NetFlow:
O que acontece na sua?

Por Lorenzo Busatti

apresentado em português por Guilherme Ramires

Sobre mim

Lorenzo Busatti

- Fundador da Grifonline S.r.l. [ISP] (1997)
- Fundador da Linkwave [WISP] (2006)
- MikroTik Trainer (2010)
- Membro da RIPE, AMS-IX, MIX-IT


linkwave
2006 2016
10 anni di wireless!

Sobre mim


Liechtenstein
Suisse
Svizzera
Switzerland
Graz
Klagenfurt am Wörthersee
Maribor
Slovenija
Slovenia
Zagreb
Pécs
Karlovac
Milano
Verona
Venezia
Padova
Torino
Asti
Parma
Bologna
Genova
Ravenna
Hrvatska
Croatia
Bosna i Hercegovi
Босна и Херцегови
Bosnia an Herzegovi
Zadar
Šibenik
Mostar
San Marino
Monaco
Cannes
Toulon
Livorno
Firenze
Italia
Italy
Grosseto
Pescara
Viterbo
L'Aquila
Roma
Ajaccio
Latina
Foggia
Bari
Napoli
Olbia
Sassari
Potenza
Salerno
Taranto
Brindi
Lecce
Sardegna
Tyrrhenian Sea
Adriatic Sea
Cagliari
Cosenza
Catanzaro
Palermo
Messina
Trapani
Marsala
Catania
Agrigento
Gela
Siracusa
Ragusa
Annaba
Tunis
Google
Camaiore
Pistoia
Prato
Viareggio
Lucca
E76
Quarrata
Firenze
San Piero In Bagno
San Marin
Pisa
Empoli
Bibbiena
Cascina
Pontedera
Figline Valdarno
Urbania
Sansepolcro
Livorno
Rosignano Solvay
Poggibonsi
Montevarchi
Arezzo
Colle di Val d'Elsa
Città di Castello
Gubbio
Cecina
Siena
Castiglion Fiorentino
E80
E35
Umbertide
Cortona
Sinalunga
Campiglia Marittima
Massa Marittima
Montepulciano
Perugia
Città della Pieve
Ribolla
Piombino
Follonica
Arcidosso
Marsciano
Portoferraio
A1
Todi
Grosseto
Acquapendente
Orvieto
Castiglione della Pesc
E45
Pitigliano
E80
Montefiascone
Amelia
Orbetello
Viterbo
Narni
Montalto di Castro
Vetralla
Civita Castellana
Tarquinia
Civitavecchia
Bracciano
Cerveteri
Ladispoli
Roma
Fiumicino

Eu sou um entusiasta do MikroTik

Eu sou um entusiasta do MikroTik

Eu sou um evangelista MikroTikiano

Sobre mim

- Fundador da (2016)

ROUTING & WIRELESS® ACADEMY

Uma ONG para

Training Partners de alta qualidade

Dedicado ao Max

O tráfego da sua rede…

O tráfego da sua rede…

É uma das “coisas”

mais importantes

O tráfego da sua rede…

O que você sabe a respeito?

O tráfego da sua rede…

Qual o crescimento de tráfego dos seus clientes para o Netflix?

O tráfego da sua rede…

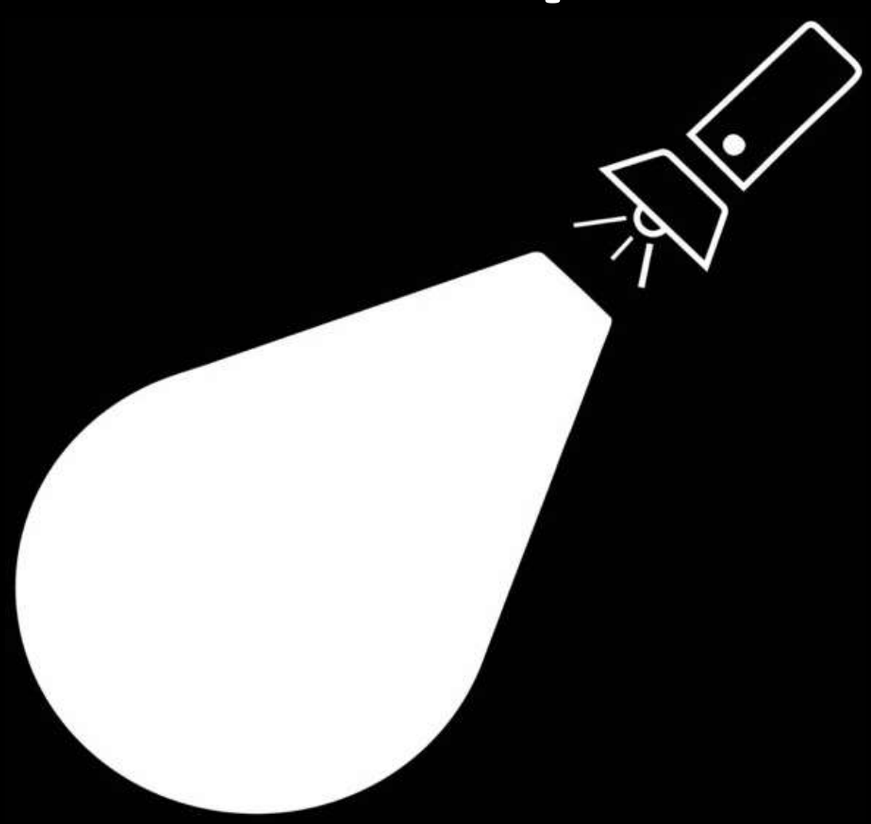
Qual o mais importante AS que você deveria estabeler conexão?

O tráfego da sua rede...

Que usuário é o campeão de consumo?

O tráfego da sua rede…

Com algumas poucas ferramentas você pode descobrir mais do que você imagina☺



NetFlow em pilulas

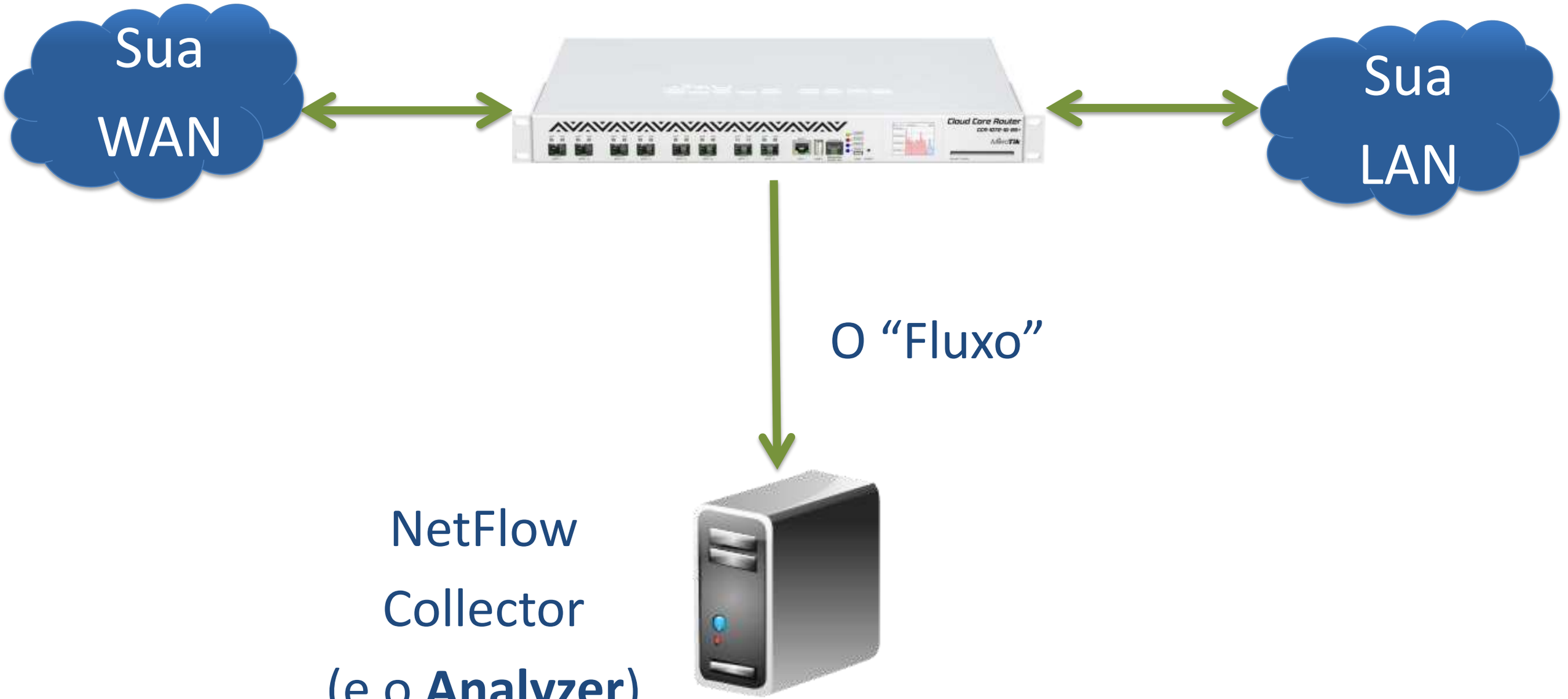
- É um recurso bem “comum” nos routers
- **Coletor** de **estatísticas** de tráfego IP
- Essas estatísticas serão **exportadas** para o **coletor** do **NetFlow**
- Elas são chamadas de: **flow record**
- Este formato é baseado em modelos pré-definidos (desde de a **Versão 9**)

NetFlow no RouterOS

- Sim, suportado!!
- Chamado: **Traffic Flow** (NetFlow é uma nomenclatura própria da Cisco….)
- "Encontrado" no menu: **`/ip traffic-flow`**
- Existe desde o ROS v. 2.9
- Atualmente suporta as **Versões 1, 5, 9**
- **Suporta IPFIX desde o ROS 6.36**

- Consulte a wiki para identificar as diferenças entre versões…. ☺

Traffic Flow em ação



Dois Ingredientes

Os “**Fluxos**”

Um NetFlow Collector (e **Analyzer**)

Limitações do Traffic Flow

- Atualmente o RouterOS não suporta leitura de ASNs BGP ☹
- Estamos na torcida para esta implementação nas próximas versões.... ☺

A parte “tecnica”

(porém bem rápida ….)

Packet transport protocol

- Os registros são exportados utilizando o protocolo UDP
- A porta padrão é a: 2055 (pode ser definida pelo usuário)
- O router não mantem os registros já exportados
- Se um pacote do NetFlow for descartado, todos os registros inerentes serão perdidos também
- Não exporta o “conteúdo” do tráfego. Somente estatísticas.
- O conteúdo do pacote não é encriptado

Estrutura Geral (v9)

NetFlow Packet **header**

- Modelo
  - NetFlow **Record** 1
  - NetFlow **Record** 2
  - NetFlow **Record** n
- Modelo
  - NetFlow **Record** n + 1
  - NetFlow **Record** n + 2
  - NetFlow **Record** n + n

O cabeçalho do pacote

- Versão (v1, v5, v7, v8, v9)
- Sequence number
- Timestamp
- Número de registros (v5 ou v8) ou lista de modelos e registros (v9)

O formato modelo (template)

- ID
- length
- Field Count
- Field 1 Type
- Field 1 Length
- Field 2 Type
- Field 2 Length
- Field N Type
- Field N Length

(alguns campos) v9

IN_BYTES
OUT_BYTES
IN_PKTS
OUT_PKTS
PROTOCOL
SRC_TOS
TCP_FLAGS
L4_SRC_PORT
L4_DST_PORT
IPV4_SRC_ADDR
IPV4_DST_ADDR

DIRECTION
IPV4_NEXT_HOP
IPV6_SRC_ADDR
IPV6_DST_ADDR
ICMP_TYPE
IN_SRC_MAC
IN_DST_MAC
OUT_DST_MAC
OUT_SRC_MAC
SRC_VLAN
DST_VLAN

SRC_AS
DST_AS
BGP_IPV4_NEXT_HOP
IP_PROTOCOL_VERSION
MPLS_LABEL_(1-10)
IF_NAME
IF_DESC

FORWARDING STATUS
(muitos sub-códigos!!!)

Visão do tráfego ao vivo

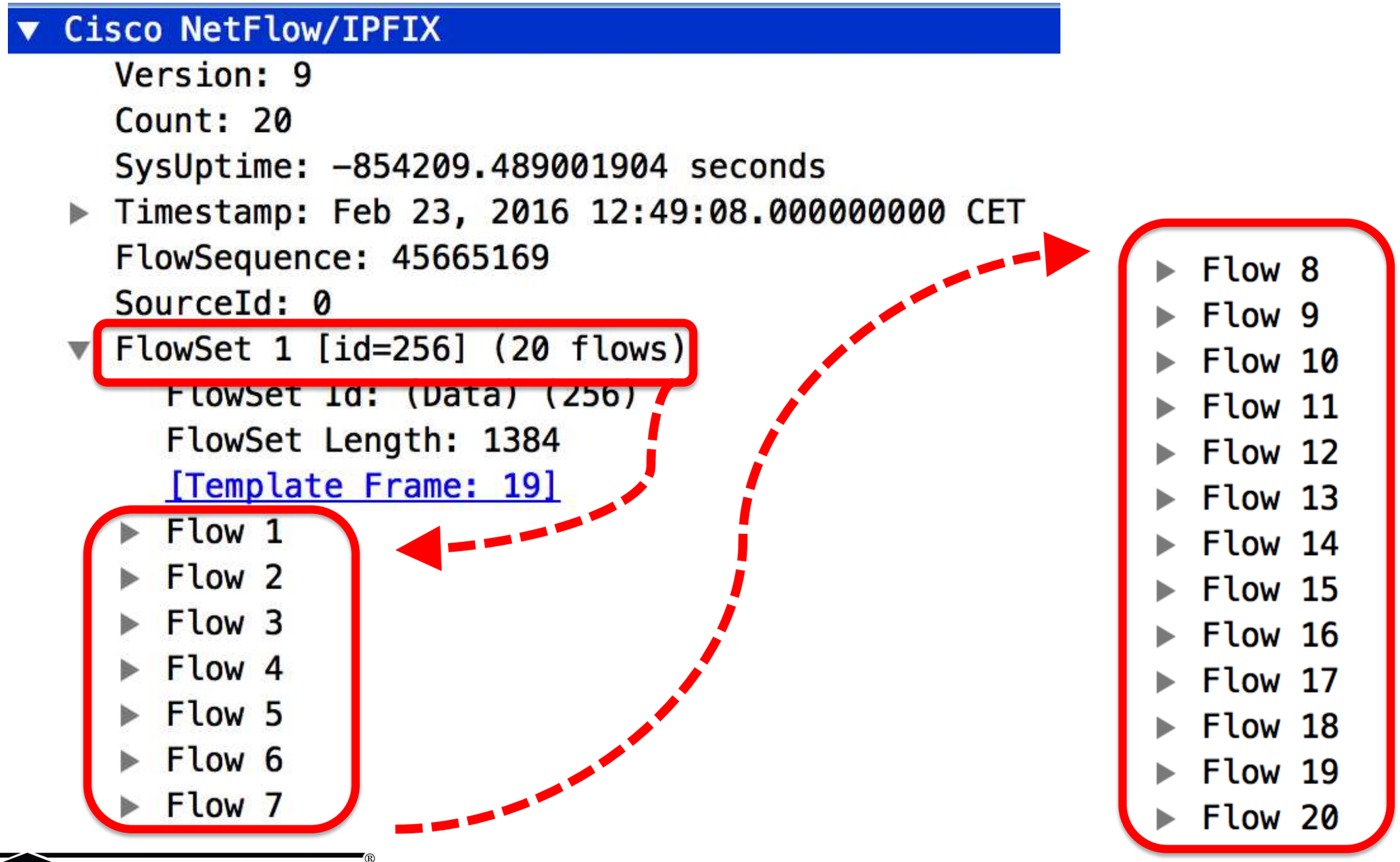
O cabeçalho do pacote

```
└  731 1…  [redacted]  CFLOW  1446 total: 20 (v9) records Obs-Doma

▶ Frame 731: 1446 bytes on wire (11568 bits), 1446 bytes captured (11568 bits)
▶ Ethernet II, Src: AxiomTec_52:93:bc (00:60:e0:52:93:bc), Dst: Routerbo_cf:4c:74 (00:0c:42:cf:4c:74)
▶ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
▶ User Datagram Protocol, Src Port: 2055 (2055), Dst Port: 2055 (2055)
▼ Cisco NetFlow/IPFIX
    Version: 9
    Count: 20
    SysUptime: -854209.489001904 seconds
  ▶ Timestamp: Feb 23, 2016 12:49:08.000000000 CET
    FlowSequence: 45665169
    SourceId: 0
  ▶ FlowSet 1 [id=256] (20 flows)
```

Visão do tráfego ao vivo

O modelo(Template)



Visão do tráfego ao vivo

Um Fluxo

```
▼ Flow 1
  ▼ [Duration: 1.290000000 seconds (switched)]
      StartTime: 854193.160000000 seconds
      EndTime: 854194.450000000 seconds
    Packets: 4
    Octets: 160
    InputInt: 8
    OutputInt: 3
    SrcAddr:
    DstAddr: 85.73.239.223
    Protocol: TCP (6)
    IP ToS: 0x00
    SrcPort: 64866 (64866)
    DstPort: 61053 (61053)
    NextHop: 80.249.208.179
    DstMask: 0
    SrcMask: 0
    TCP Flags: 0x14
    Destination Mac Address: AxiomTec_52:93:bc (00:60:e0:52:93:bc)
    Post Source Mac Address: AxiomTec_06:02:d4 (00:60:e0:06:02:d4)
    Post NAT Source IPv4 Address:
    Post NAT Destination IPv4 Address: 85.73.239.223
    Post NAPT Source Transport Port: 0
    Post NAPT Destination Transport Port: 0
```

IPFIX

O NetFlow é uma tecnologia proprietária cisco.

IPFIX é um protocolo **IETF**, um **padrão** baseado nas RFC5101 e RFC5102 (baseado no NetFlow v9)

IPFIX

RouterOS suporta o IPFIX desde a versão **6.36**

Quer saber mais sobre o IPFIX?

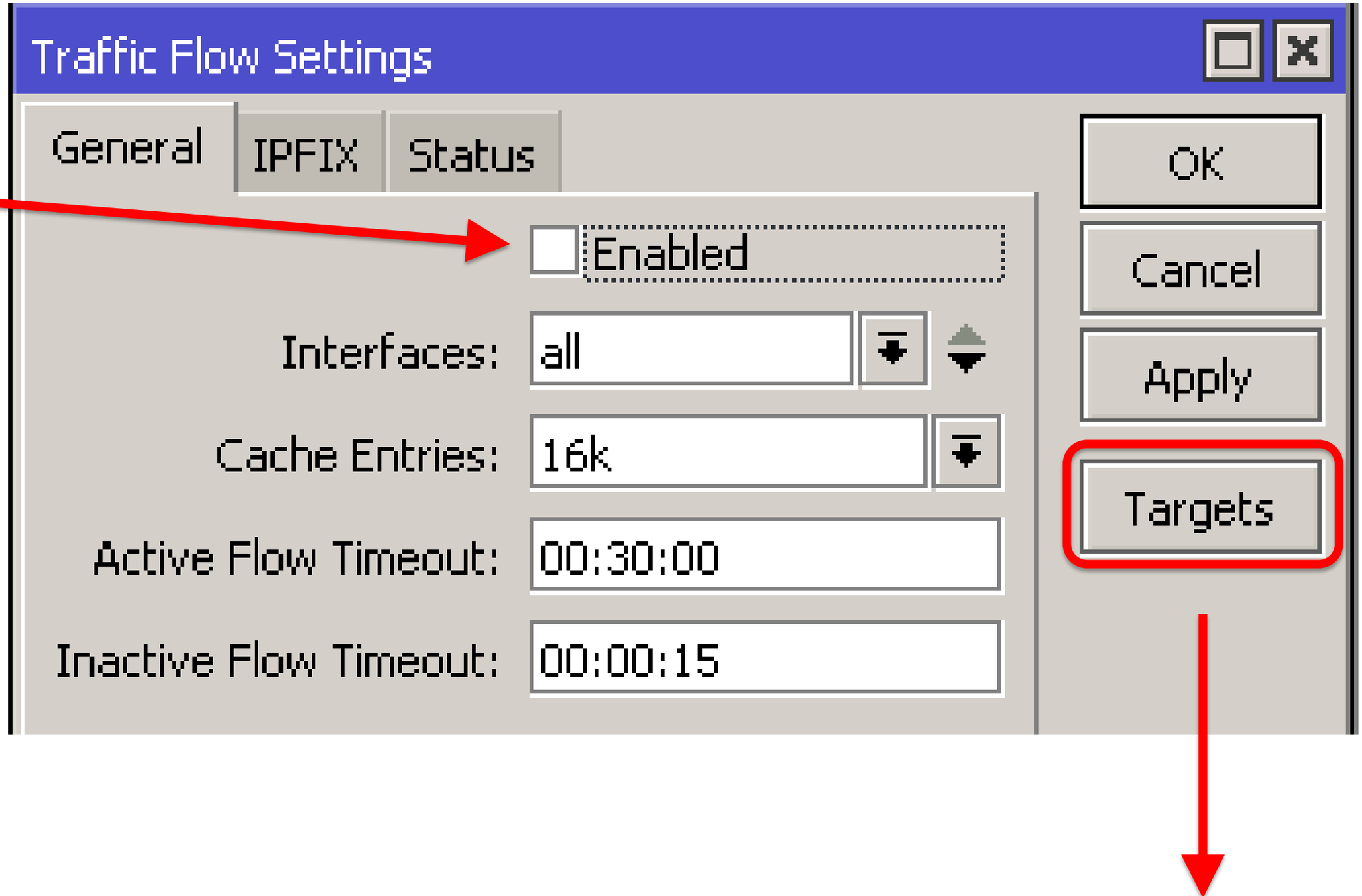
https://en.wikipedia.org/wiki/IP_Flow_Information_Export

Sumário

O Traffic Flow irá “exportar” quase “tudo” exceto o “conteúdo” efetivo do tráfego.

Configurando o router

IP –> Traffic Flow



IP –> Traffic Flow - Targets

Traffic Flow Targets

Find

Src. Address	Dst. Address	Port	Version
	1.2.3.4	2055	9
	5.6.7.8	2055	IPFIX

2 items

New Traffic Flow Target

Src. Address:

Dst. Address: <NetFlowCollectorIP>

Port: 2055

Version: 9

v9/IPFIX Template Refresh: 20

v9/IPFIX Template Timeout: 1800

OK

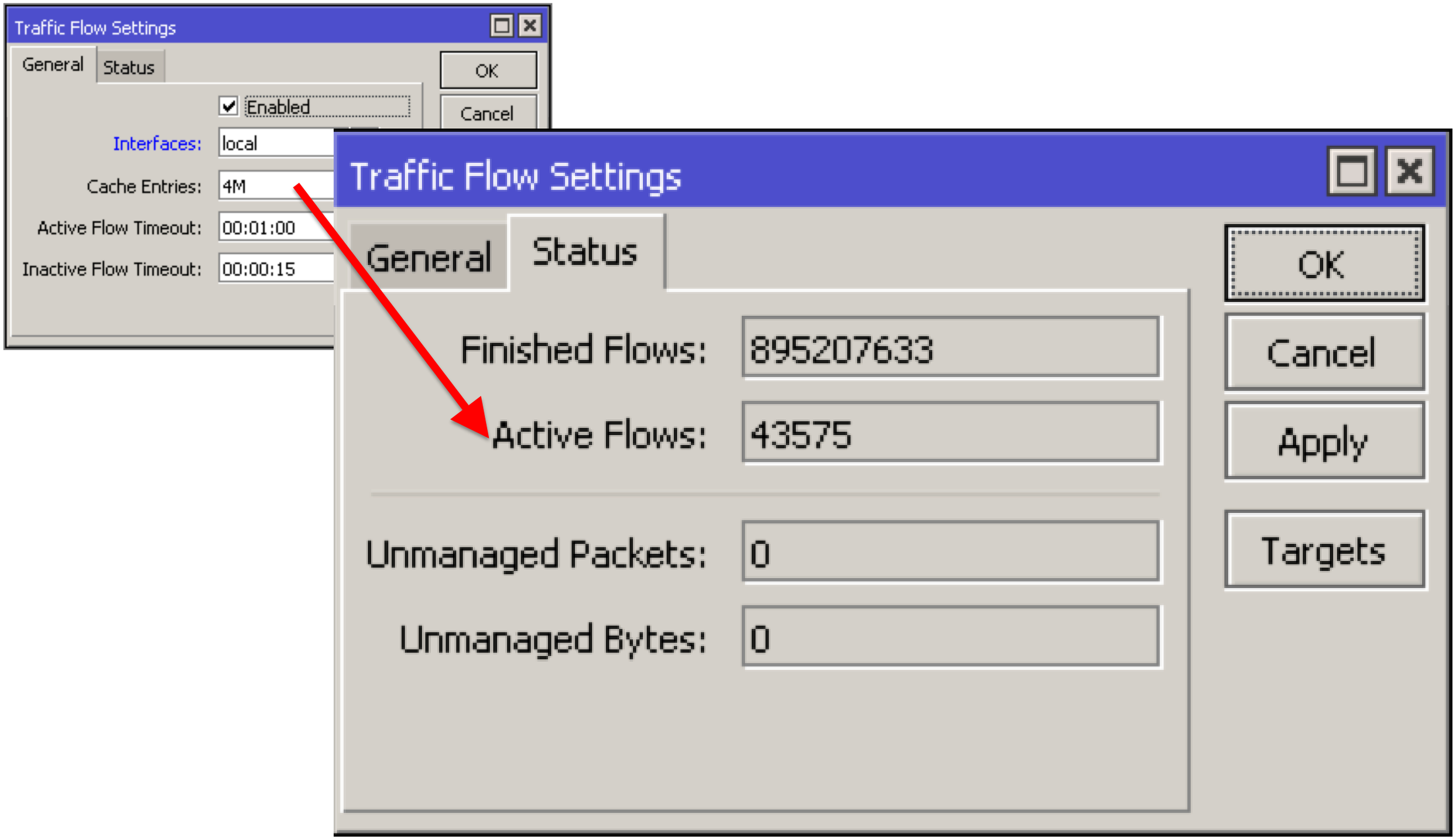
Cancel

Apply

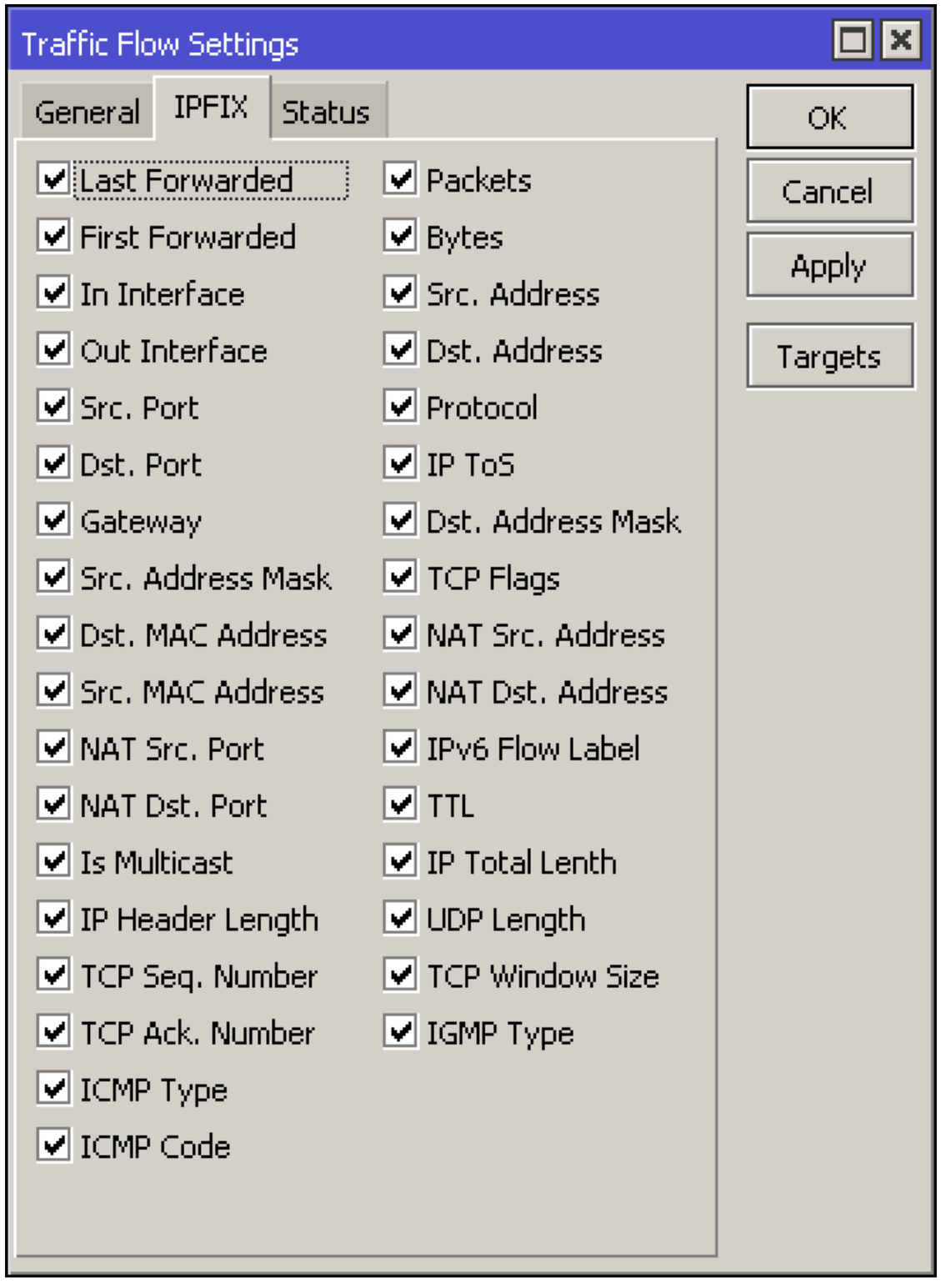
Copy

Remove

IP –> Traffic Flow -> Status



IPFIX settings



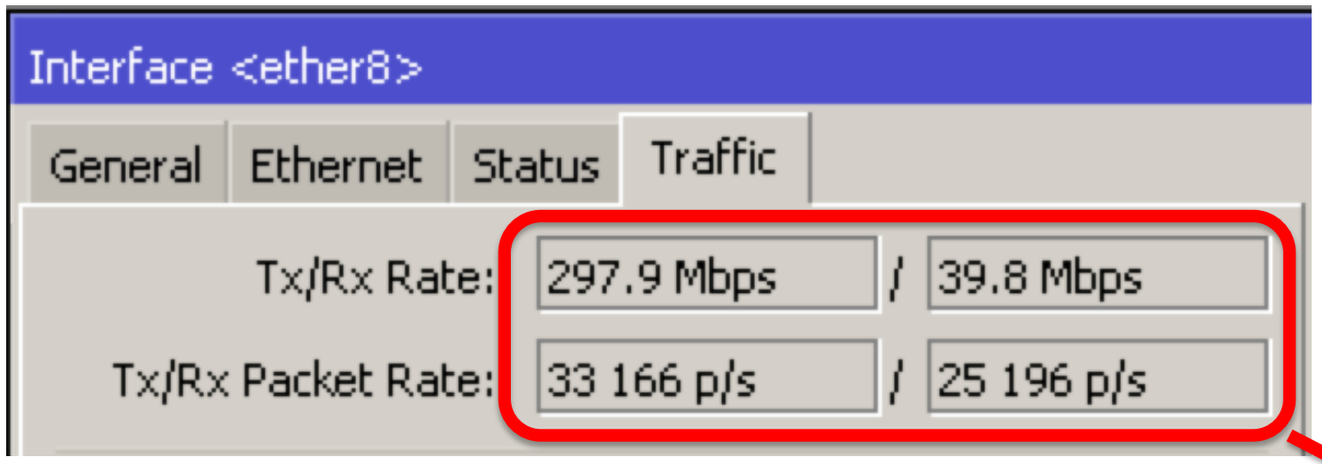
Quanto recurso será requisitado (banda) ?

Traffic Flow “tráfego”

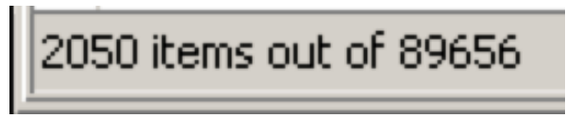
Não existe uma fórmula exata para calcular o consumo dos “fluxos” exportados, porém irei demonstrar um exemplo ”ao vivo”.

Traffic Flow “tráfego”

The router traffic



The sessions



The “**Flows**”

Eth. P...	Pro...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate
800 (ip)	17 ...	[redacted]3:2055	[redacted]:2055			0 bps	1130.3 kbps

O coletor NetFlow (e Analizador)

O que eu preciso agora?

- O **Coletor** irá coletar os fluxos exportados pelo seu router.

- O **Analizador** vai tornar os dados legiveis e utilizáveis para você.

- A maioria dos Coletores também são Analizadores.

Qual escolher?

- **Open** source OU **Closed** source?
- **Windows** OU **Linux?**
- Em **Cloud** OU no seu **Data center**;
- **Pago** OU **Grátis?**
- ……

Exemplos

ntop

ManageEngine
NetFlow Analyzer

PRTG
NETWORK
MONITOR

Talaia

Scrutinizer™
NetFlow & sFlow Analyzer

Colasoft
Get to Know Your Network

Qual escolher?

Eu não representante de vendas de nenhuma dessas marcas.

Você pode pesquisar na internet e “experimentar” antes de comprar.

Qual escolher?

Nesta apresentação vou demonstrar um exemplo usando o serviço em nuvem provido pela:

Talaia

(14 dias para teste)

http://talaia.io

Porém a parte mais importante é:

O que é possível ver?????

Que tráfego?

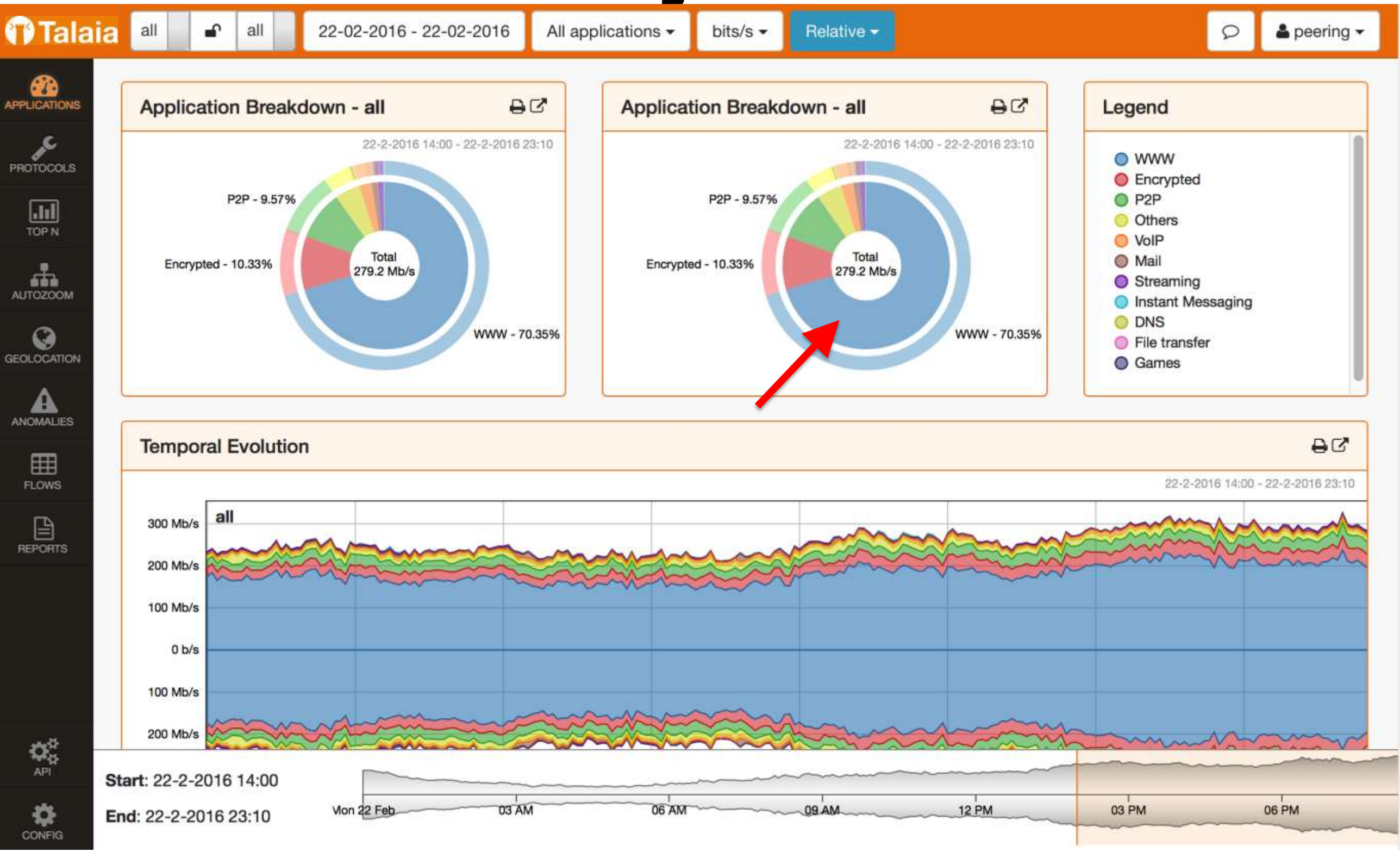
Apenas alguns exemplos:

- Monitoramento de consumo de Banda
- Aplicações Utilizadas
- Identificação de domínios visitados
- Principais consumidores (usuários e destinos)
- Tráfego por geo-localização.
- Detecção de ataques.

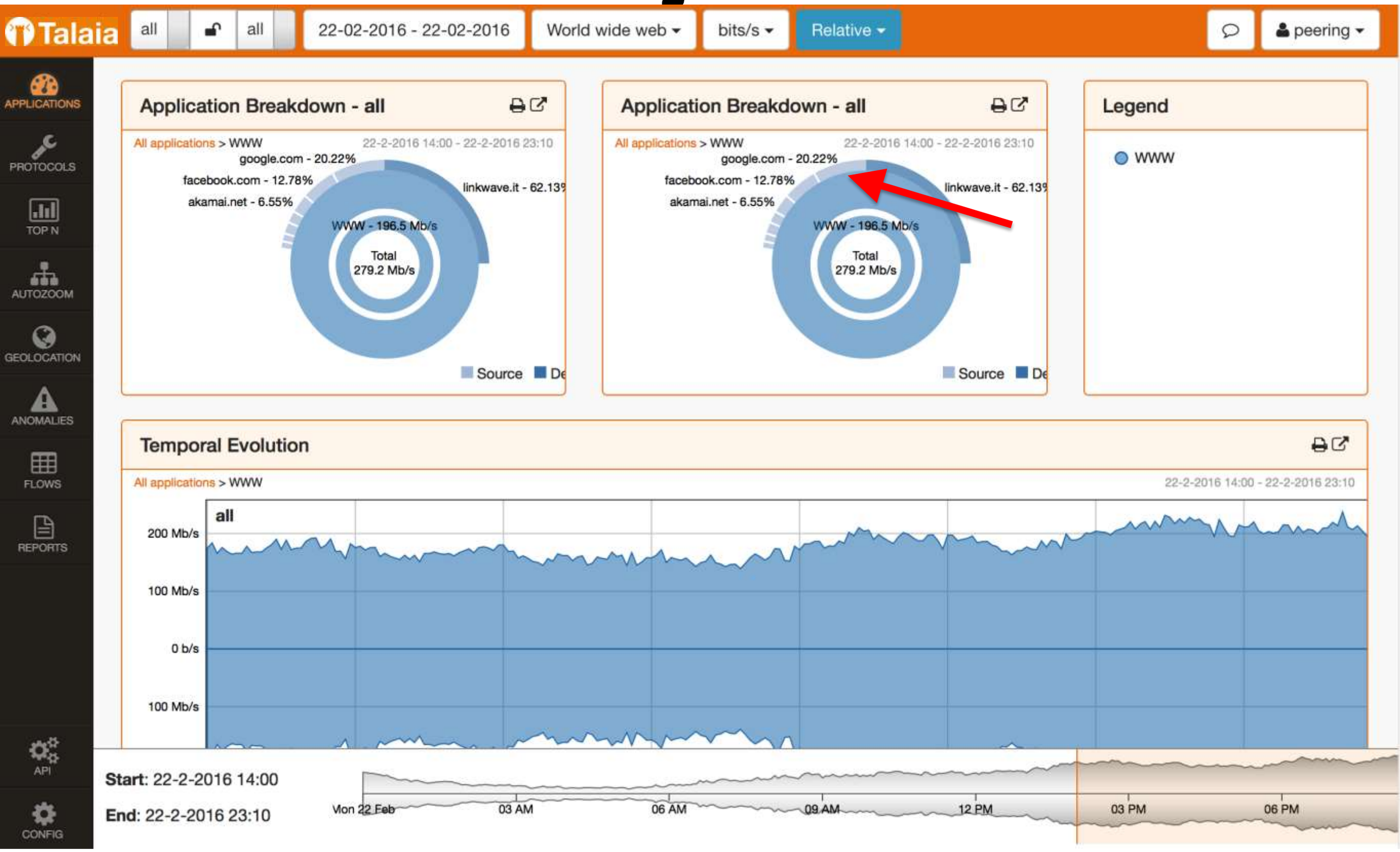
Que tráfego?

- E desde o RouterOS 6.33 o **fastpath**

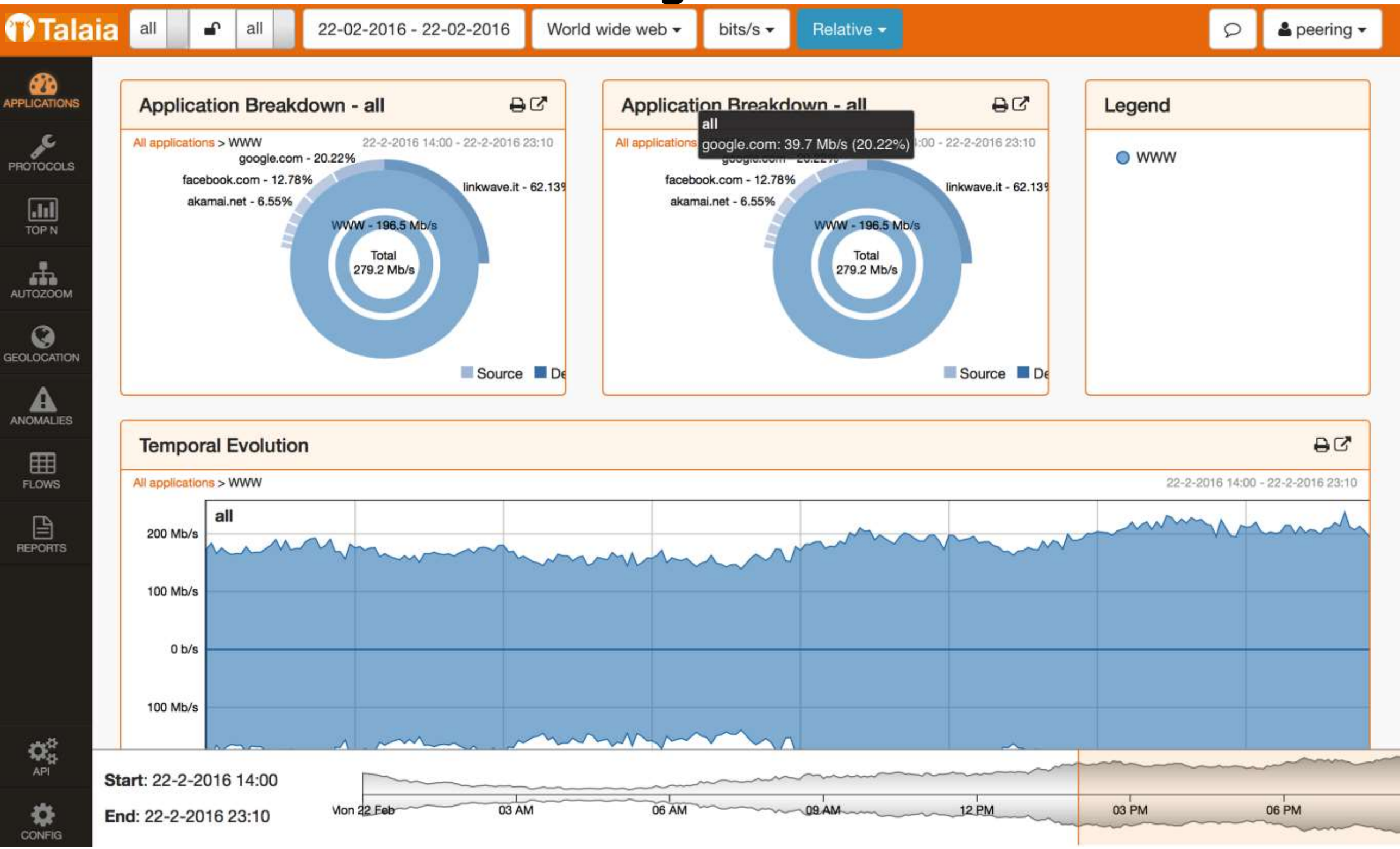
Demonstração “ao vivo”



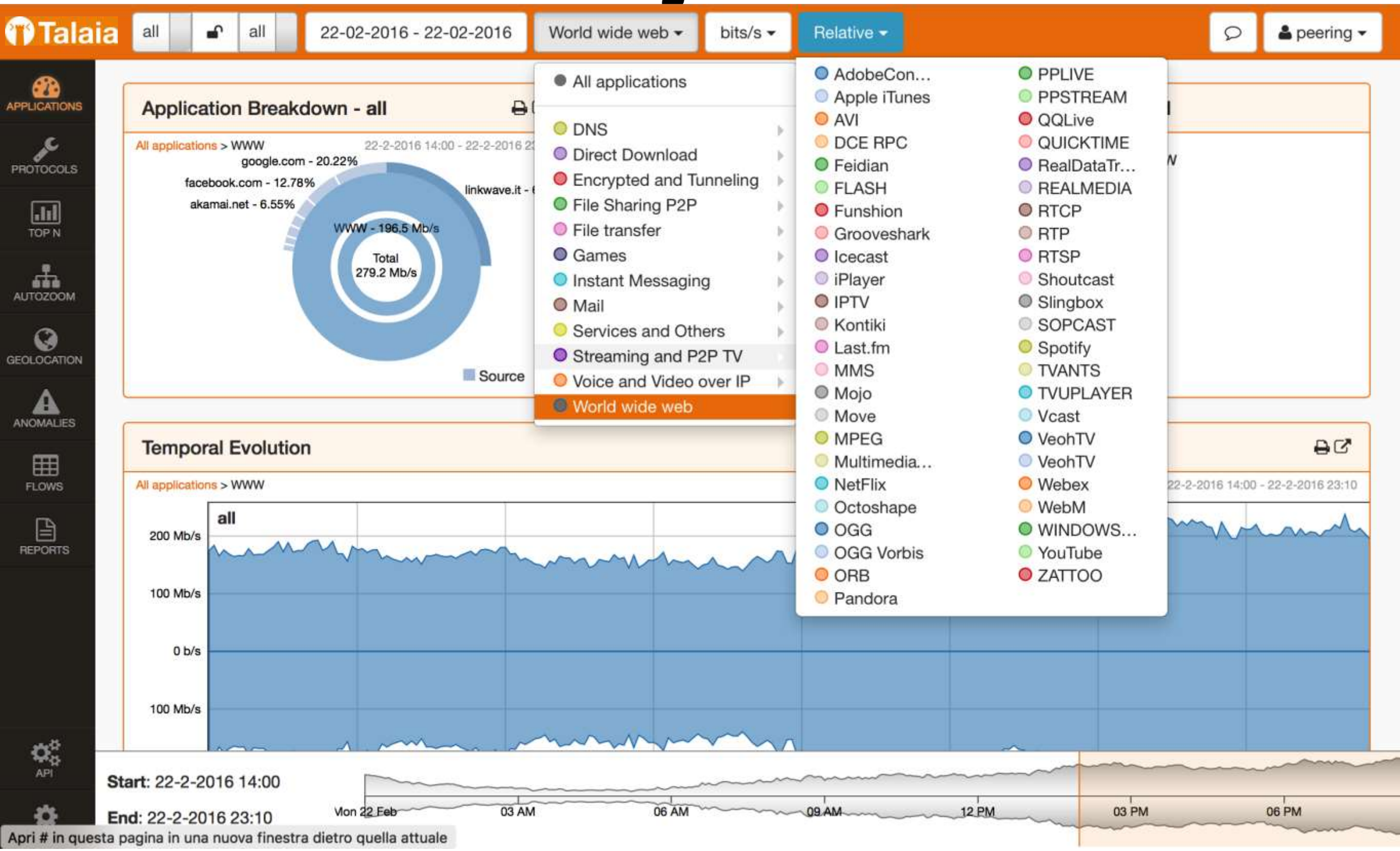
Demonstração “ao vivo”



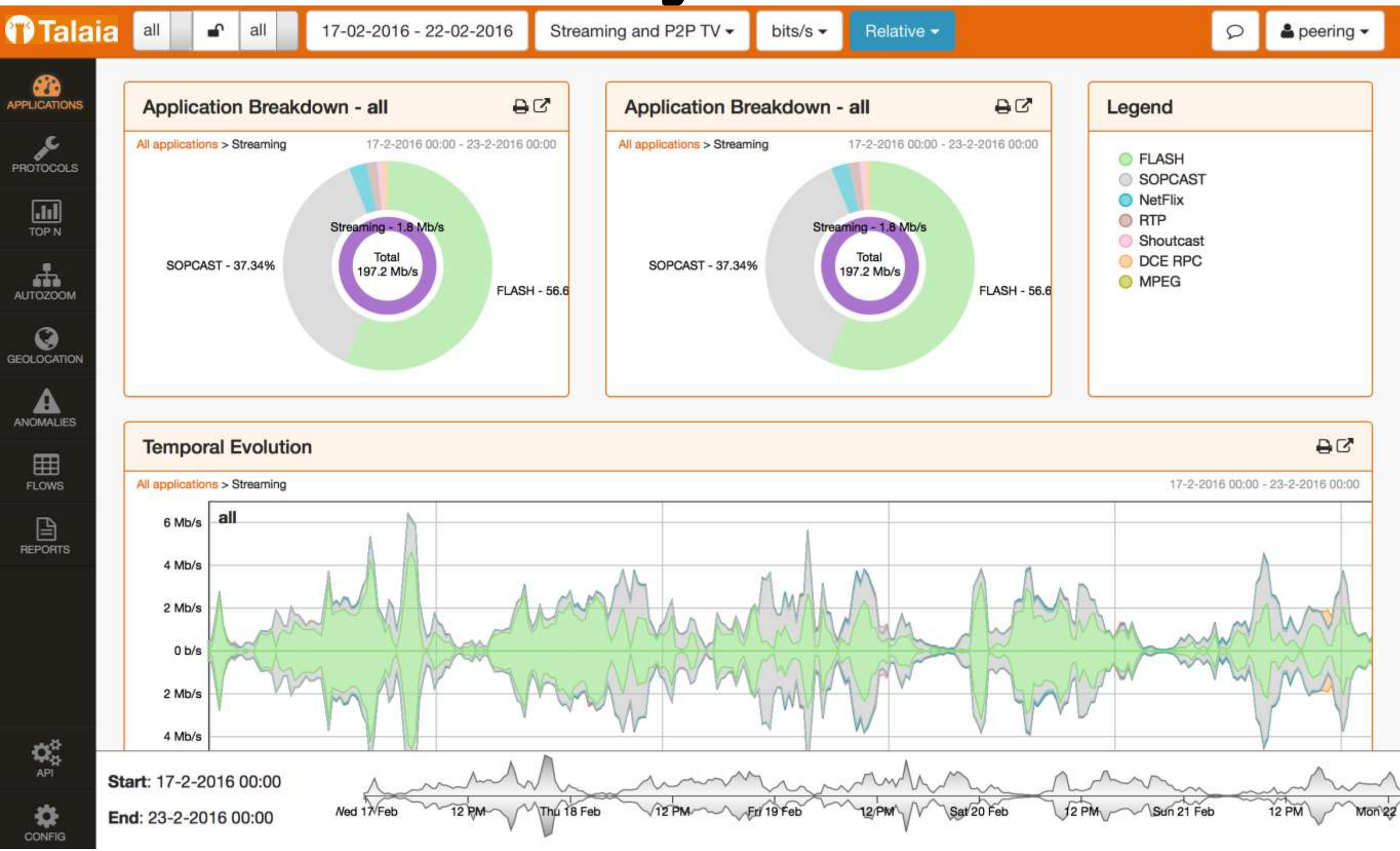
Demonstração “ao vivo”



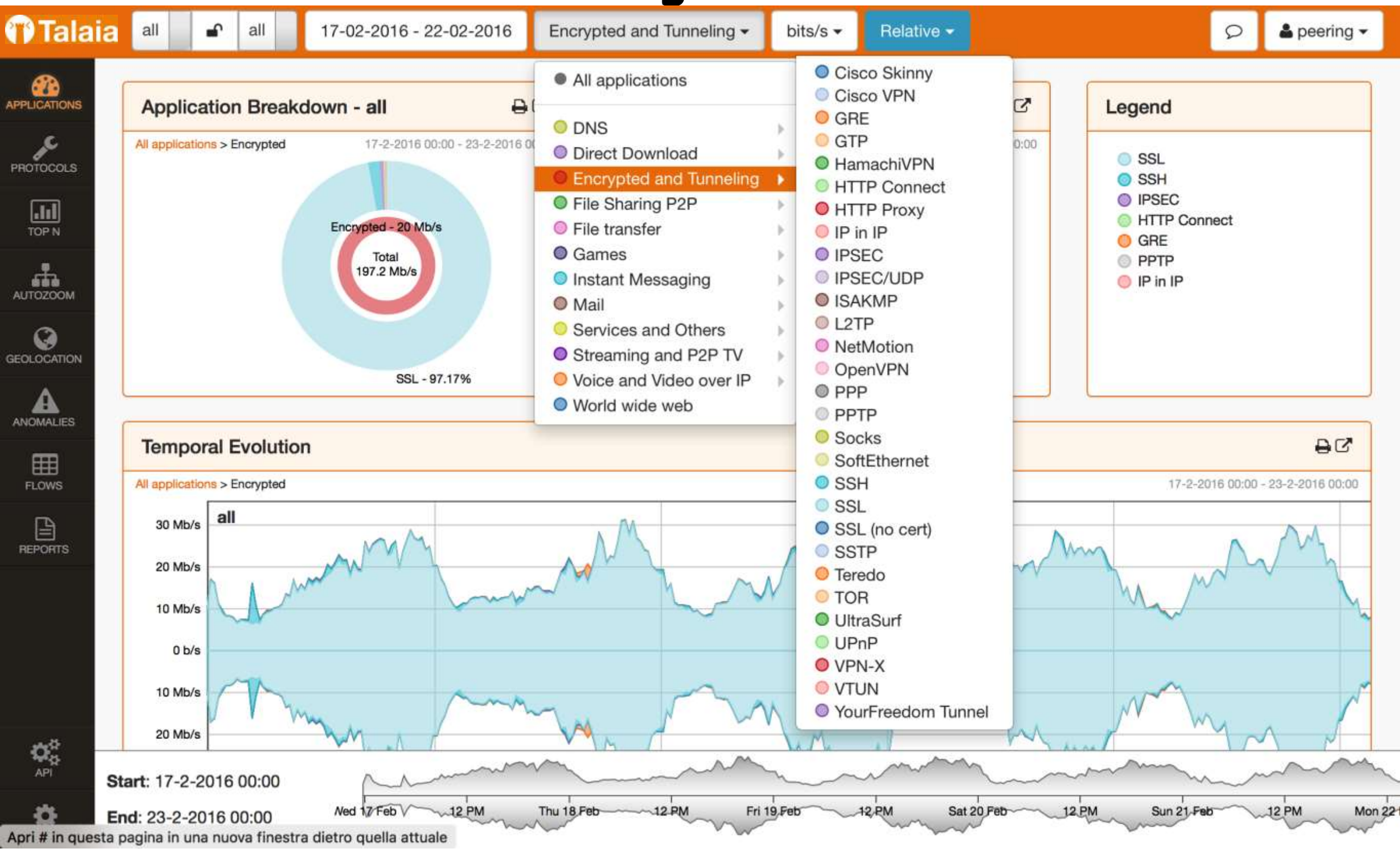
Demonstração “ao vivo”



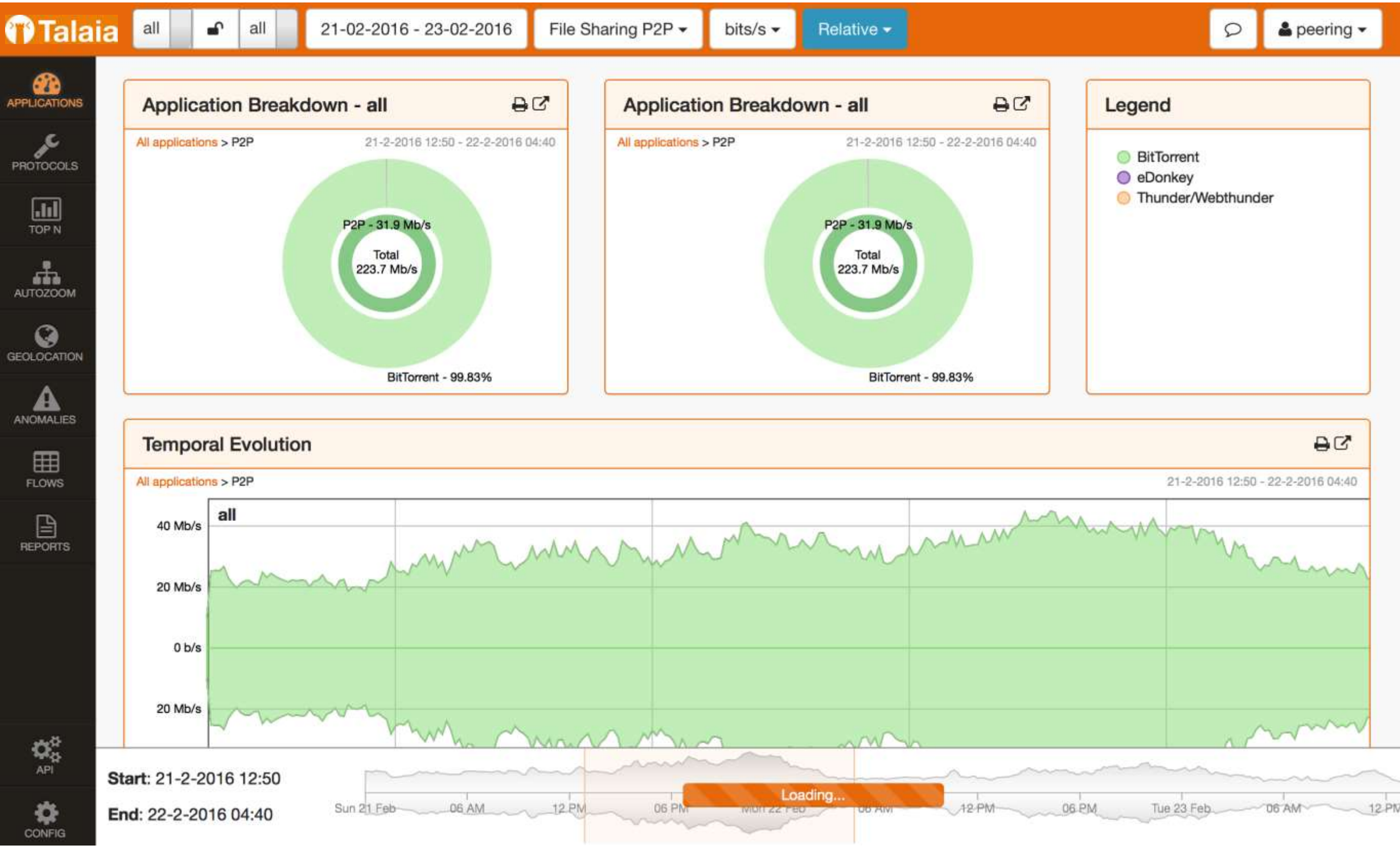
Demonstração “ao vivo”



Demonstração “ao vivo”



Demonstração “ao vivo”



Demonstração “ao vivo”

- CitrixOnline GotoMeeting
- FiCall
- Generic Voice
- H323
- IAX
- Iskoot
- Lync
- MGCP
- MyPeople
- NOE
- ooVoo
- Scydo
- SIP
- Skype
- Tango
- TeamSpeak
- Truphone
- Ventrilo
- Viber
- VoipSwitch VoIP Tunnel
- AdobeCon…
- Apple iTunes
- AVI
- DCE RPC
- Feidian
- FLASH
- Funshion
- Grooveshark
- Icecast
- iPlayer
- IPTV
- Kontiki
- Last.fm
- MMS
- Mojo
- Move
- MPEG
- Multimedia…
- NetFlix
- Octoshape
- OGG
- OGG Vorbis
- ORB
- Pandora
- PPLIVE
- PPSTREAM
- QQLive
- QUICKTIME
- RealDataTr…
- REALMEDIA
- RTCP
- RTP
- RTSP
- Shoutcast
- Slingbox
- SOPCAST
- Spotify
- TVANTS
- TVUPLAYER
- Vcast
- VeohTV
- VeohTV
- Webex
- WebM
- WINDOWS…
- YouTube
- ZATTOO
- Gmail
- IMAP
- IMAPs
- Lotus Notes
- POP
- POPS
- SMTP
- SMTPs

Demonstração “ao vivo”

- Activesync
- AFP
- Apple
- BGP
- Blackberry
- Citrix
- CitrixGoTo
- collectd
- ComodoUnite
- Corba
- DHCP
- DHCPv6
- EGP
- I23V5
- ICMP
- ICMPv6
- IGMP
- IPP
- JAP
- JBK3000
- Kerberos
- LDAP
- LDP
- LPD
- Mapi
- msSQL
- MySQL
- NETBIOS
- NetFlow/IP…
- NFS
- NTP
- Oracle
- OSPF
- PCAnywhere
- PostgreSQL
- RADIUS
- RDP
- RemoteScan
- RSync
- SAP
- SCTP
- sFlow
- Skinny
- SMB/CIFS
- SNMP
- Socrates
- SSDP
- STUN
- Syslog
- TDS
- TeamViewer
- Telnet
- Tunnelvoice
- Ubuntu ONE
- UltraBac
- Usenet
- VMWare
- VNC
- VRRP
- WAP-WSP
- WAP-WTLS
- WAP-WTP-…
- WebDAV
- Whois-DAS
- WindowsU…
- XDMCP
- eBuddy
- Fring
- Gadu-Gadu
- Goober
- Google Talk
- IMO
- IMplus
- IRC
- Jabber
- MEEBO
- MSN
- MSRP
- NIMBUZZ
- Oscar
- Paltalk
- POPO
- QQ
- Unencrypted Jabber
- WhatsApp
- XDCC

Demonstração “ao vivo”

- Armagetron
- Battlefield
- ClubPenguin
- CrossFire
- Dofus
- Fiesta
- Florensia
- GameKit
- Guild Wars
- Halflife2
- MapleStory
- PS3
- QQGame
- Quake
- rFactor
- Second Life
- SplashFighter
- Steam
- Warcraft III
- Wii
- World of Kung Fu
- World of Warcraft
- XBOX

- Aimini
- ANtsP2P
- AppleJuice
- Ares
- Bitcoin Mining
- BitTorrent
- DirectConnect
- eDonkey
- eDonkey
- Freenet
- Gnutella
- Gnutella
- iMesh
- Kazaa/Fasttrack
- KaZaa/Fasttrack
- Manolito
- Mute
- OFF
- OpenFT
- Pando
- Soulseek
- Soulseek
- StealthNet
- Thunder/Webthunder
- UUSEE
- WinMX
- WINNY

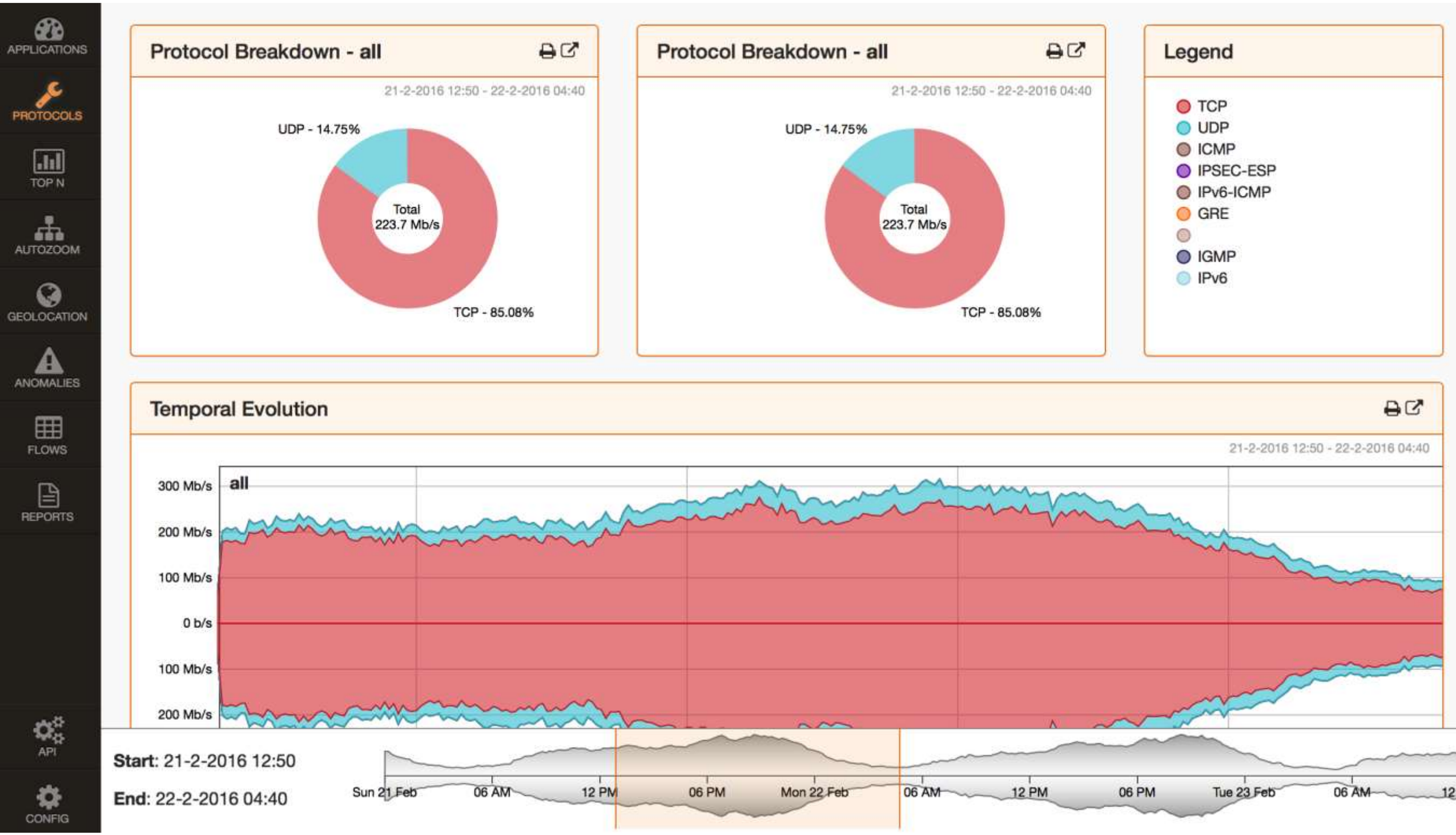
- Cisco Skinny
- Cisco VPN
- GRE
- GTP
- HamachiVPN
- HTTP Connect
- HTTP Proxy
- IP in IP
- IPSEC
- IPSEC/UDP
- ISAKMP
- L2TP
- NetMotion
- OpenVPN
- PPP
- PPTP
- Socks
- SoftEthernet
- SSH
- SSL
- SSL (no cert)
- SSTP
- Teredo
- TOR
- UltraSurf
- UPnP
- VPN-X
- VTUN
- YourFreedom Tunnel

- Apple iCloud
- Dropbox
- FTP
- TFTP

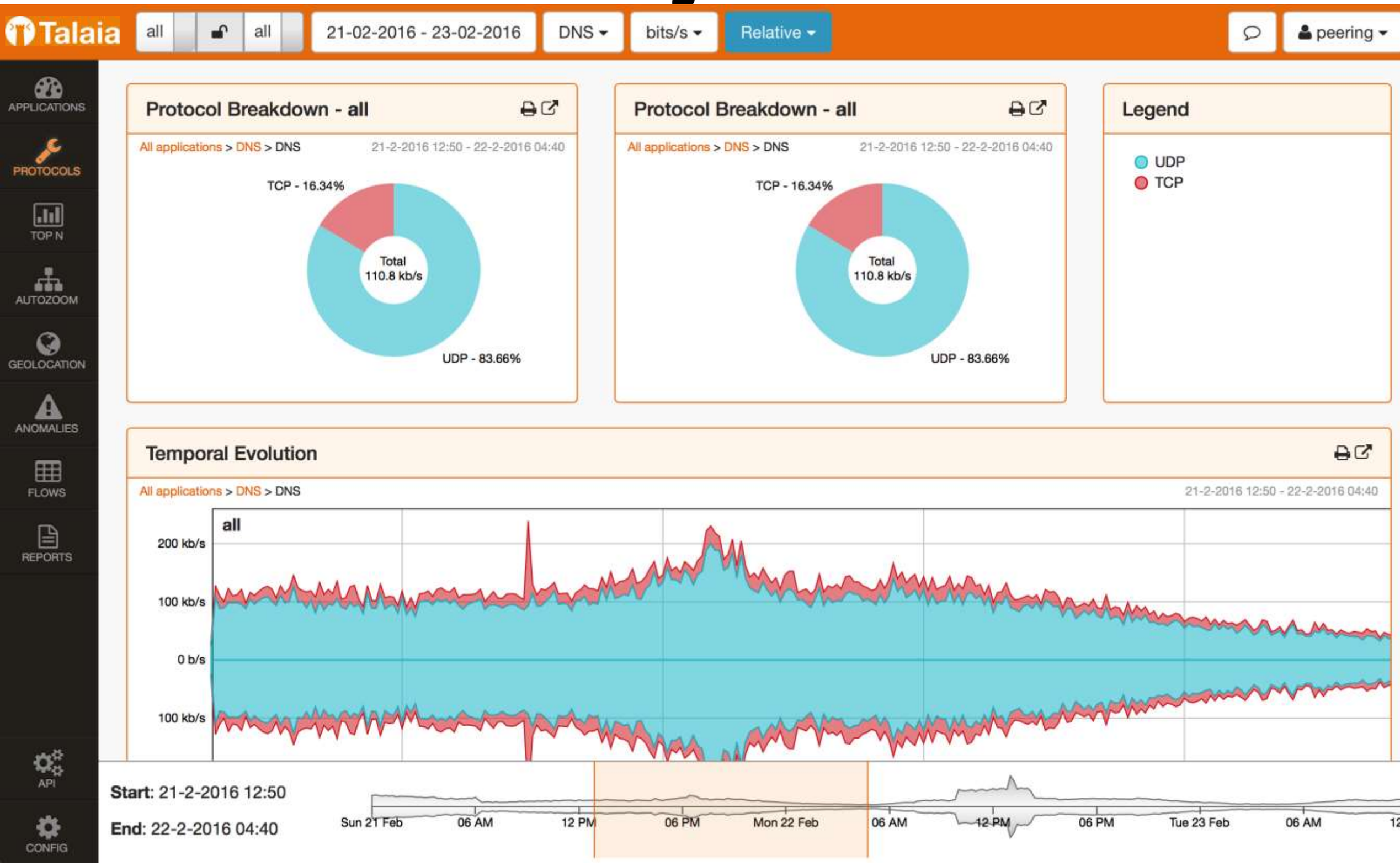
- DirectDownloadLink
- Filetopia
- Skyfile postpaid
- Skyfile prepaid
- Skyfile rudics
- Wuala

- DNS
- LLMNR
- MulticastDNS

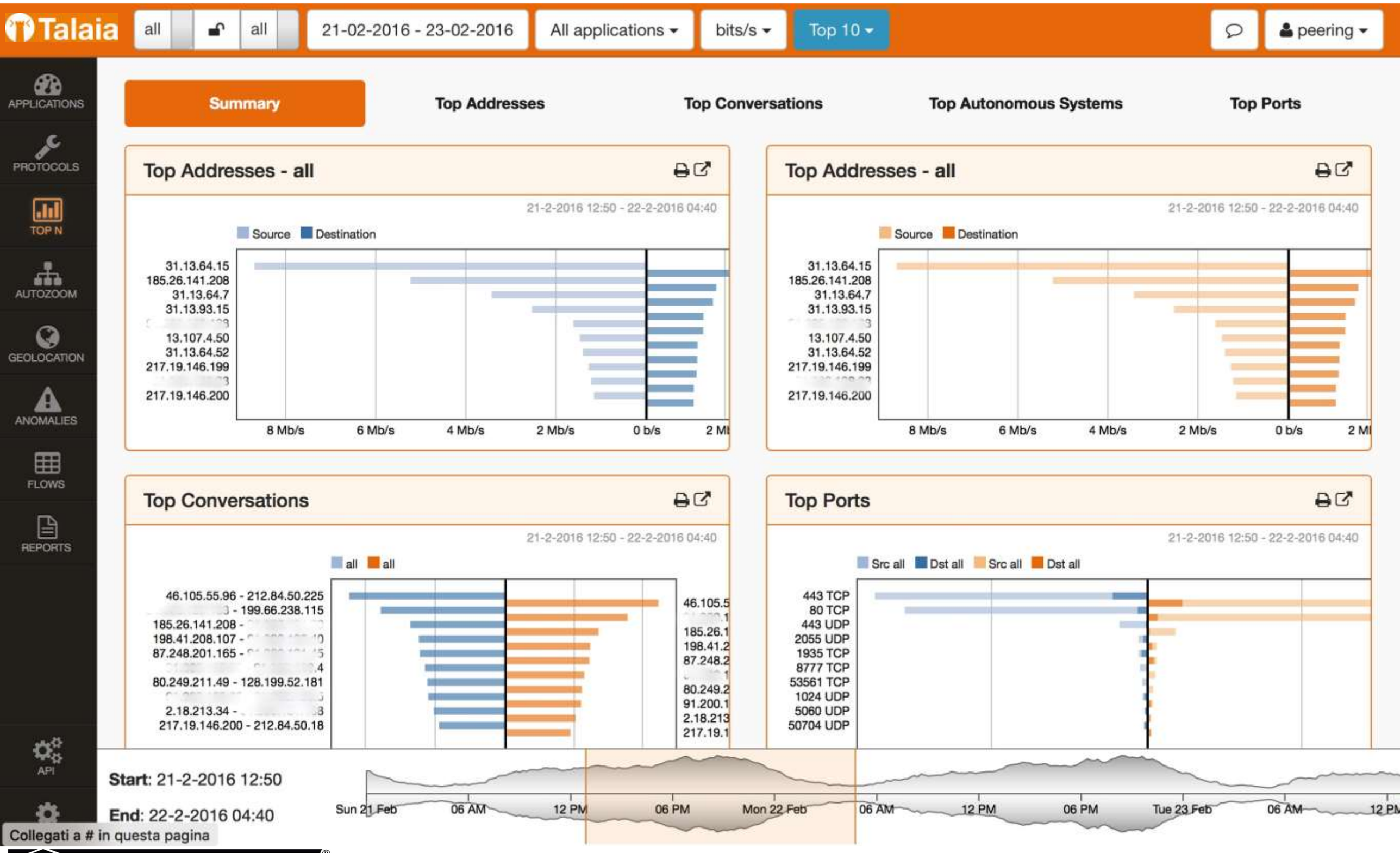
Demonstração “ao vivo”



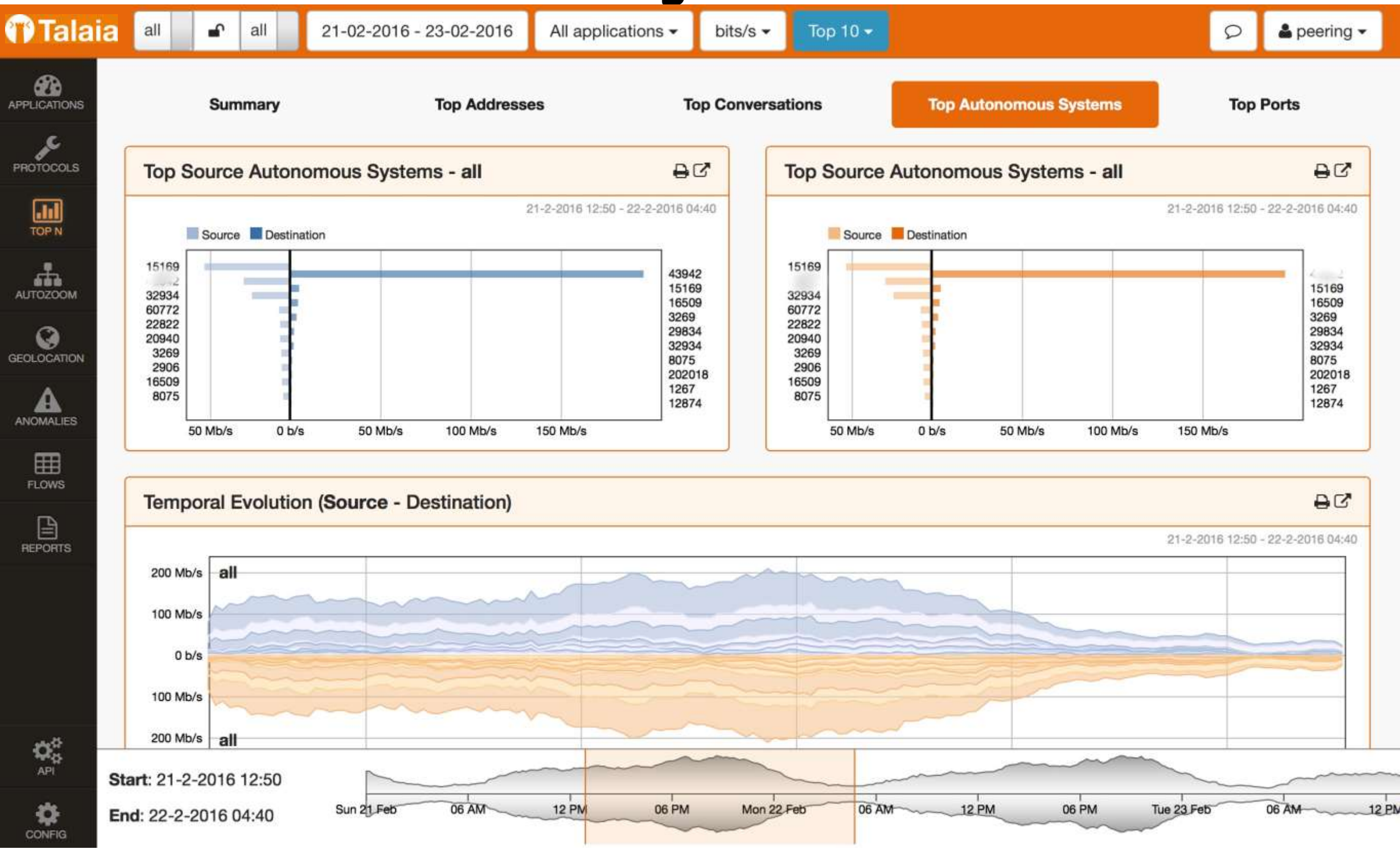
Demonstração “ao vivo”



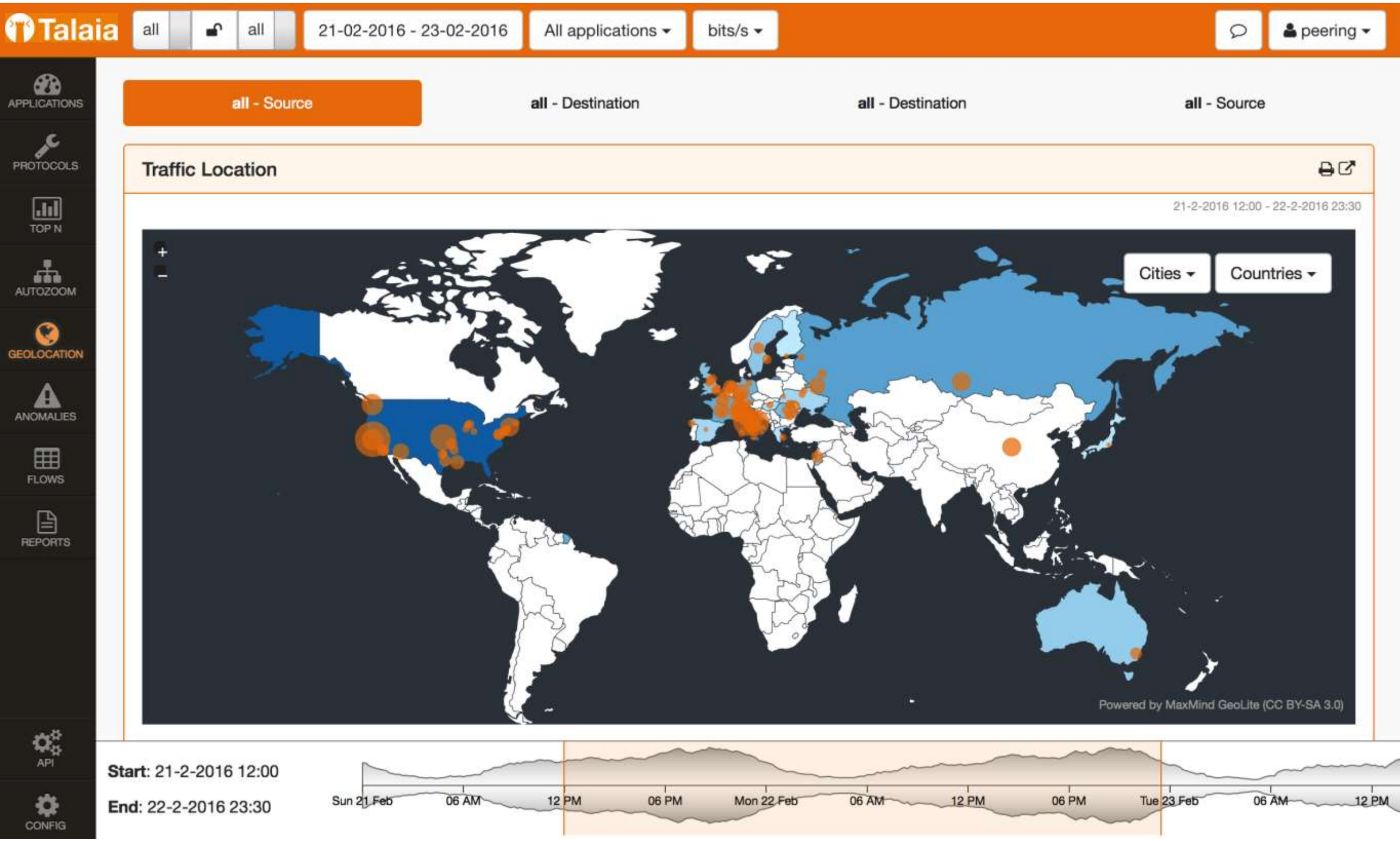
Demonstração “ao vivo”



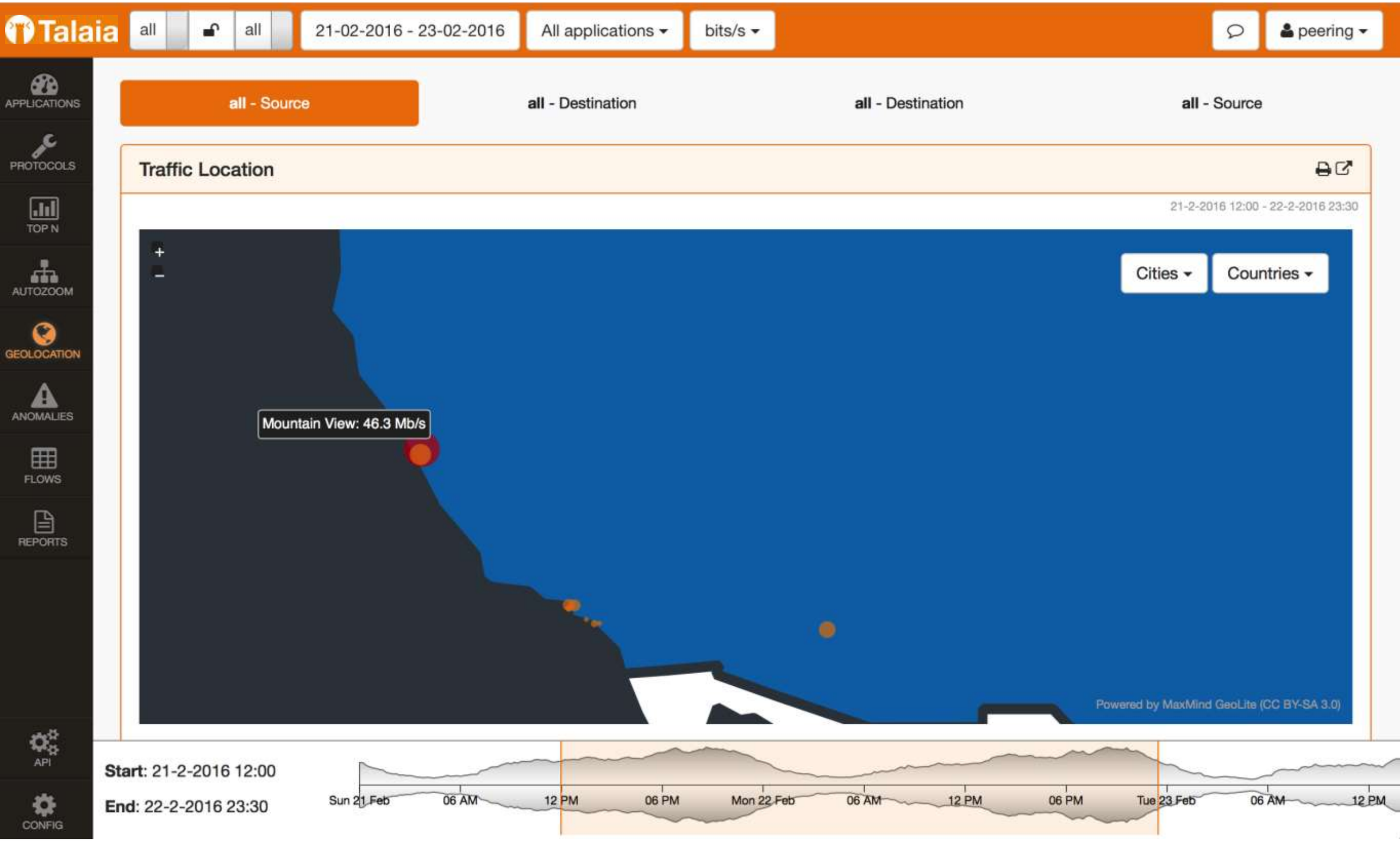
Demonstração “ao vivo”



Demonstração “ao vivo”



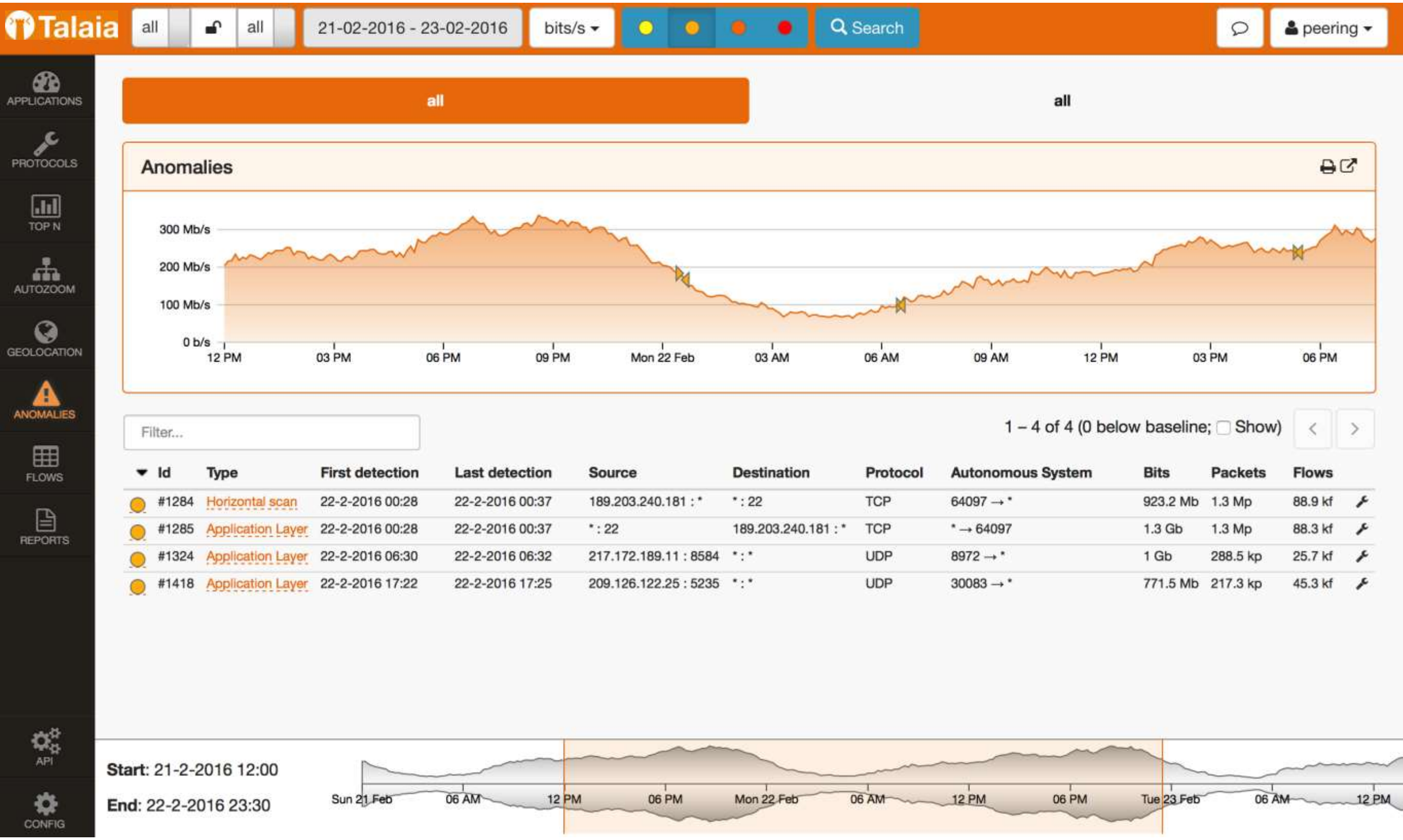
Demonstração “ao vivo”



Demonstração “ao vivo”

Você pode também gerar relatórios, visualizar e exportar os fluxos armazenados, etc……..

Demonstração “ao vivo”



Conclusão

- ✓ Com o Traffic Flow e o NetFlow Analyzer você pode saber o que acontece na sua rede e que tipo de tráfego é trocado entre seus clientes.
- ✓ Com este previlegiado ponto de vista você pode planejar e prever diversas “coisas” para sua rede.

Conclusão

- ✓ Espero que todos adotem este previlegiado “método de monitoramento” o mais breve possível ☺

Obrigado!

Perguntas?

http://training.grifonline.it
training@grifonline.it