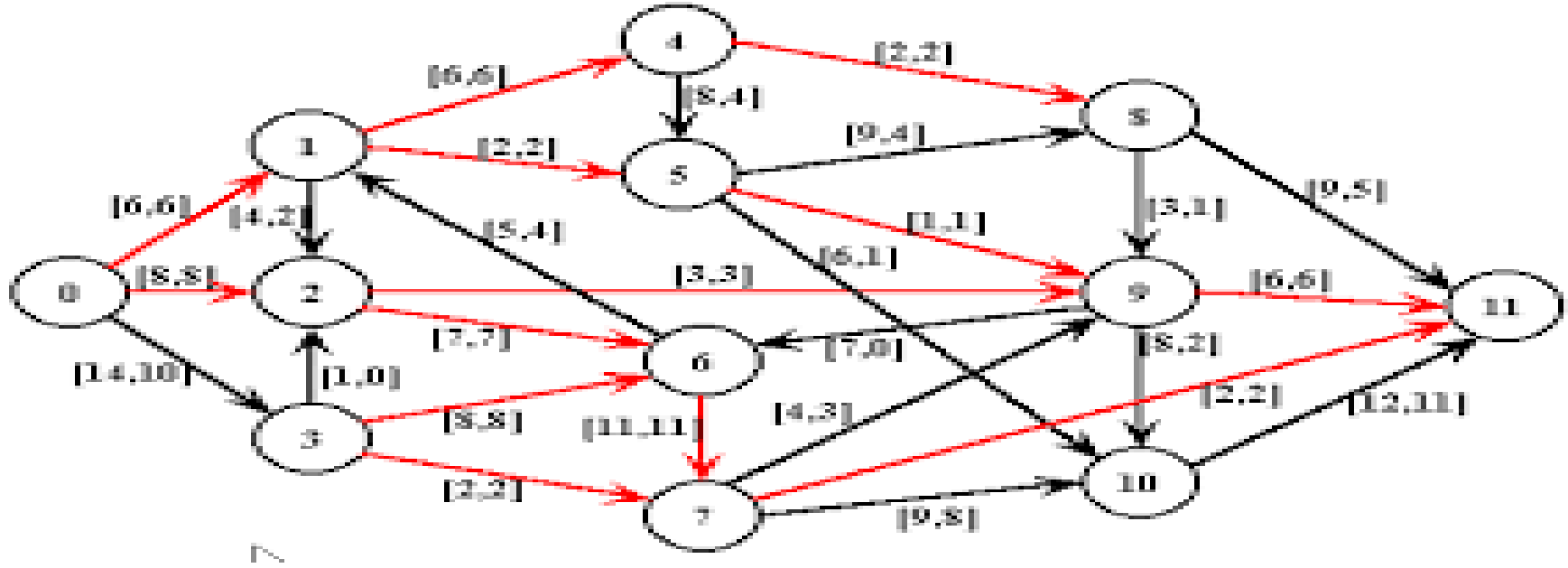


# QUEM SOMOS

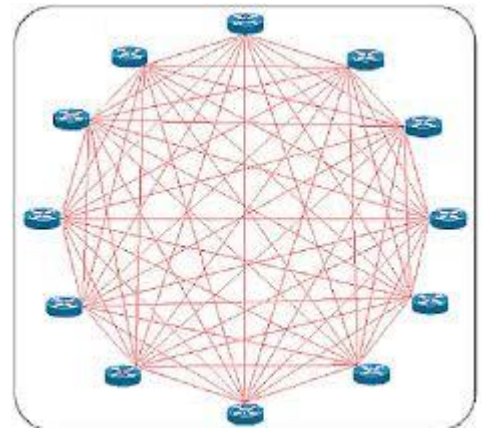
**ROADMAP, EM ANDAMENTO, RFS 2020.1**

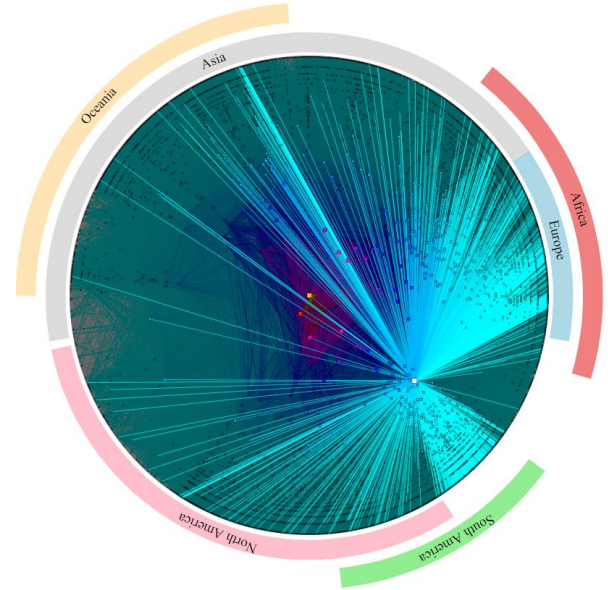



Em Expansão




# Ações de Otimização para um AS – Roadmap ITS





# Ações de Otimização para um AS – Roadmap ITS

**Investimento em infraestrutura de Backbone: DWDM de última geração: Muxponder 100gbps | Carrier Grade**

**ITS - AS28186**

**Projeto Pioneiro e Vanguardista com a Huawei de DWDM com alta densidade**

**Plataforma OTN OptiX OSN 9800**

https://e.huawei.com/br/products/fixe network/transport/wdm/osn-9800

# Ações de Otimização para um AS – Roadmap ITS

**Vanguardista com Huawei: GPON C++ | Alinhamento OLT x ONU , mesmo vendor ! (FEC !) – RFS: 2019.2/Nov-Dez**


**ONUs Huawei, respeitando FEC e em alguns casos, XGS-PON (xPon ~10gbps) + FEC**

# Ações de Otimização para um AS – Roadmap ITS

- **Evolução no acesso, Homologação de circuitos com método RFC 2544 e EtherSAN Y.1564, com Smartclass Viavi MTS 5800**

- **Homologamos em projeto próprio com a Viavi, topologia para homologação de segmento e da CPE ao nosso CORE, RFC 2544.**


# Ações de Otimização para um AS – Roadmap ITS

# AS MAIS BEM INTERCONECTADO DA BAHIA

- https://bgp.he.net/country/BR
- https://asrank.caida.org/asns?asn=28186&type=search

**Networks: Brazil**

| ASN | Name | Adjacencies v4 | Routes v4 | Adjacencies v6 | Routes v6 |
|---|---|---|---|---|---|
| AS263009 | FORTE TELECOM LTDA. | 3,246 | 579 | 1,590 | 117 |
| AS267613 | ELETRONET S.A. | 2,821 | 1,942 | 1,685 | 240 |
| AS28186 | ITS TELECOMUNICACOES LTDA | 2,500 | 583 | 1,619 | 51 |
| AS14840 | COMMCORP COMUNICACOES LTDA | 2,298 | 736 | 1,760 | 143 |
| AS28260 | ALTA REDE CORPORATE NETWORK TELECOM LTDA - EPP | 2,159 | 512 | 44 | 59 |
| AS52873 | SOFTDADOS CONECTIVIDADE | 1,887 | 239 | 1,283 | 55 |
| AS265187 | STEEL WEB PROVEDORES DE ACESSO LTDA | 1,853 | 31 | 1,404 | 14 |
| AS1916 | Associao Rede Nacional de Ensino e Pesquisa | 1,824 | 703 | 1,403 | 130 |
| AS61832 | Fortel Fortaleza Telecomunicacoes Ltda | 1,583 | 1,653 | 154 | 238 |
| AS23106 | AMERICAN TOWER DO BRASIL-COMUNICAO MULTIMDIA LT | 1,454 | 1,432 | 1,187 | 227 |
| AS28329 | G8 NETWORKS LTDA | 1,420 | 1,110 | 837 | 537 |
| AS25933 | Vogel Solues em Telecom e Informtica S/A | 1,340 | 803 | 117 | 96 |
| AS61597 | GP Internet e Consultoria LTDA - ME | 1,328 | 3 | 1,042 | 1 |
| AS262589 | INTERNEXA BRASIL OPERADORA DE TELECOMUNICACOES S.A | 1,298 | 4,905 | 160 | 456 |

| | | | | | |
|---|---|---|---|---|---|
| **AS number** | 28186 | | | | |
| **AS name** | unknown | | | | |
| **organization** | ITS TELECOMUNICACOES LTDA | | | | |
| **country** | Brazil | | | | |
| **AS rank** | 269 | | | | |
| **customer cone** | 136 asn | 834 prefix | 321536 address | | |
| **AS degree** | 2672 global | 181 transit | 5 provider | 2586 peer | 81 customer |

# Ações de Otimização para um AS – Roadmap ITS

## AS MAIS BEM INTERCONECTADO DA BAHIA

- DE-CIX Frankfurt/USA
- DE-CIX New York/USA
- N.O.T.A. (Equinix Miami)/USA
- LINX Lon1/UK
- IX.br - PTT.Brasília
- IX.br - PTT.Curitiba
- IX.br - PTT.Fortaleza
- IX.br - PTT.Porto Alegre
- IX.br - PTT.Rio de Janeiro
- IX.br - PTT.São Paulo (Dupla abordagem de PIX SP2 / SP4)
- IX.br - PTT.Salvador

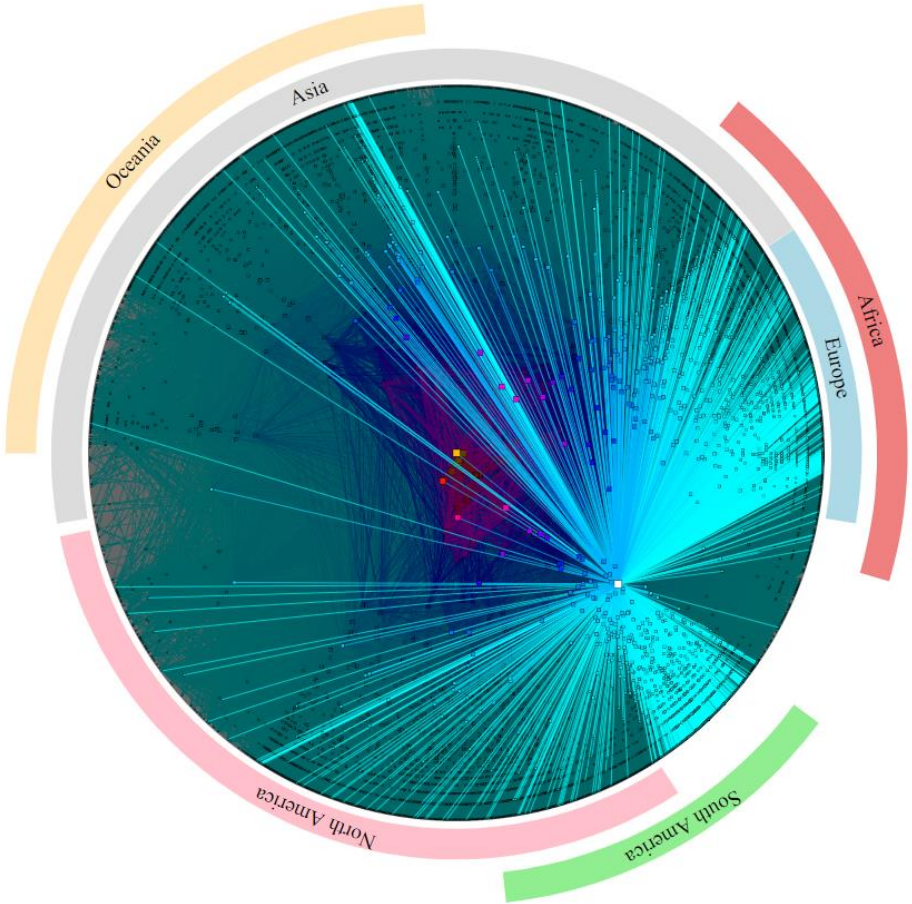
**Em andamento:**

- ✓ ***AMS-IX (RFS: Out_Nov/2019)/HOL***
- ✓ Equinix Ashburn (RFS: Dez/2019)/USA
- ✓ SIX Seattle IX (RFS: Fev_Mar/2020)/USA
- ✓ MSK-IX (Inédito) RFS: Dez/2019/RU
- ✓ HK-IX (Inédito) RFS: Dez/2019/HK_CN
- ✓ JPNAP (Inédito) RFS: Jan_Fev/2020/JP
- ✓ NAPAfrica RFS: Jan_Fev/2020/AFS
- ✓ France-IX RFS: Mar_Abr/2020/FR
- ✓ Peering CZ RFS: Mar_Abr/2020/CZ

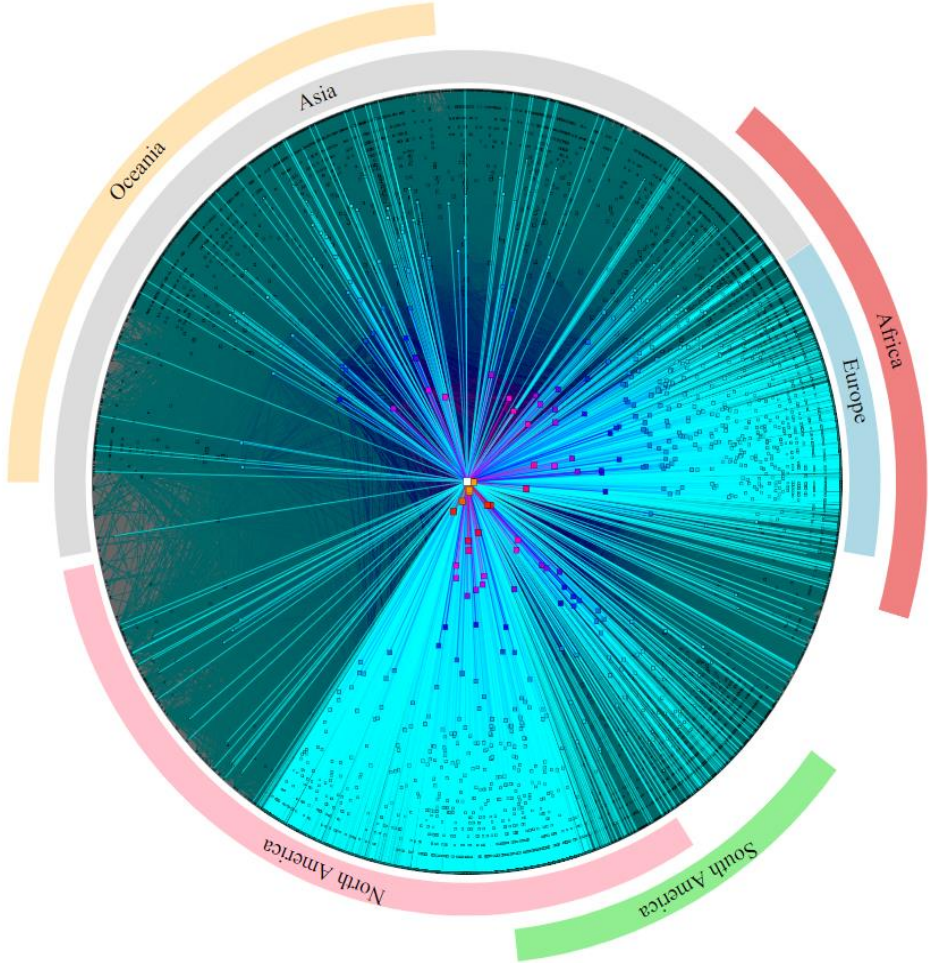
**Entre outros para 2020**

# Ações de Otimização para um AS – Roadmap ITS

## Política de Interconexão e Otimização



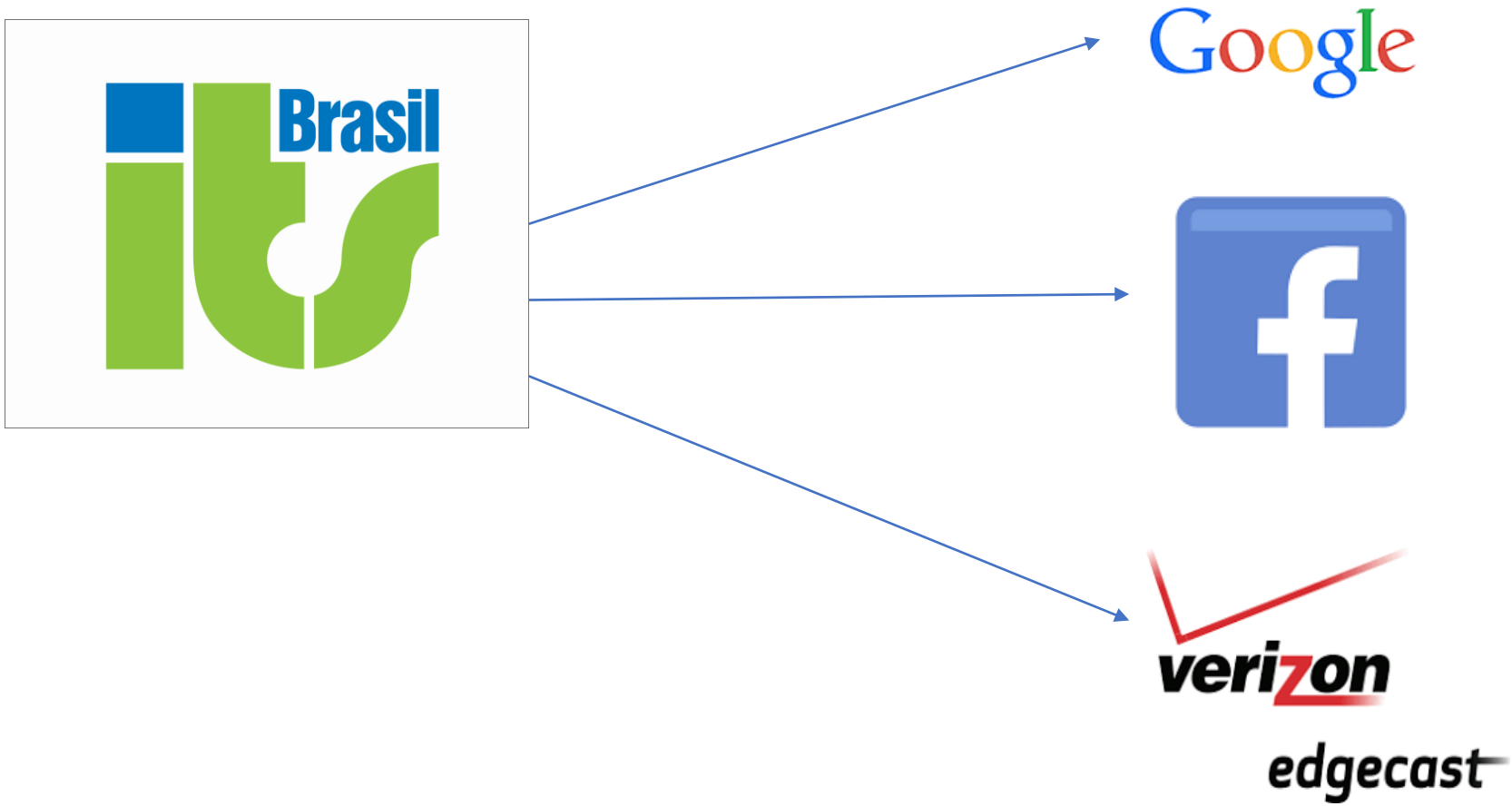

AS Core 28186




AS Core 3356

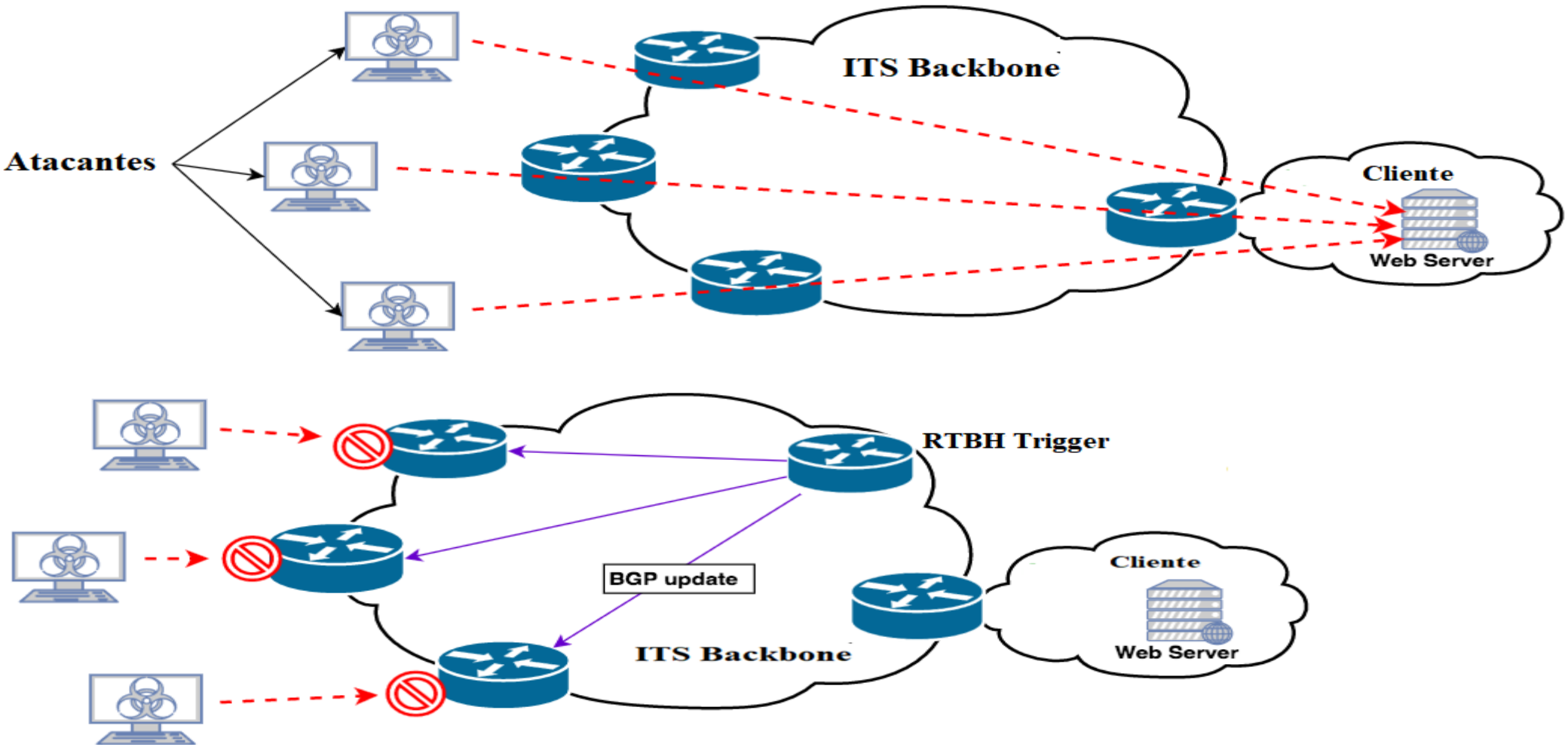
# Ações de Otimização para um AS – Roadmap ITS

## PNI - Private Network Interconnection



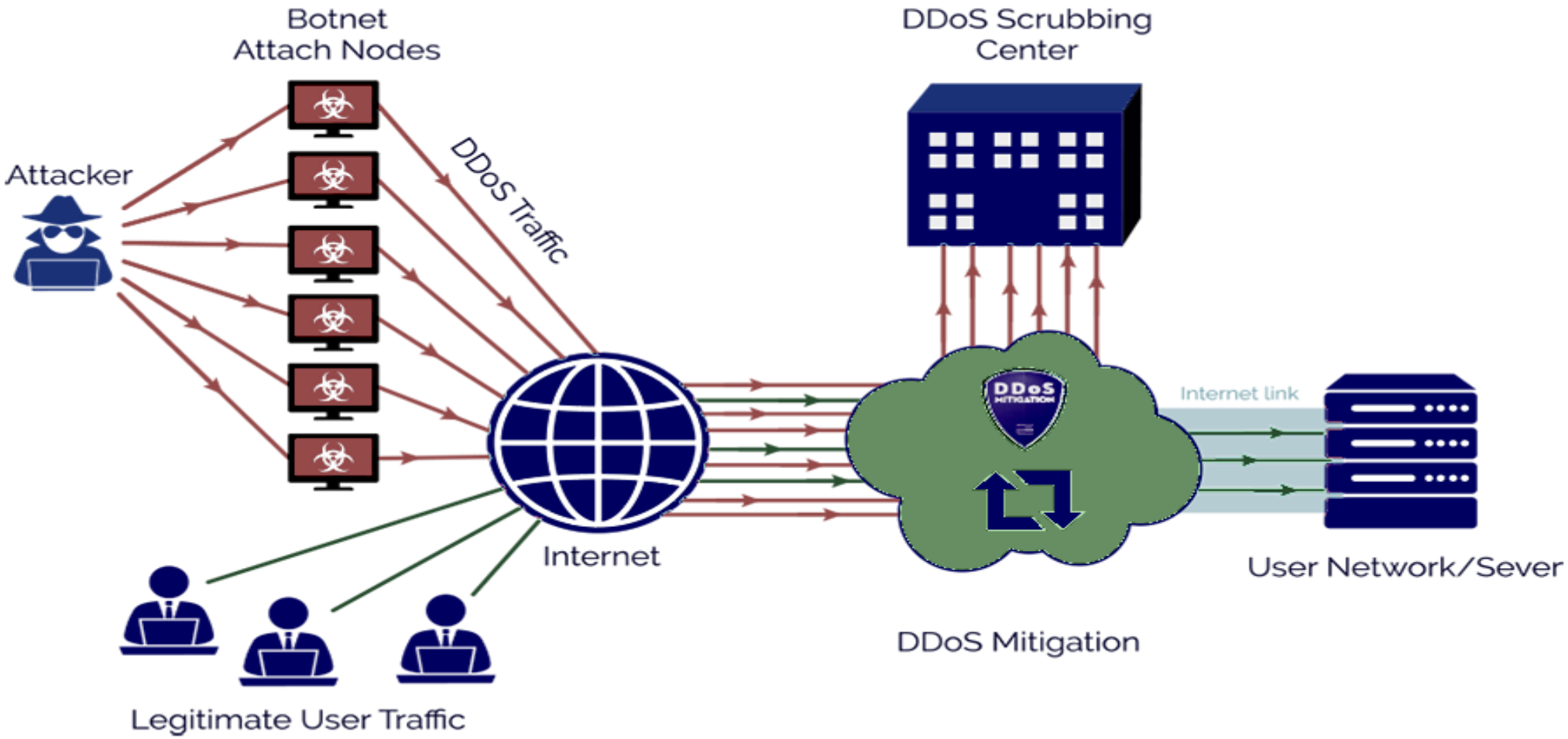
# Ações de Otimização para um AS – Roadmap ITS

## MITIGAÇÃO DDOS – Amplo RTBH



# Ações de Otimização para um AS – Roadmap ITS

## MITIGAÇÃO DDOS – Scrubbing Center



# Ações de Otimização para um AS – Roadmap ITS

## IRR - BCP

https://bgp.he.net/AS28186#_irr

https://www.radb.net/query?advanced_query=&keywords=as28186&-T+option=&ip_option=&-i+option=

RADB

```
aut-num:    AS28186
as-name:    ITS
descr:      ITS TELECOMUNICACOES LTDA
member-of:  AS-IXBR-ATM4-SP, AS-IXBR-ATM6-SP, AS-PTTMETRO-ATM4-SP, AS-PTTMETRO-ATM6-SP, AS-IXBR-SP,
AS-IXBR-ATM4-RJ, AS-IXBR-ATM6-RJ, AS-PTTMETRO-ATM4-RJ, AS-PTTMETRO-ATM6-RJ, AS-IXBR-RJ, AS-IXBR-
ATM4-BA, AS-IXBR-ATM6-BA, AS-PTTMETRO-ATM4-BA, AS-PTTMETRO-ATM6-BA, AS-IXBR-BA, AS-IXBR-ATM4-DF, AS-
IXBR-ATM6-DF, AS-PTTMETRO-ATM4-DF, AS-PTTMETRO-ATM6-DF, AS-IXBR-DF, AS-IXBR-ATM4-PR, AS-IXBR-ATM6-
PR, AS-PTTMETRO-ATM4-PR, AS-PTTMETRO-ATM6-PR, AS-IXBR-PR, AS-IXBR-ATM4-RS, AS-IXBR-ATM6-RS, AS-
PTTMETRO-ATM4-RS, AS-PTTMETRO-ATM6-RS, AS-IXBR-RS, AS-IXBR-ATM4-CE, AS-IXBR-ATM6-CE, AS-PTTMETRO-
ATM4-CE, AS-PTTMETRO-ATM6-CE, AS-IXBR-CE, AS-ITXBR1, AS-IXBR-TRANSIT4-SP, AS-IXBR-TRANSIT6-SP, AS-
IXBR-TRANSIT4-RJ, AS-IXBR-TRANSIT6-RJ, AS-IXBR-TRANSIT4-BA, AS-IXBR-TRANSIT6-BA, AS-IXBR-TRANSIT4-
DF, AS-IXBR-TRANSIT6-DF, AS-IXBR-TRANSIT4-RS, AS-IXBR-TRANSIT6-RS, AS-IXBR-TRANSIT4-PR, AS-IXBR-
TRANSIT6-PR, AS-IXBR-TRANSIT4-CE, AS-IXBR-TRANSIT6-CE, AS-DECIX, AS-DECIX-V6, AS-DECIX-CONNECTED,
AS-DECIX-RS, AS-DECIX-RS-V6, AS-NOTA, AS-NOTA-V6, AS-LINX, AS-DECIX-NYC, AS-DECIX-NYC-V6
import:     from AS12956 AND AS7738 AND AS3549  action pref = 200; accept ANY
            AND NOT AS-ITSBRASIL-CUSTOMER AND <^AS-ITSBRASIL-CUSTOMER+$>
import:     from AS26162 action pref = 600; accept AS-IXBR-ATM4-SP AND AS-IXBR-ATM6-SP AND AS-
PTTMETRO-ATM4-SP AND AS-PTTMETRO-ATM6-SP AND
            AS-IXBR-SP AND AS-IXBR-ATM4-RJ AND AS-IXBR-ATM6-RJ AND AS-PTTMETRO-ATM4-RJ AND AS-
PTTMETRO-ATM6-RJ AND AS-IXBR-RJ AND AS-IXBR-ATM4-BA AND AS-IXBR-ATM6-BA AND AS-PTTMETRO-ATM4-BA AND
AS-PTTMETRO-ATM6-BA AND AS-IXBR-BA AND AS-IXBR-ATM4-DF AND AS-IXBR-ATM6-DF AND AS-PTTMETRO-ATM4-DF
AND AS-PTTMETRO-ATM6-DF AND AS-IXBR-DF AND AS-IXBR-ATM4-PR AND AS-IXBR-ATM6-PR AND AS-PTTMETRO-ATM4-
PR AND AS-PTTMETRO-ATM6-PR AND AS-IXBR-PR AND AS-IXBR-ATM4-RS AND AS-IXBR-ATM6-RS AND AS-PTTMETRO-
ATM4-RS AND AS-PTTMETRO-ATM6-RS AND
            AS-IXBR-RS AND AS-IXBR-ATM4-CE AND AS-IXBR-ATM6-CE AND AS-PTTMETRO-ATM4-CE AND AS-
PTTMETRO-ATM6-CE AND AS-IXBR-CE AND AS-ITXBR1 AND NOT {0.0.0.0/0} AND NOT AS7738 AND NOT AS12956 AND
NOT AS3549 AND NOT AS-ITSBRASIL-CUSTOMER AND <^AS-ITSBRASIL-CUSTOMER+$>
import:     from AS6695  action pref = 500; accept AS-DECIX AND AS-DECIX-V6 AND AS-DECIX-CONNECTED
AND NOT {0.0.0.0/0} AND NOT AS7738 AND NOT AS12956 AND NOT AS3549 AND NOT AS-ITSBRASIL-CUSTOMER AND
<^AS-ITSBRASIL-CUSTOMER+$>
import:     from AS65535  action pref = 550; accept AS-NOTA AND AS-NOTA-V6 AND NOT {0.0.0.0/0} AND
NOT AS7738 AND NOT AS12956 AND NOT AS3549 AND NOT AS-ITSBRASIL-CUSTOMER AND <^AS-ITSBRASIL-
CUSTOMER+$>
import:     from AS-ITSBRASIL-CUSTOMER  action pref = 800; accept AS-ITSBRASIL-CUSTOMER AND <^AS-
ITSBRASIL-CUSTOMER+$> AND NOT {0.0.0.0/0}
import:     from AS8714  action pref = 520; accept AS-LINX AND NOT {0.0.0.0/0} AND NOT AS7738 AND
NOT AS12956 AND NOT AS3549 AND NOT AS-ITSBRASIL-CUSTOMER AND <^AS-ITSBRASIL-CUSTOMER+$>
import:     from AS63034  action pref = 550; accept AS-DECIX-NYC AND AS-DECIX-NYC-V6 AND NOT
{0.0.0.0/0} AND NOT AS7738 AND NOT AS12956 AND NOT AS3549 AND NOT AS-ITSBRASIL-CUSTOMER AND <^AS-
ITSBRASIL-CUSTOMER+$>
export:     to AS-ITSBRASIL-CUSTOMER   announce ANY
export:     to AS12956 AND AS7738 AND AS3549   announce AS-ITSBRASIL AND AS-ITSBRASIL-CUSTOMER AND
<^AS-ITSBRASIL-CUSTOMER+$> AND NOT {0.0.0.0/0}
export:     to AS26162   announce AS-ITSBRASIL AND AS-ITSBRASIL-CUSTOMER AND <^AS-ITSBRASIL-
CUSTOMER+$> AND NOT {0.0.0.0/0}
export:     to AS6695   announce AS-ITSBRASIL AND AS-ITSBRASIL-CUSTOMER AND <^AS-ITSBRASIL-
CUSTOMER+$> AND NOT {0.0.0.0/0}
export:     to AS65535   announce AS-ITSBRASIL AND AS-ITSBRASIL-CUSTOMER AND <^AS-ITSBRASIL-
CUSTOMER+$> AND NOT {0.0.0.0/0}
export:     to AS8714   announce AS-ITSBRASIL AND AS-ITSBRASIL-CUSTOMER AND <^AS-ITSBRASIL-
CUSTOMER+$> AND NOT {0.0.0.0/0}
export:     to AS63034   announce AS-ITSBRASIL AND AS-ITSBRASIL-CUSTOMER AND <^AS-ITSBRASIL-
CUSTOMER+$> AND NOT {0.0.0.0/0}
admin-c:    Daniel Landim
tech-c:     Equipe Redes ITS
remarks:    ITS Brasil Autonomous System
remarks:    https://www.itsbrasil.net
remarks:    Any administrative and comercial issues about AS28186, please send email to:
daniel(at)itsbrasil.net
remarks:    Any technical (routing, security, abuse, peering) and other issues about AS28186, please
send email to: redes(at)itsbrasil.net
notify:     redes@itsbrasil.net
mnt-by:     MAINT-AS28186
changed:    francisco@itsbrasil.net 20190731  #00:18:31Z
source:     RADB
```

# Ações de Otimização para um AS – Roadmap ITS

## PEERINGDB

## BCP

PeeringDB

Pesquisar aqui para uma rede, IX, ou infraestrutura.

Pesquisa Avançada

Registar ou Login

### ITS BRASIL

| | |
|---|---|
| Organização | ITS Brasil |
| Também conhecido como | ITS Telecomunicacoes |
| Website da Empresa | https://www.itsbrasil.net |
| ASN primário | 28186 |
| IRR as-set/route-set | RADB::AS-ITSBRASIL |
| URL do Servidor de rotas | |
| URL do Looking Glass | https://lg.itsbrasil.net/ |
| Tipo de rede | Fornecedor de Serviços de Rede |
| Prefixos IPv4 | 2000 |
| Prefixos IPv6 | 500 |
| Níveis de tráfego | 300-500 Gbps |
| Proporções de tráfego | Inbound Pesado |
| Alcance geográfico | América do Sul |
| Protocolos suportados | Unicast IPv4 Multicast IPv6 |
| Ultima atualização | 2019-01-11T17:39:53Z |
| Notas | |

### Informação da Política de Peering

| | |
|---|---|
| Política de Peering | |
| Política geral | Aberto |
| Localidades Múltiplas | Opcional |
| Requisito de Proporção | Não |
| Requisito de contrato | Opcional |

### Contact Information

| Função | Nome | Telefone<br>E-mail |
|---|---|---|
| Abuse | Gerencia de Redes ( Network Management) | redes@itsbrasil.net |
| Maintenance | Joao Lyma | +55 71 3402 0800<br>lyma@itsbrasil.net |
| NOC | Romulo Lima | +55 71 3402 0800<br>romulo@itsbrasil.net |
| Policy | Francisco Badaro | +55+71+34020870<br>francisco@itsbrasil.net |
| Public Relations | Daniel Landim | daniel@itsbrasil.net |
| Sales | Comercial | +55 71 3402 0800<br>comercial@itsbrasil.net |
| Technical | Gerencia de Redes ( Network Management) | +55 71 3402 0800<br>redes@itsbrasil.net |

### Pontos de Troca de Peering Público

Filter

| Troca<br>ASN | IPv4<br>IPv6 | Velocid...<br>Peer RS |
|---|---|---|
| DE-CIX Frankfurt DE-CIX Frankfurt Peering LAN<br>28186 | 80.81.195.235<br>2001:7f8::6e1a:0:1 | 20G |
| DE-CIX New York DE-CIX New York Peering LAN<br>28186 | 206.82.104.33<br>2001:504:36::6e1a:0:1 | 10G |
| Equinix Miami (formerly NOTA)<br>28186 | 198.32.125.236<br>2001:478:124::1236 | 10G |
| IX.br (PTT.br) Brasília ATM/MPLA<br>28186 | 200.192.110.17<br>2001:12f8:0:13::17 | 1G |
| IX.br (PTT.br) Curitiba ATM/MPLA<br>28186 | 200.219.140.119<br>2001:12f8:0:4::119 | 1G |
| IX.br (PTT.br) Fortaleza ATM/MPLA<br>28186 | 200.219.146.158<br>2001:12f8:0:9::158 | 10G |
| IX.br (PTT.br) Porto Alegre ATM/MPLA<br>28186 | 200.219.143.187<br>2001:12f8:0:6::2:8186 | 1G |
| IX.br (PTT.br) Rio de Janeiro ATM/MPLA<br>28186 | 45.6.53.158<br>2001:12f8:0:2::53:158 | 20G |
| IX.br (PTT.br) Salvador ATM/MPLA<br>28186 | 200.219.145.7<br>2001:12f8:0:8::7 | 10G |
| IX.br (PTT.br) São Paulo ATM/MPLA<br>28186 | 187.16.219.51<br>2001:12f8::219:51 | 60G |
| IX.br (PTT.br) São Paulo ATM/MPLA<br>28186 | 187.16.223.133<br>2001:12f8::223:133 | 40G |
| LINX LON1 Main<br>28186 | 195.66.225.182<br>2001:7f8:4::6e1a:1 | 10G |

### Private Peering Facilities

Filter

| Infraestrutura<br>ASN | País<br>Cidade |
|---|---|
| ITS Telecomunicacoes Datacenter LIZ<br>28186 | Brasil<br>Salvador |
| ITS Telecomunicacoes Datacenter RED<br>28186 | Brasil<br>Salvador |

https://www.peeringdb.com/net/3284

# Ações de Otimização para um AS – Roadmap ITS

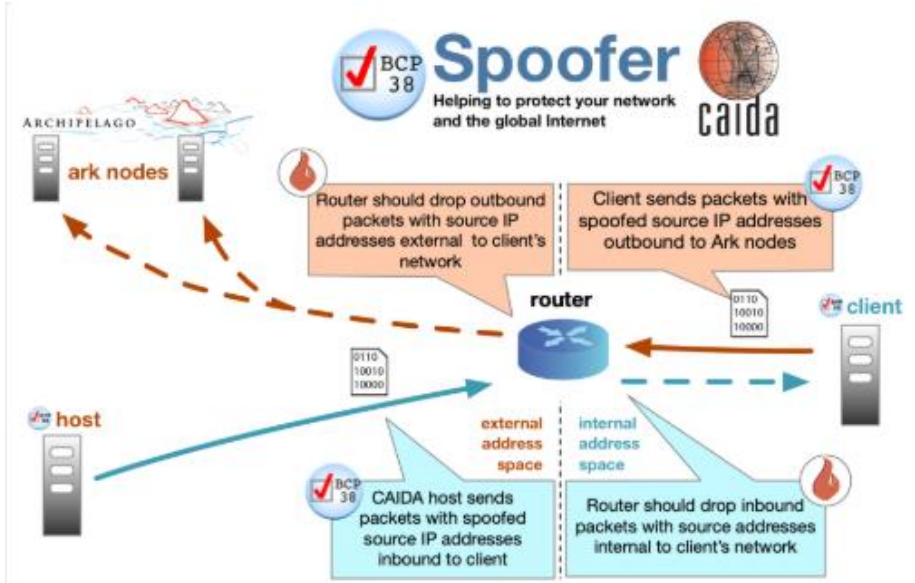
## Pendência - RFS:2020.1

MANRS

https://www.manrs.org/

https://www.manrs.org/isps/participants/

BCP 38




https://www.caida.org/projects/spoofer/

# Roadmap – ITS AS28186

## Otimização Global – MIRRORS
## RFS: 2019.2/Nov-Dez

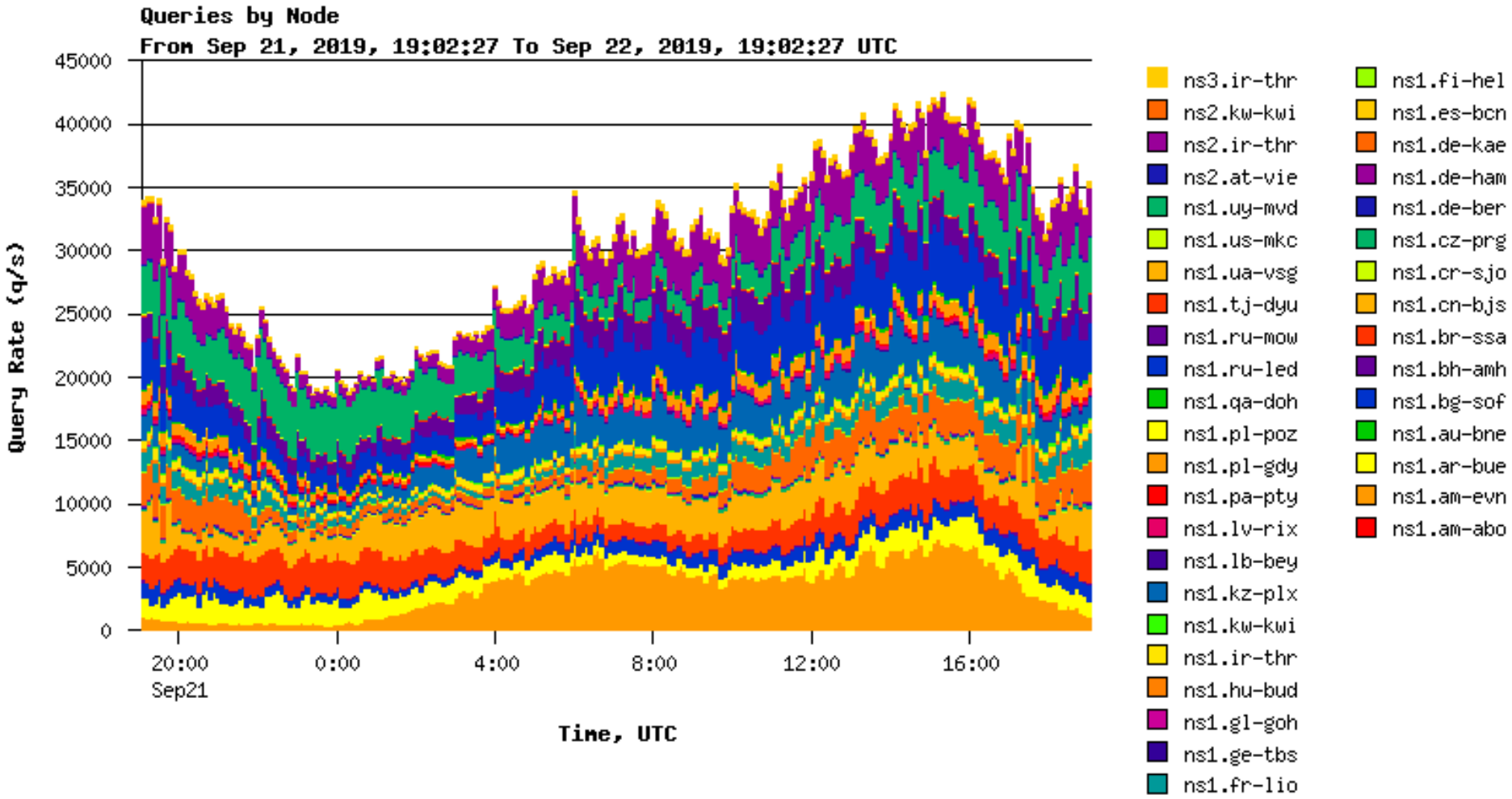
- Centos
- Fedora
- Debian
- Ubuntu
- Arch Linux
- Linux Mint
- OpenSuse
- Gentoo
- Deepin
- Slackware
- OpenBSD

- SourceForge
- CPAN
- Apache
- GNU
- LDP
- Cygwin

# Roadmap – ITS AS28186

## Otimização Global – DNS

**L**, J, F, E, I no .BR e agora **K**



# Roadmap – ITS AS28186

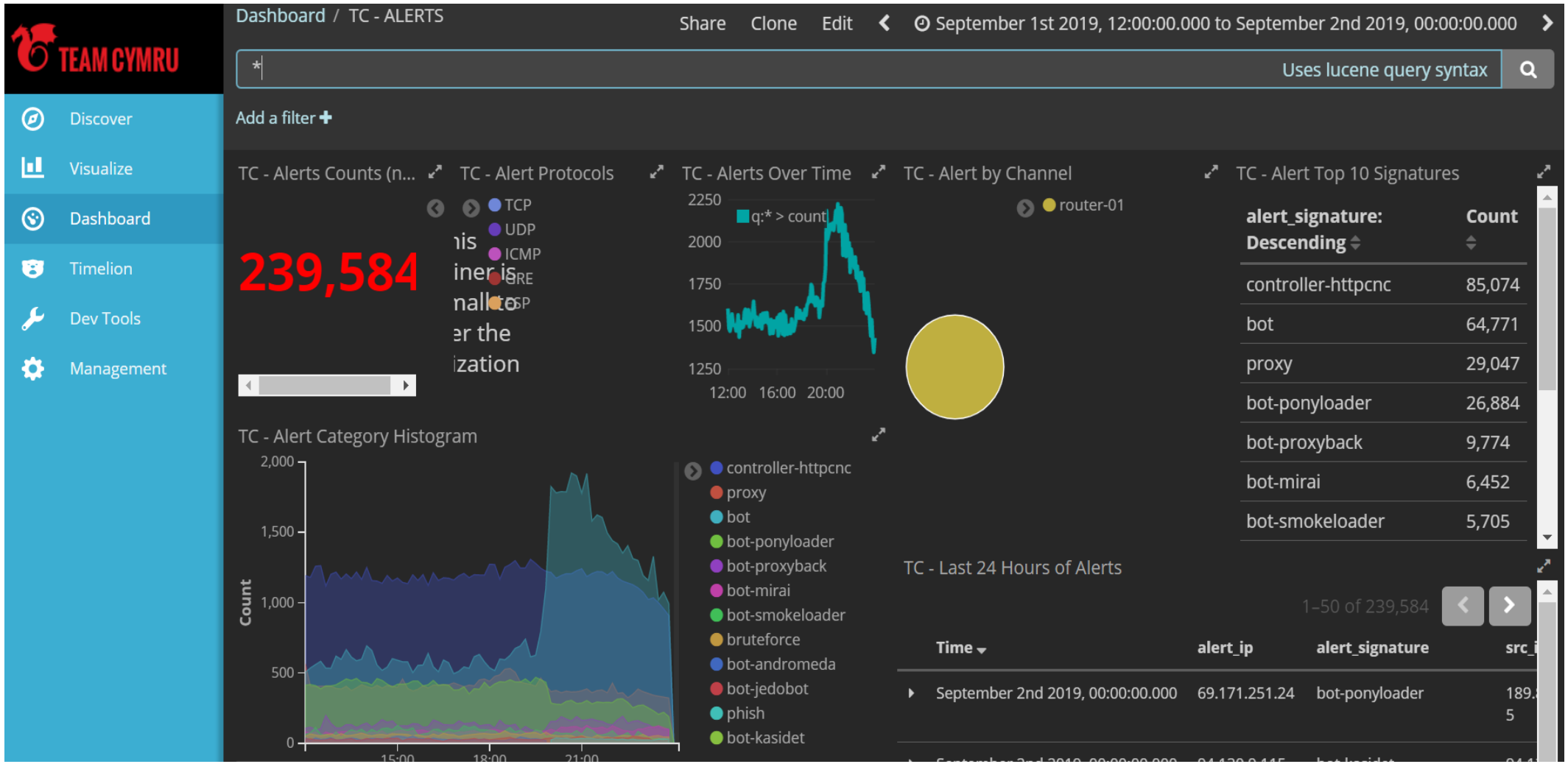
## Ações de Segurança – Análise de Fluxos

- ❑ **TC NIMBUS (Antigo FlowSonar) – *"Conhece profundamente a ti mesmo"***
- ❑ **TC CONSOLE – *"Conhece a ti mesmo"***
- ❑ **TC UTRS – *RTBH Publico***
- ❑ **TC BOGONS – *Sanitização em roteamento***

https://www.team-cymru.com/nimbus.html
https://www.team-cymru.com/TC-Console.html
https://www.team-cymru.com/utrs.html
https://www.team-cymru.com/bogon-reference-bgp.html

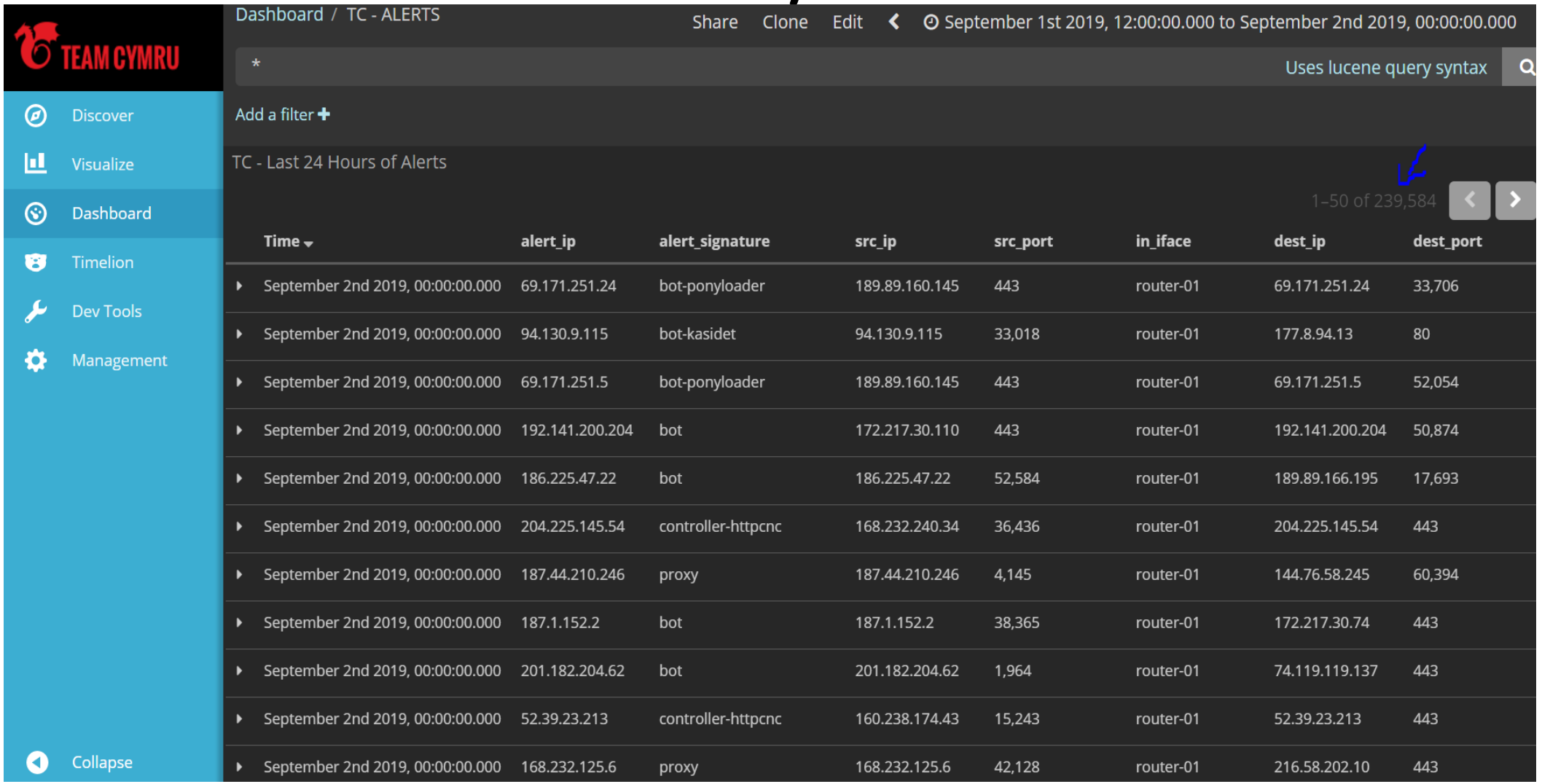
# Roadmap – ITS AS28186

## Ações de Segurança – Combate a C&C/BOTNET



# Roadmap – ITS AS28186

## Ações de Segurança – Combate a C&C/BOTNET




| Time | alert_ip | alert_signature | src_ip | src_port | in_iface | dest_ip | dest_port |
|---|---|---|---|---|---|---|---|
| September 2nd 2019, 00:00:00.000 | 69.171.251.24 | bot-ponyloader | 189.89.160.145 | 443 | router-01 | 69.171.251.24 | 33,706 |
| September 2nd 2019, 00:00:00.000 | 94.130.9.115 | bot-kasidet | 94.130.9.115 | 33,018 | router-01 | 177.8.94.13 | 80 |
| September 2nd 2019, 00:00:00.000 | 69.171.251.5 | bot-ponyloader | 189.89.160.145 | 443 | router-01 | 69.171.251.5 | 52,054 |
| September 2nd 2019, 00:00:00.000 | 192.141.200.204 | bot | 172.217.30.110 | 443 | router-01 | 192.141.200.204 | 50,874 |
| September 2nd 2019, 00:00:00.000 | 186.225.47.22 | bot | 186.225.47.22 | 52,584 | router-01 | 189.89.166.195 | 17,693 |
| September 2nd 2019, 00:00:00.000 | 204.225.145.54 | controller-httpcnc | 168.232.240.34 | 36,436 | router-01 | 204.225.145.54 | 443 |
| September 2nd 2019, 00:00:00.000 | 187.44.210.246 | proxy | 187.44.210.246 | 4,145 | router-01 | 144.76.58.245 | 60,394 |
| September 2nd 2019, 00:00:00.000 | 187.1.152.2 | bot | 187.1.152.2 | 38,365 | router-01 | 172.217.30.74 | 443 |
| September 2nd 2019, 00:00:00.000 | 201.182.204.62 | bot | 201.182.204.62 | 1,964 | router-01 | 74.119.119.137 | 443 |
| September 2nd 2019, 00:00:00.000 | 52.39.23.213 | controller-httpcnc | 160.238.174.43 | 15,243 | router-01 | 52.39.23.213 | 443 |
| September 2nd 2019, 00:00:00.000 | 168.232.125.6 | proxy | 168.232.125.6 | 42,128 | router-01 | 216.58.202.10 | 443 |

# Roadmap – ITS AS28186

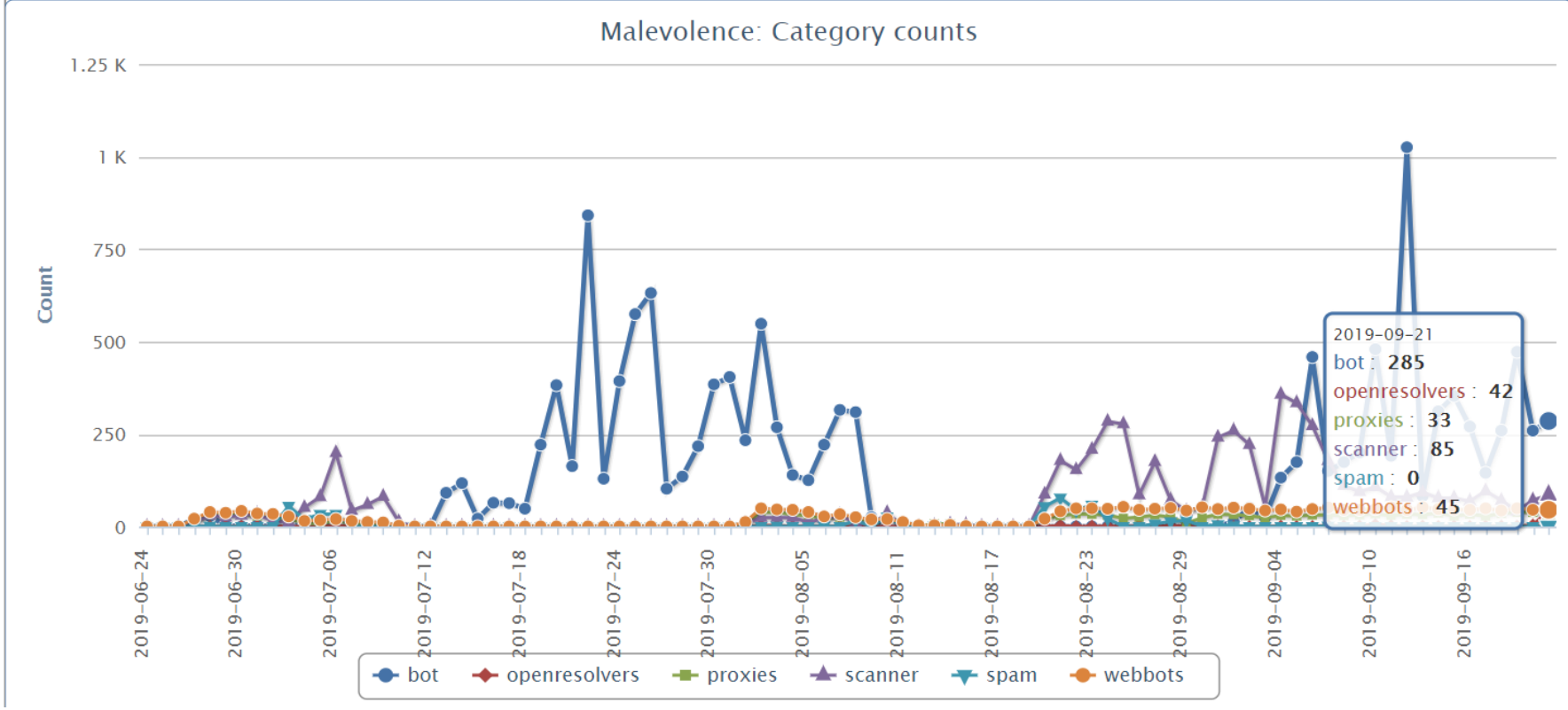
# Ações de Segurança – Combate a C&C/BOTNET

TC Console

Francisco Neto | Settings | Log out
Page load time: 2019-09-23 00:29:20 UTC

Home | Feeds | Traffic | History | Incident Collaboration

Updated daily. Note that new accounts may not see a graph for a day or two while data is gathered.



# Roadmap – ITS AS28186

# Ações de Segurança – Combate a C&C/BOTNET

| Timestamp (UTC) | IP | ASN | Port | Protocol | Confidence | Country Code | Notes | Category | Family | FP Report |
|---|---|---|---|---|---|---|---|---|---|---|
| 2019-09-22 02:59:50 | 189.89.184.42 | 28186 | 3397 | | | BR | | webbots | Conficker | FP! |
| 2019-09-22 02:52:00 | 187.44.167.78 | 28186 | | | | BR | HTTP CONNECT (60786) | proxies | | FP! |
| 2019-09-22 02:51:47 | 187.44.196.110 | 28186 | 50682 | 6 | | BR | dstport:445 | scanner | firewall | FP! |
| 2019-09-22 02:41:59 | 189.89.155.20 | 28186 | 51356 | 6 | | BR | dstport:2323 | scanner | firewall | FP! |
| 2019-09-22 02:41:00 | 187.44.196.110 | 28186 | 50682 | 6 | | BR | dstport:445 | scanner | firewall | FP! |
| 2019-09-22 02:35:24 | 187.44.196.110 | 28186 | 50682 | 6 | | BR | dstport:445 | scanner | firewall | FP! |
| 2019-09-22 02:23:01 | 187.44.221.38 | 28186 | | | | BR | SOCKS4 (4145) | proxies | | FP! |
| 2019-09-22 02:22:42 | 187.44.228.158 | 28186 | 1053 | 17 | | BR | dstport:9050 | scanner | firewall | FP! |
| 2019-09-22 02:22:42 | 187.44.228.158 | 28186 | 57354 | 6 | | BR | dstport:9050 | scanner | firewall | FP! |
| 2019-09-22 02:18:08 | 187.44.196.110 | 28186 | 50682 | 6 | | BR | dstport:445 | scanner | firewall | FP! |
| 2019-09-22 02:00:54 | 189.89.155.20 | 28186 | 40705 | 6 | | BR | dstport:80 | scanner | firewall | FP! |
| 2019-09-22 01:59:47 | 189.89.184.42 | 28186 | 3852 | | | BR | | webbots | Conficker | FP! |
| 2019-09-22 01:58:23 | 189.89.157.54 | 28186 | 51838 | 6 | 50 | BR | destaddr: 145.14.144... | bot | azorult | FP! |
| 2019-09-22 01:57:01 | 189.89.132.194 | 28186 | | | | BR | SOCKS4 (4145) | proxies | | FP! |
| 2019-09-22 01:54:29 | 187.44.228.158 | 28186 | 50439 | 6 | | BR | dstport:6881 | scanner | firewall | FP! |
| 2019-09-22 01:54:16 | 187.44.228.158 | 28186 | 50390 | 6 | | BR | dstport:9050 | scanner | firewall | FP! |
| 2019-09-22 01:53:45 | 187.44.196.110 | 28186 | 50682 | 6 | | BR | dstport:445 | scanner | firewall | FP! |
| 2019-09-22 01:53:45 | 187.44.196.110 | 28186 | 50682 | 6 | | BR | dstport:445 | scanner | firewall | FP! |
| 2019-09-22 01:51:19 | 187.44.196.110 | 28186 | 50682 | 6 | | BR | dstport:445 | scanner | firewall | FP! |
| 2019-09-22 01:49:02 | 187.44.228.158 | 28186 | 65419 | 6 | | BR | dstport:6881 | scanner | firewall | FP! |
| 2019-09-22 01:45:48 | 187.44.228.158 | 28186 | 64660 | 6 | | BR | dstport:6881 | scanner | firewall | FP! |
| 2019-09-22 01:44:38 | 187.44.196.110 | 28186 | 50682 | 6 | | BR | dstport:445 | scanner | firewall | FP! |
| 2019-09-22 01:44:01 | 187.44.228.158 | 28186 | 64180 | 6 | | BR | dstport:6881 | scanner | firewall | FP! |
| 2019-09-22 01:43:59 | 187.44.228.158 | 28186 | 11835 | 17 | | BR | dstport:6881 | scanner | firewall | FP! |
| 2019-09-22 01:42:32 | 187.44.196.110 | 28186 | 50682 | 6 | | BR | dstport:445 | scanner | firewall | FP! |
| 2019-09-22 01:42:26 | 187.44.228.158 | 28186 | 11835 | 17 | | BR | dstport:9050 | scanner | firewall | FP! |
| 2019-09-22 01:42:26 | 187.44.228.158 | 28186 | 63768 | 6 | | BR | dstport:9050 | scanner | firewall | FP! |
| 2019-09-22 01:41:36 | 187.44.129.30 | 28186 | 54769 | 6 | 50 | BR | destaddr: 145.14.145... | bot | azorult | FP! |
| 2019-09-22 01:40:20 | 187.44.129.30 | 28186 | 54771 | 6 | 50 | BR | destaddr: 145.14.145... | bot | azorult | FP! |

# Roadmap – ITS AS28186

# Ações de Segurança – Combate a C&C/BOTNET

1 - 100 of 7597 records found  Page: - 1 - 2 3 4 5 6 7 8 »  Show: 100 per page

| Host | Detection Time | Source | Last Update |
|---|---|---|---|
| 187.44.155.133 (187-44-155-133.STATIC.itsweb.com.br) | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 177.39.228.15 (177-39-228-15.iacunet.com.br) | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 168.232.127.188 (168-232-127-188.dynamic.infotelecom.net.br) | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 170.84.118.178 (170-84-118-178.dynamic.netlideres.net.br) | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 186.232.236.74 (static-186-232-236-74.abmtelecom.net.br) | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 191.242.67.162 | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 168.205.27.154 | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 177.39.202.218 (177-39-202-218.dynamic.rg3telecom.com.br) | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 177.155.150.180 | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 177.39.224.230 (177-39-224-230.iacunet.com.br) | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 177.93.249.11 | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 177.136.127.52 (52.127.136.177.teletalk.net.br) | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 132.255.138.132 (132.255.138.132-user.allconnect.net.br) | | Barracuda Block List | 2019-09-22 06:25:09.402773 |
| 187.108.35.98 | | Composite Block List from cbl.abuseat.org | 2019-09-22 05:15:28.441434 |
| 186.226.183.226 (ns1.serrinha.ba.gov.br) | | Composite Block List from cbl.abuseat.org | 2019-09-22 05:15:28.441434 |
| 187.44.178.54 (187-44-178-54.STATIC.itsweb.com.br) | | Composite Block List from cbl.abuseat.org | 2019-09-22 05:15:28.441434 |
| 187.44.149.99 (187-44-149-99.STATIC.itsweb.com.br) | | Composite Block List from cbl.abuseat.org | 2019-09-22 05:20:40.682171 |
| 187.44.136.62 (187-44-136-62.STATIC.itsweb.com.br) | | Composite Block List from cbl.abuseat.org | 2019-09-22 05:20:40.682171 |
| 143.202.247.175 | | Composite Block List from cbl.abuseat.org | 2019-09-22 05:20:40.682171 |

# Roadmap – ITS AS28186

## AS´s DEVEM COLABORAR - LIMPANDO



## AO RECEBER UM AVISO, TOMEM PROVIDÊNCIAS !

# Roadmap – ITS AS28186
# Feeds

**TODOS deveriam colaborar para uma melhor difusão do conhecimento, P&D em Internet e principalmente PARA O MAPEAMENTO E AFERIÇÃO**

***"Quem não deve, NÃO TEME"***

http://www.routeviews.org/

https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/routing-information-service-ris

**ALIMENTEM CORRETAMENTE OS LGs**

# Roadmap – ITS AS28186

# Feeds – TODO AS DEVERIA COLABORAR


https://atlas.ripe.net/

https://www.caida.org/projects/ark/

https://ring.nlnog.net/

**IXP Contry Jedi (http://sg-pub.ripe.net/emile/ixp-country-jedi/latest/BR/index.html#)**
**Internet Outage Detection and Analysis (IODA)**
**(https://www.caida.org/projects/ioda/)**
**Measurement and ANalysis of Internet Congestion (MANIC)**
**(https://www.caida.org/projects/manic/)**

# Dúvidas



# EXCELÊNCIA EM TELECOMUNICAÇÕES CORPORATIVAS

**WWW.ITSBRASIL.NET**

**+55+71+34020800**