

NetFlow:

O que acontece na sua?

Por Lorenzo Busatti

apresentado em português por Guilherme Ramires

BRAZIL ON NOVEMBER 24 - 25, 2016

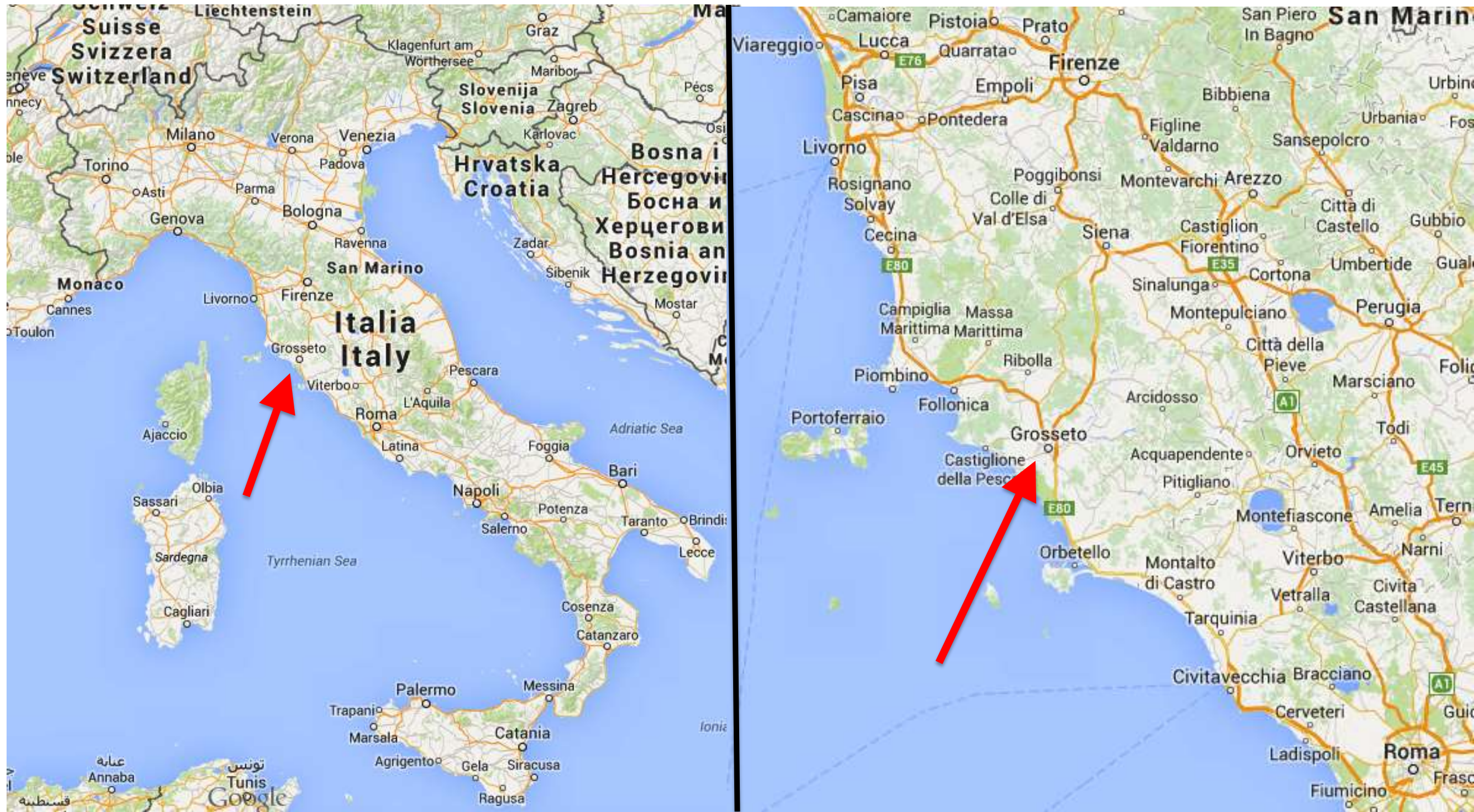
Sobre mim

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



Sobre mim





Eu sou um entusiasta do MikroTik

Eu sou um entusiasta do MikroTik

Eu sou um evangelista
MikroTikiano

Sobre mim

- Fundador da (2016)



**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...

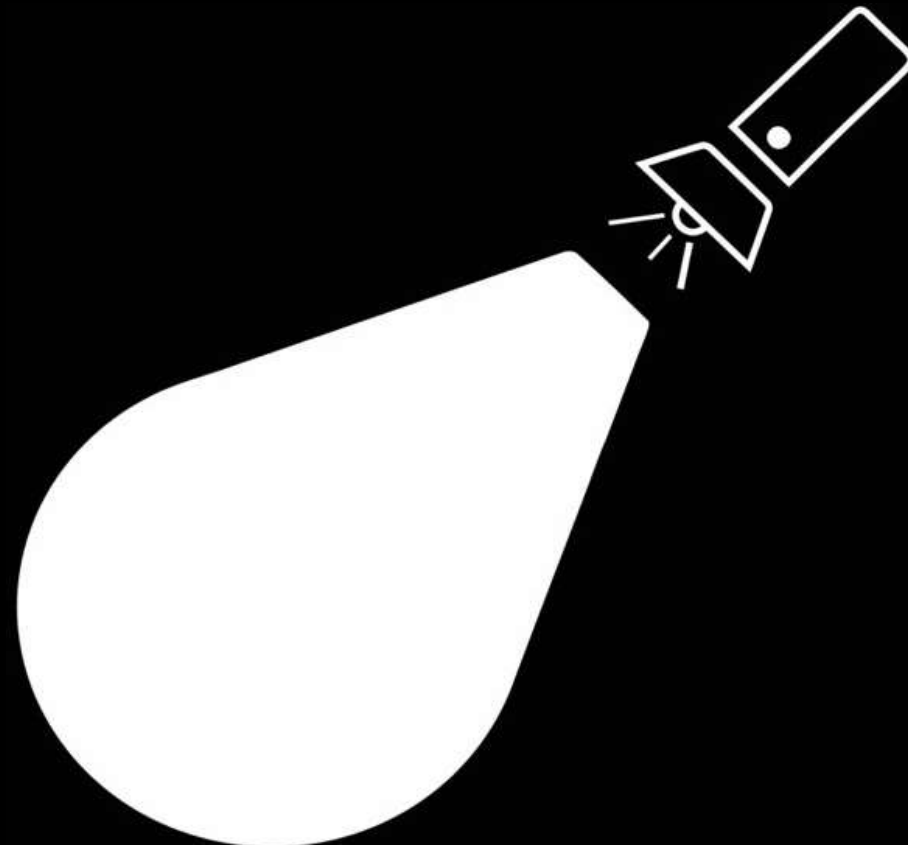
Qual o mais
importante AS que
você deveria estabelecer
conexão?

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 😊



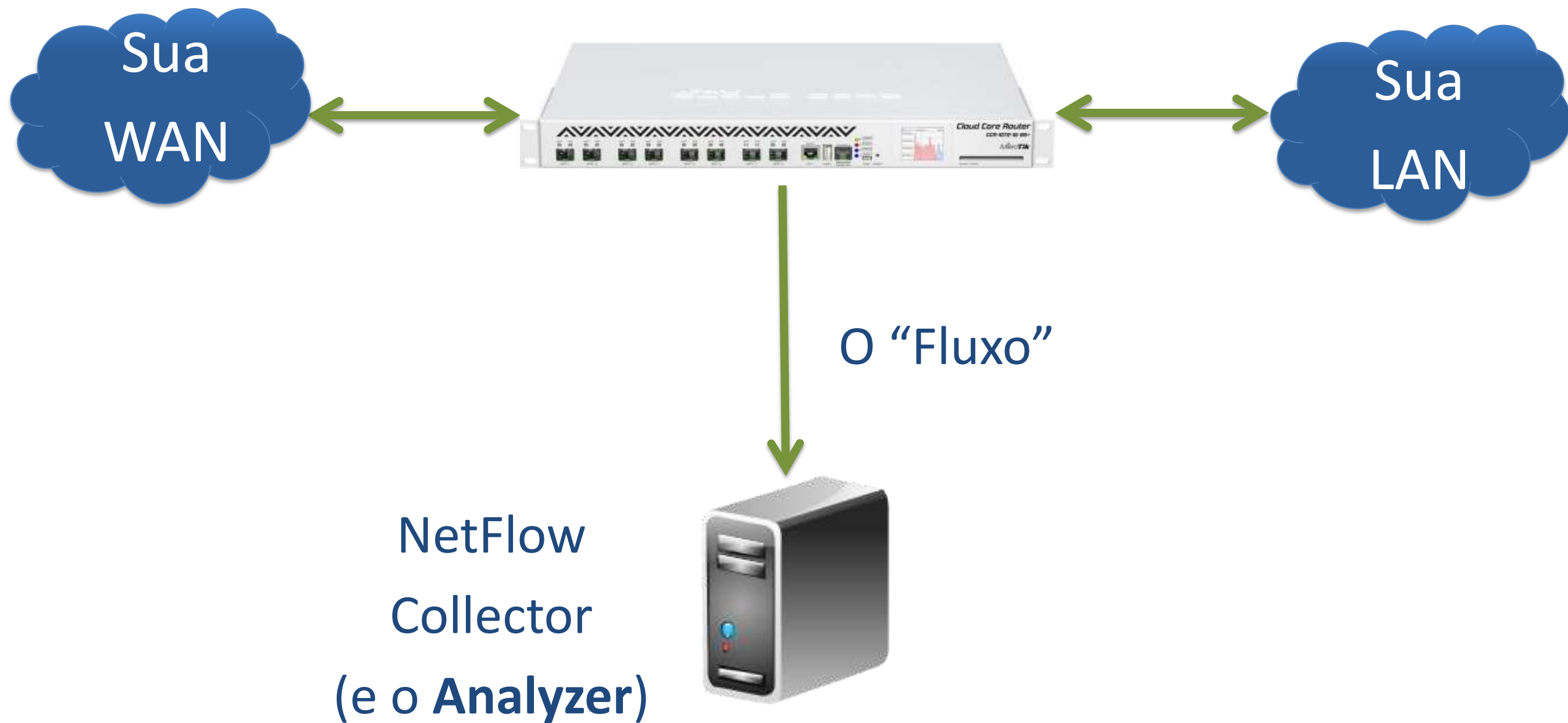
NetFlow em pilulas

- 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

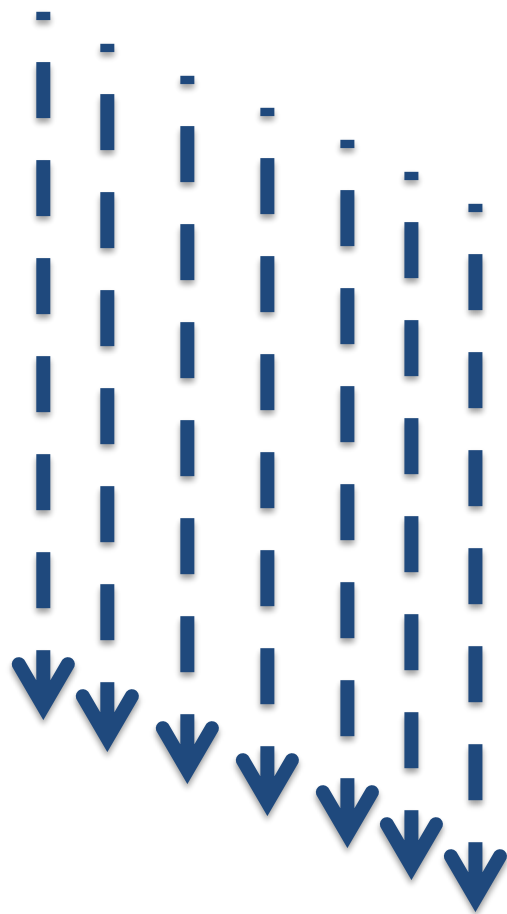
- Sim, suportado!!
- Chamado: **Traffic Flow** (NetFlow é uma nomenclatura própria da Cisco....)
- “Encontrado” no menu: **`/ip traffic-flow`**
- Existe desde o ROS v. 2.9
- Atualmente suporta as **Versões 1, 5, 9**
- **Suporta IPFIX desde o ROS 6.36** 
- Consulte a wiki para identificar as diferenças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

(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 mantém 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	DIRECTION	SRC_AS
OUT_BYTES	IPV4_NEXT_HOP	DST_AS
IN_PKTS	IPV6_SRC_ADDR	BGP_IPV4_NEXT_HOP
OUT_PKTS	IPV6_DST_ADDR	IP_PROTOCOL_VERSION
PROTOCOL	ICMP_TYPE	MPLS_LABEL_(1-10)
SRC_TOS	IN_SRC_MAC	IF_NAME
TCP_FLAGS	IN_DST_MAC	IF_DESC
L4_SRC_PORT	OUT_DST_MAC	
L4_DST_PORT	OUT_SRC_MAC	FORWARDING STATUS (muitos sub-códigos!!!)
IPV4_SRC_ADDR	SRC_VLAN	
IPV4_DST_ADDR	DST_VLAN	



Visão do tráfego ao vivo



O cabeçalho do pacote

731 1... 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: 91.200.120.30, Dst: 91.200.120.1
- ▶ 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)

▼ 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)

FlowSet Id: (Data) (256)

FlowSet Length: 1384

[\[Template Frame: 19\]](#)

- Flow 1
- Flow 2
- Flow 3
- Flow 4
- Flow 5
- Flow 6
- Flow 7

- Flow 8
- Flow 9
- Flow 10
- Flow 11
- Flow 12
- Flow 13
- Flow 14
- Flow 15
- Flow 16
- Flow 17
- Flow 18
- Flow 19
- Flow 20



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: 192.168.1.100
 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: 192.168.1.100
 Post NAT Destination IPv4 Address: 85.73.239.223
 Post NAT Source Transport Port: 0
 Post NAT 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?

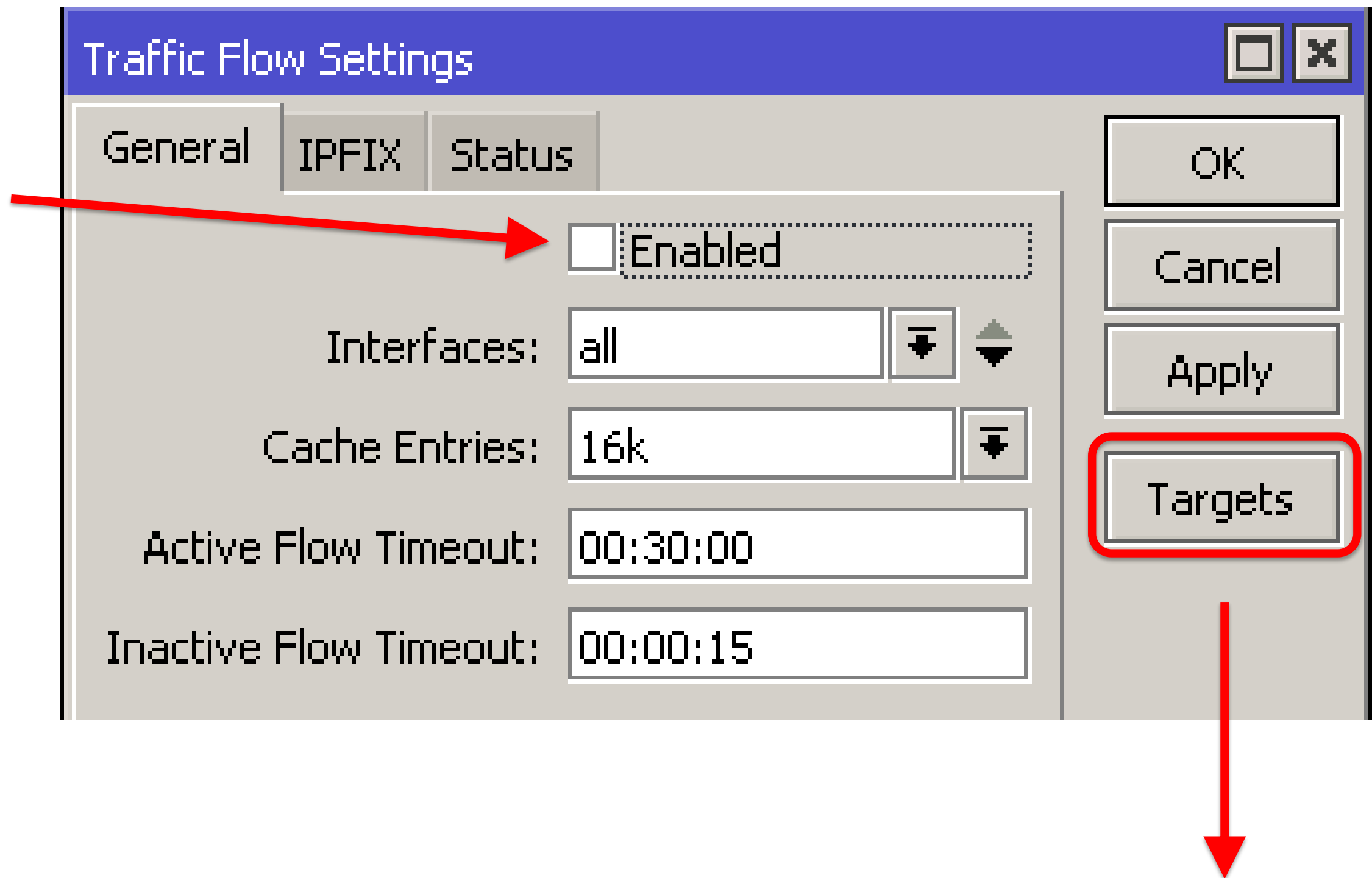
https://en.wikipedia.org/wiki/IP_Flow_Information_Export

Sumário

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

Configurando o router

IP → Traffic Flow



IP → Traffic Flow - Targets

The image shows two windows from a network management application. The main window, titled "Traffic Flow Targets", has a toolbar with a red box around the "+" button. It contains a table with two entries:

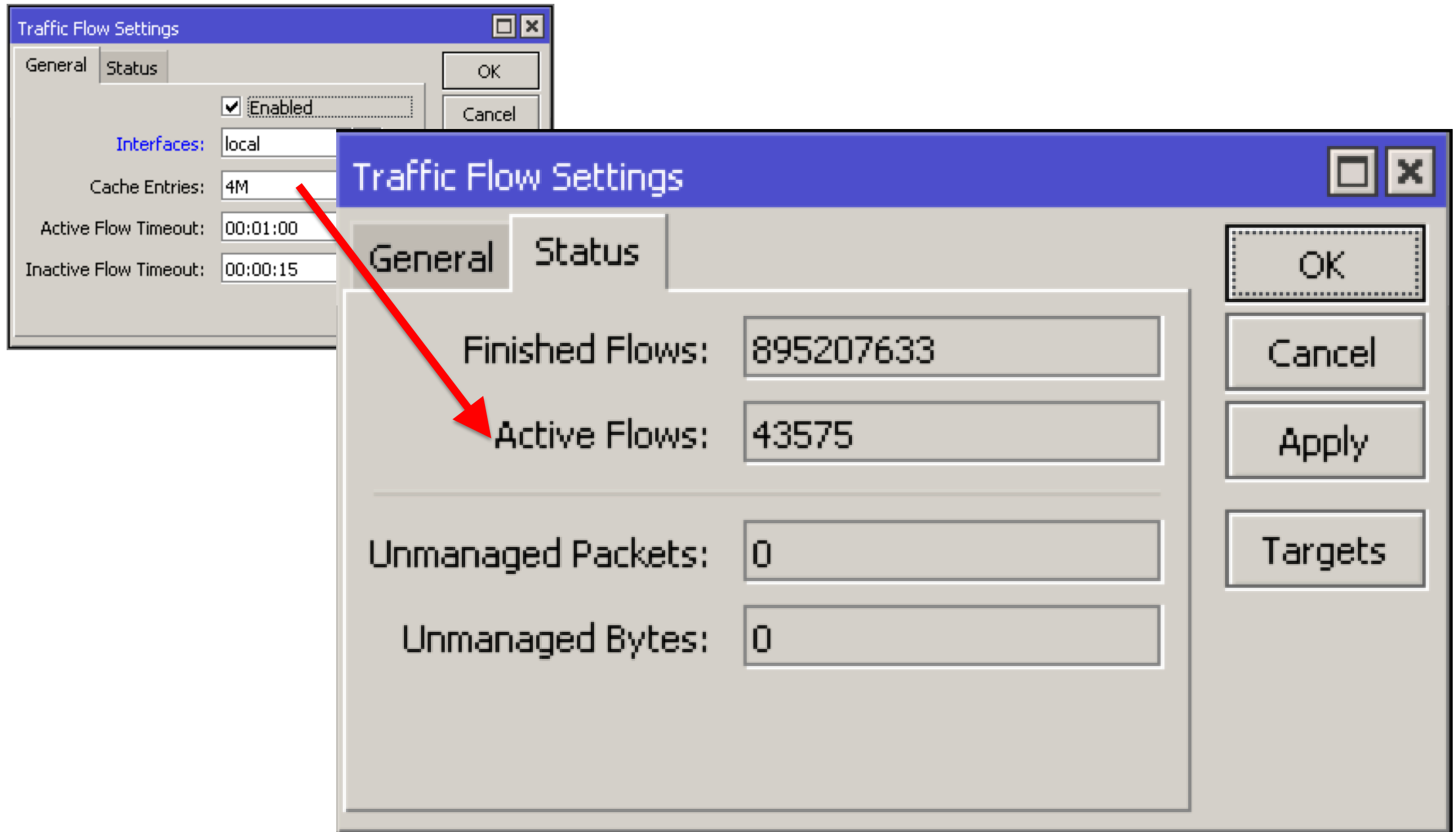
Src. Address	Dst. Address	Port	Version
1.2.3.4	2055	9	
5.6.7.8	2055	IPFIX	

The bottom of the main window shows "2 items". Overlaid on this is the "New Traffic Flow Target" dialog box. It has fields for:

- Src. Address: (empty)
- Dst. Address: <NetFlowCollectorIP> (indicated by a red arrow)
- Port: 2055
- Version: 9 (indicated by a red arrow)
- v9/IPFIX Template Refresh: 20
- v9/IPFIX Template Timeout: 1800

Buttons on the right include OK, Cancel, Apply, Copy, and Remove.

IP → Traffic Flow → Status



IPFIX settings

The screenshot shows a window titled "Traffic Flow Settings" with a blue title bar and standard window controls. It has three tabs: "General", "IPFIX", and "Status". The "IPFIX" tab is selected. The main area contains a list of 28 IPFIX fields, each with a checked checkbox. The fields are arranged in two columns. On the right side of the dialog, there are four buttons: "OK", "Cancel", "Apply", and "Targets".

Field	Field
☒ Last Forwarded	☒ Packets
☒ First Forwarded	☒ Bytes
☒ In Interface	☒ Src. Address
☒ Out Interface	☒ Dst. Address
☒ Src. Port	☒ Protocol
☒ Dst. Port	☒ IP ToS
☒ Gateway	☒ Dst. Address Mask
☒ Src. Address Mask	☒ TCP Flags
☒ Dst. MAC Address	☒ NAT Src. Address
☒ Src. MAC Address	☒ NAT Dst. Address
☒ NAT Src. Port	☒ IPv6 Flow Label
☒ NAT Dst. Port	☒ TTL
☒ Is Multicast	☒ IP Total Lenth
☒ IP Header Length	☒ UDP Length
☒ TCP Seq. Number	☒ TCP Window Size
☒ TCP Ack. Number	☒ IGMP Type
☒ ICMP Type	
☒ ICMP Code	

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 “tráfico”

The router traffic

Interface <ether8>			
General	Ethernet	Status	Traffic
Tx/Rx Rate:		297.9 Mbps	/ 39.8 Mbps
Tx/Rx Packet Rate:		33 166 p/s	/ 25 196 p/s

The sessions

2050 items out of 89656

The “Flows”

Eth. P... ▲	Pro...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate
800 (ip)	17 ...	...	...: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 legíveis 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



Qual escolher?

Eu não representante de vendas de nenhuma dessas marcas.

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

Qual escolher?

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



(14 dias para teste)

<http://talaia.io>

Porém a parte mais
importante é:

O que é possível ver?????

Que tráfego?

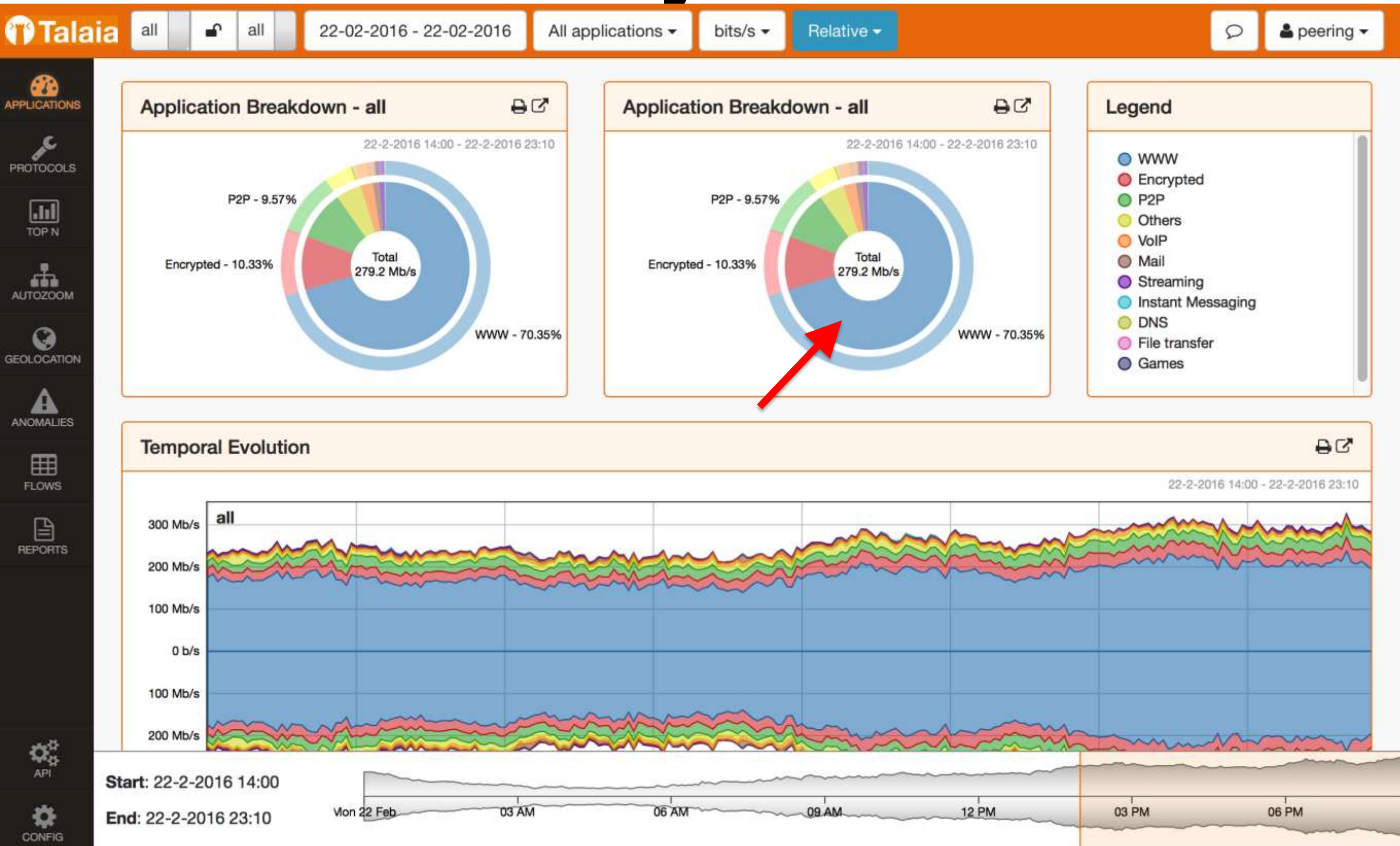
Apenas alguns exemplos:

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

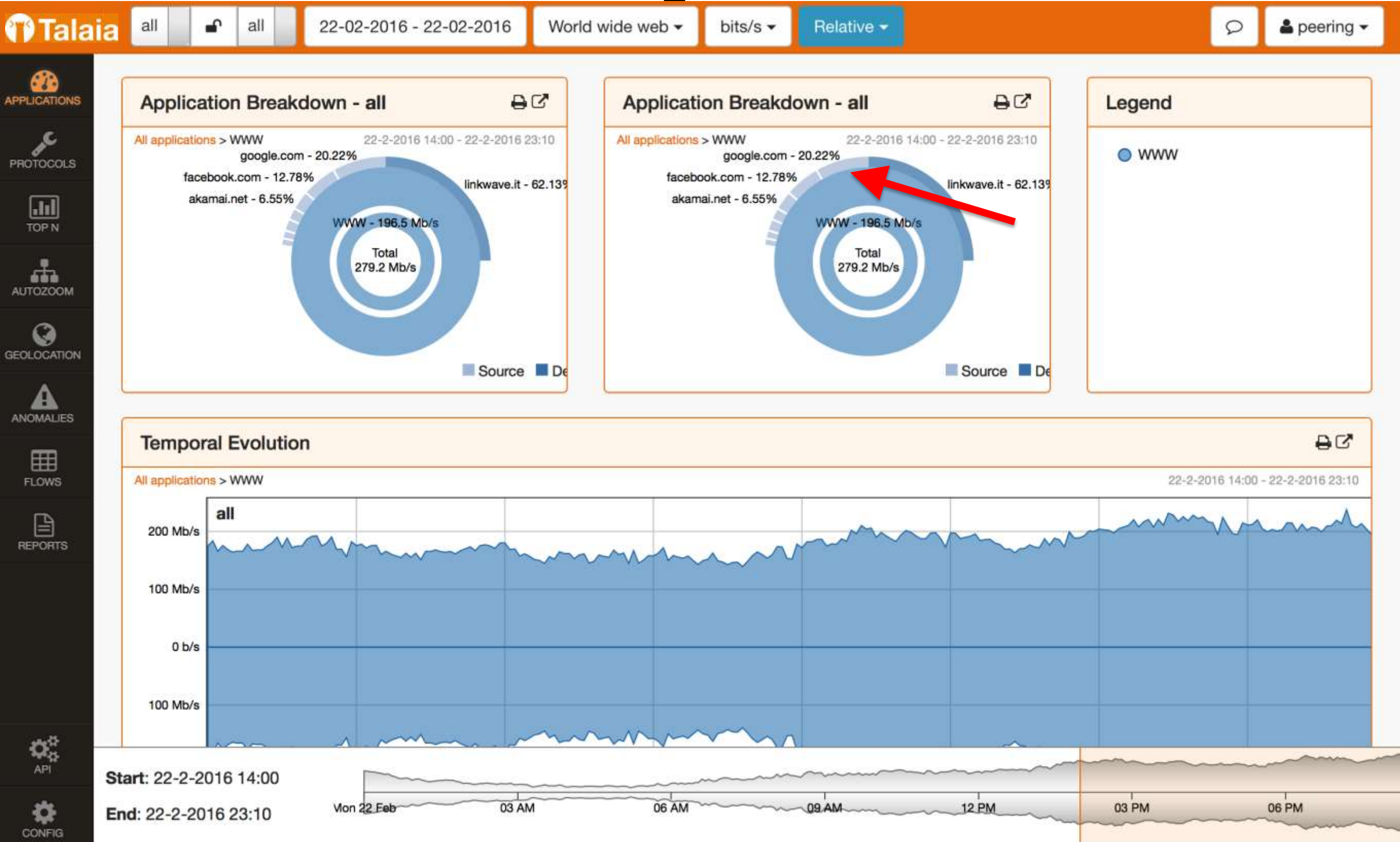
Que tráfico?

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

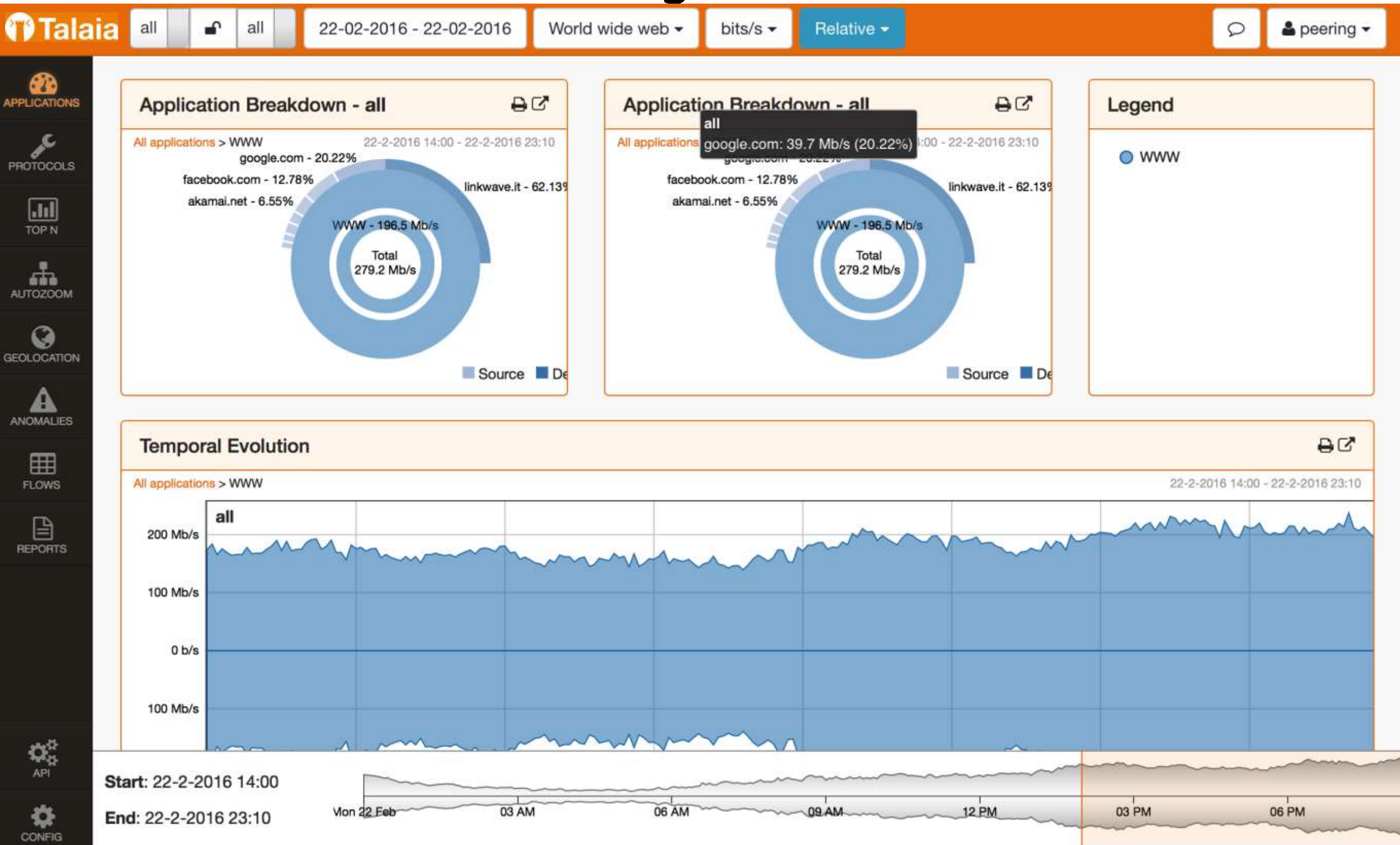
Demonstração “ao vivo”



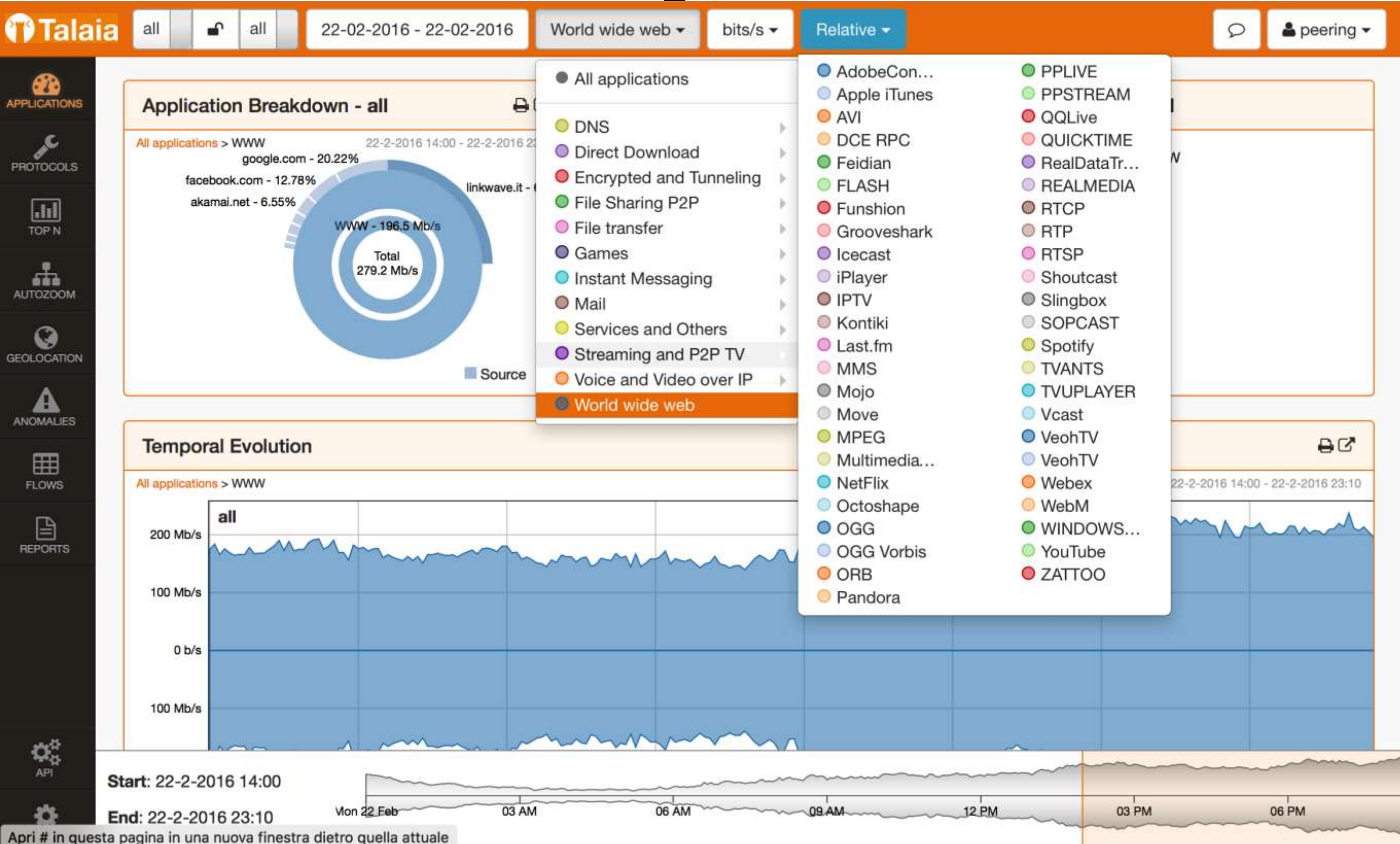
Demonstração “ao vivo”



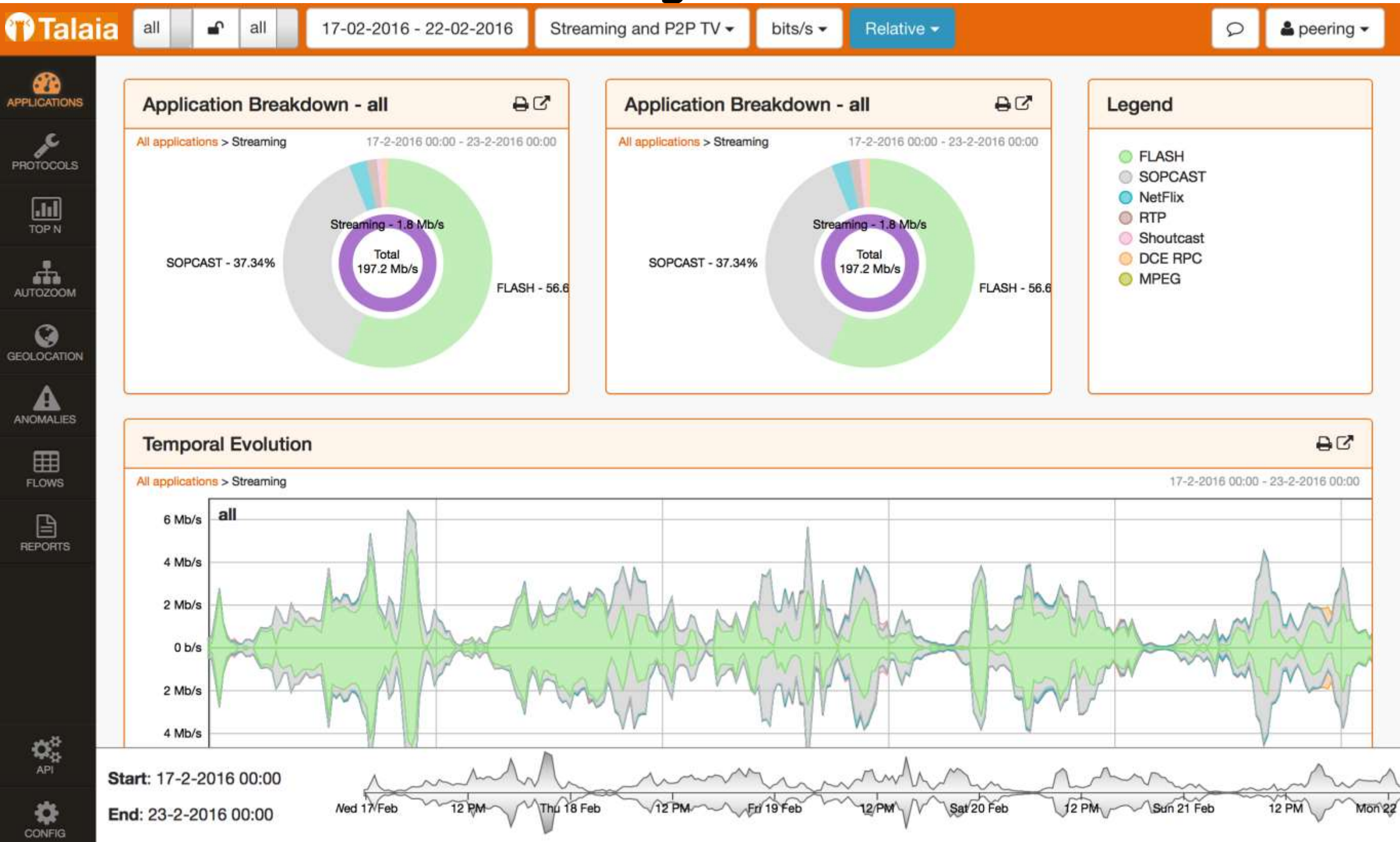
Demonstração “ao vivo”



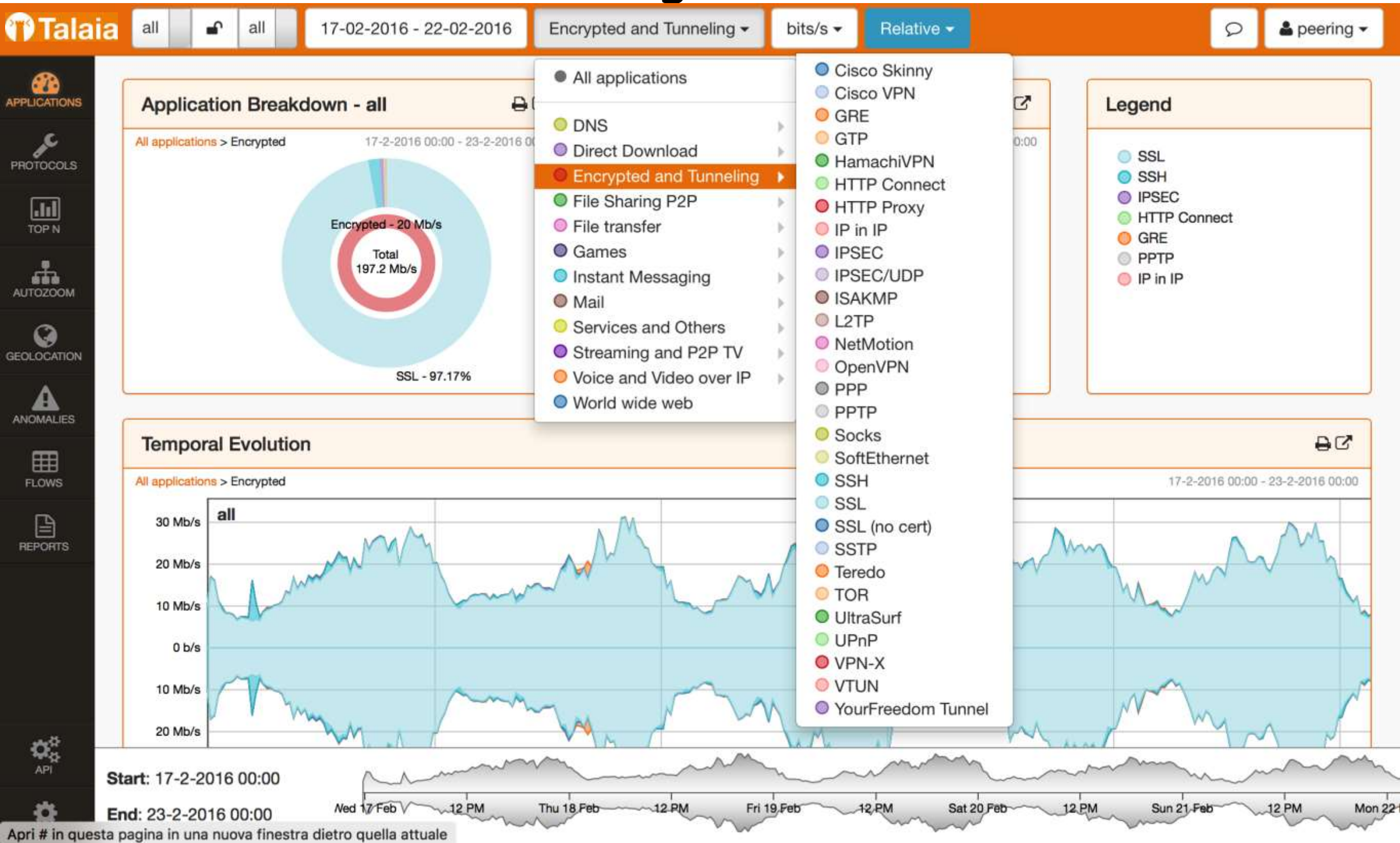
Demonstração “ao vivo”



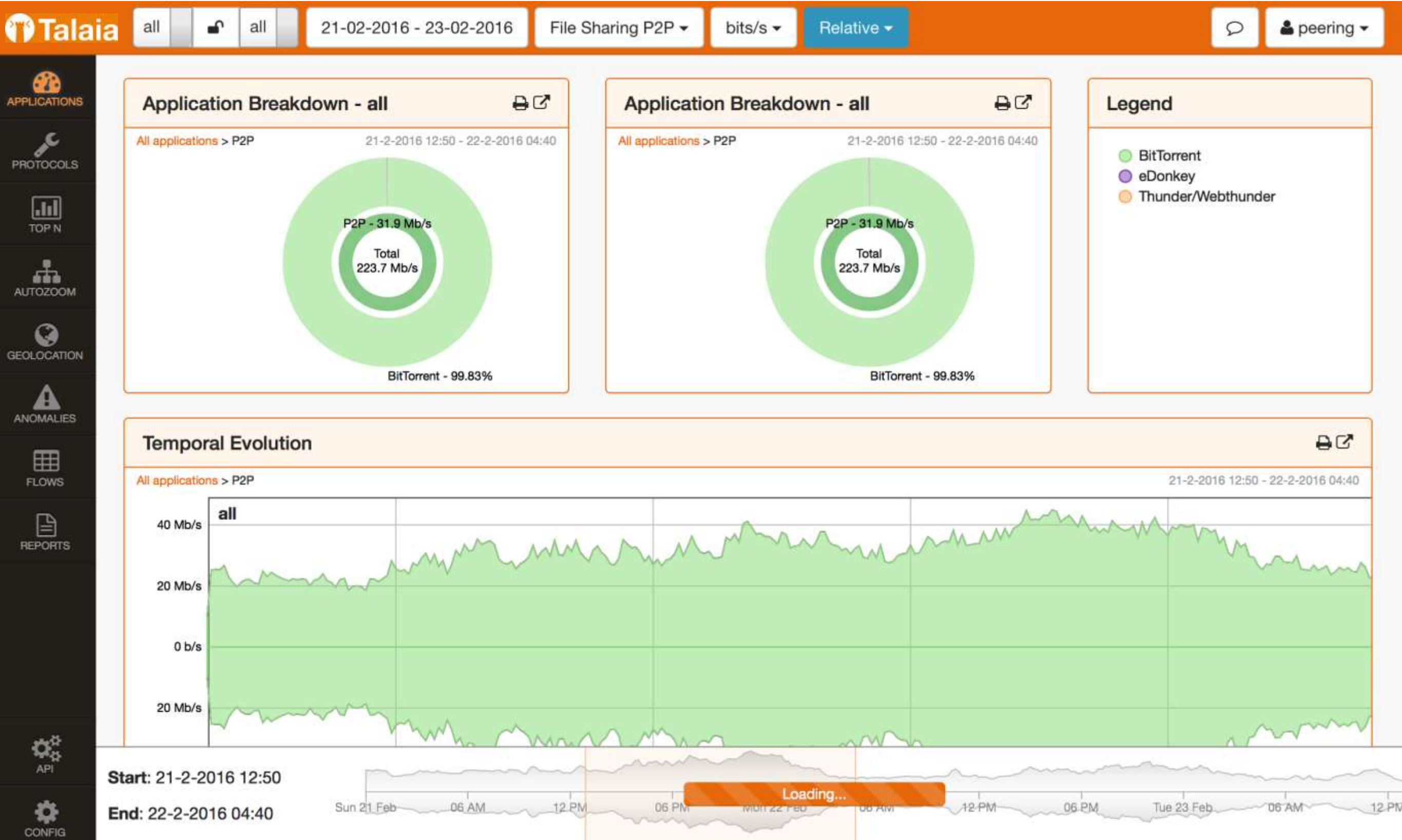
Demonstração “ao vivo”



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

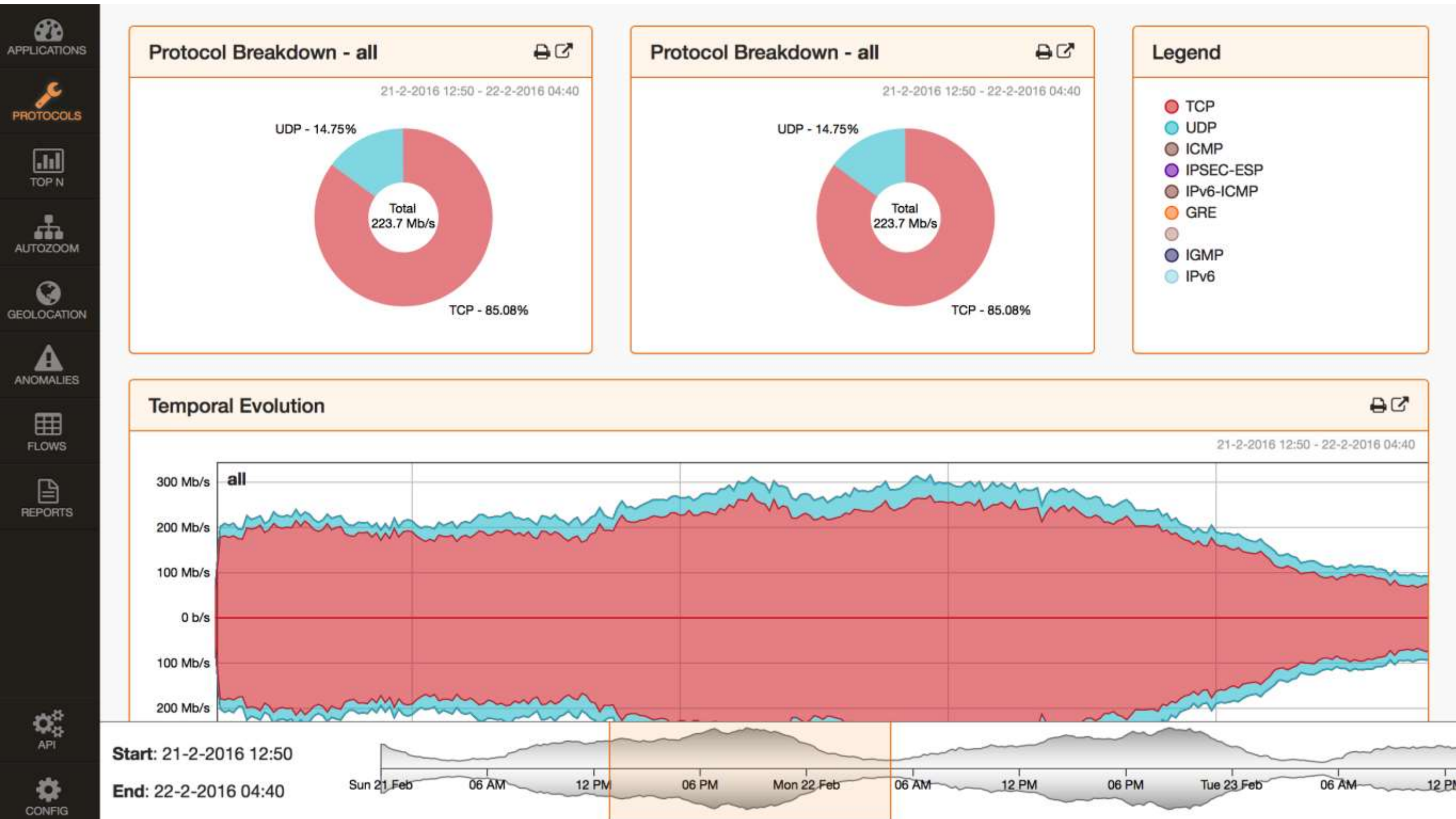
Demonstração “ao vivo”

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

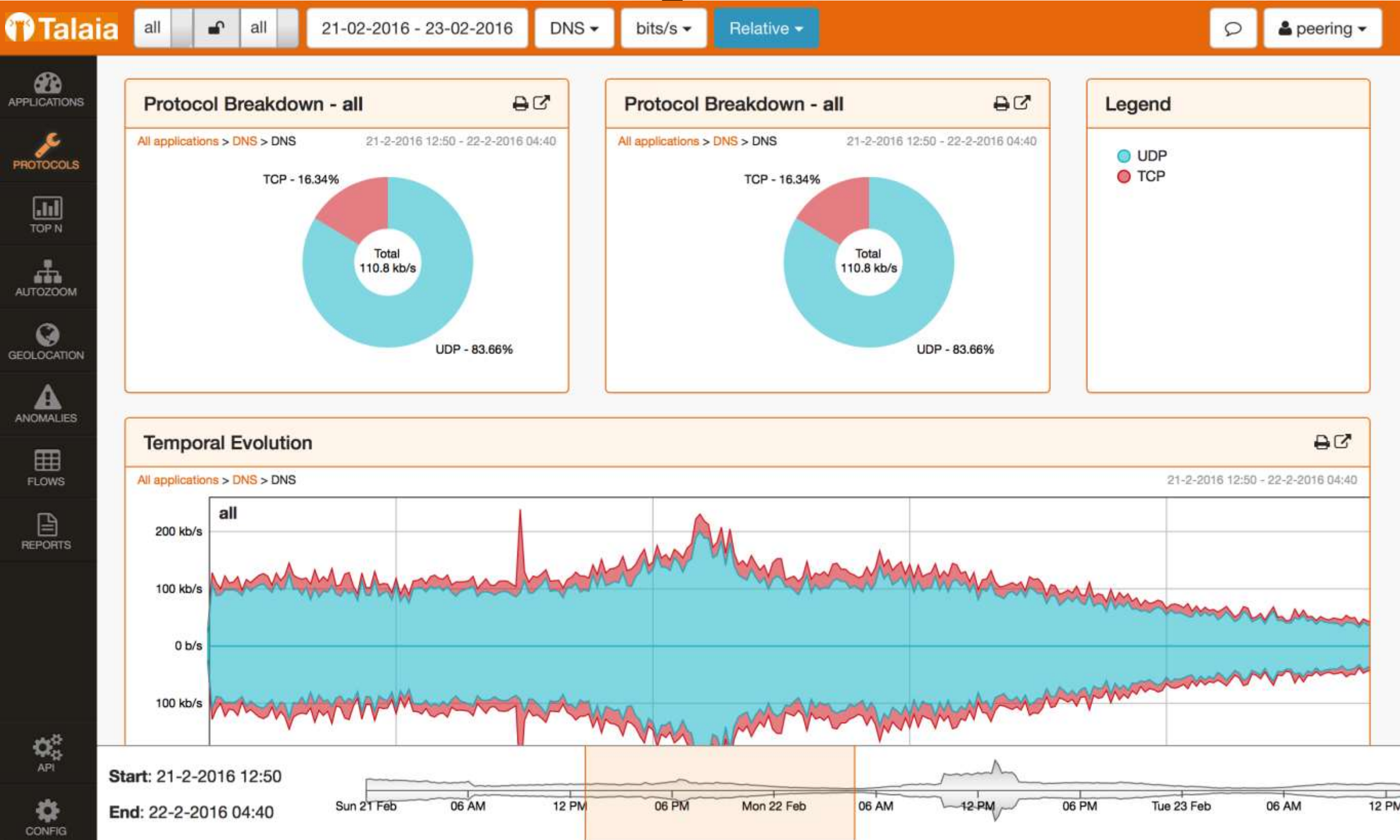
Demonstração “ao vivo”

- Armagetron
- Battlefield
- ClubPenguin
- CrossFire
- Dofus
- Fiesta
- Florencia
- 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

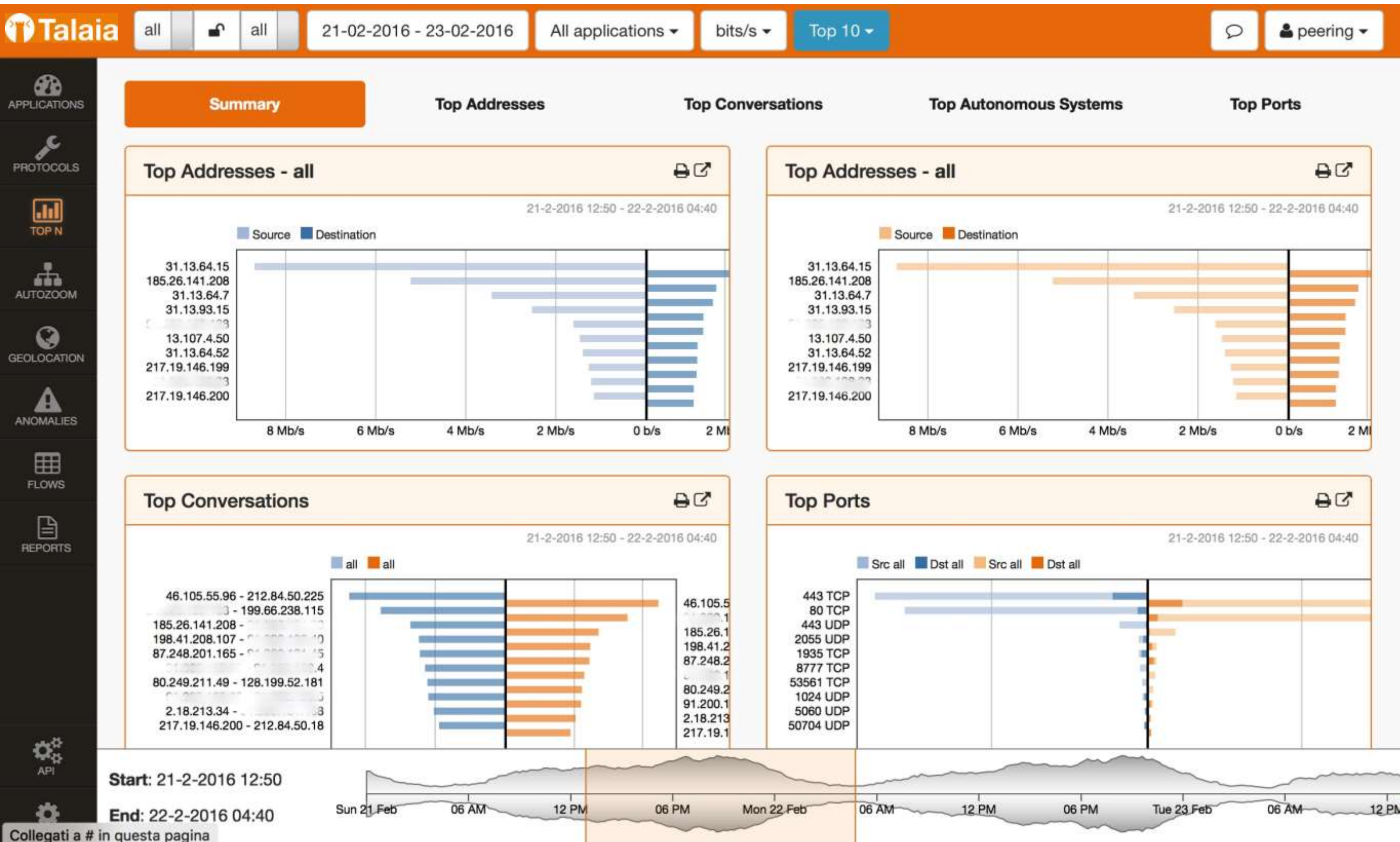
Demonstração “ao vivo”



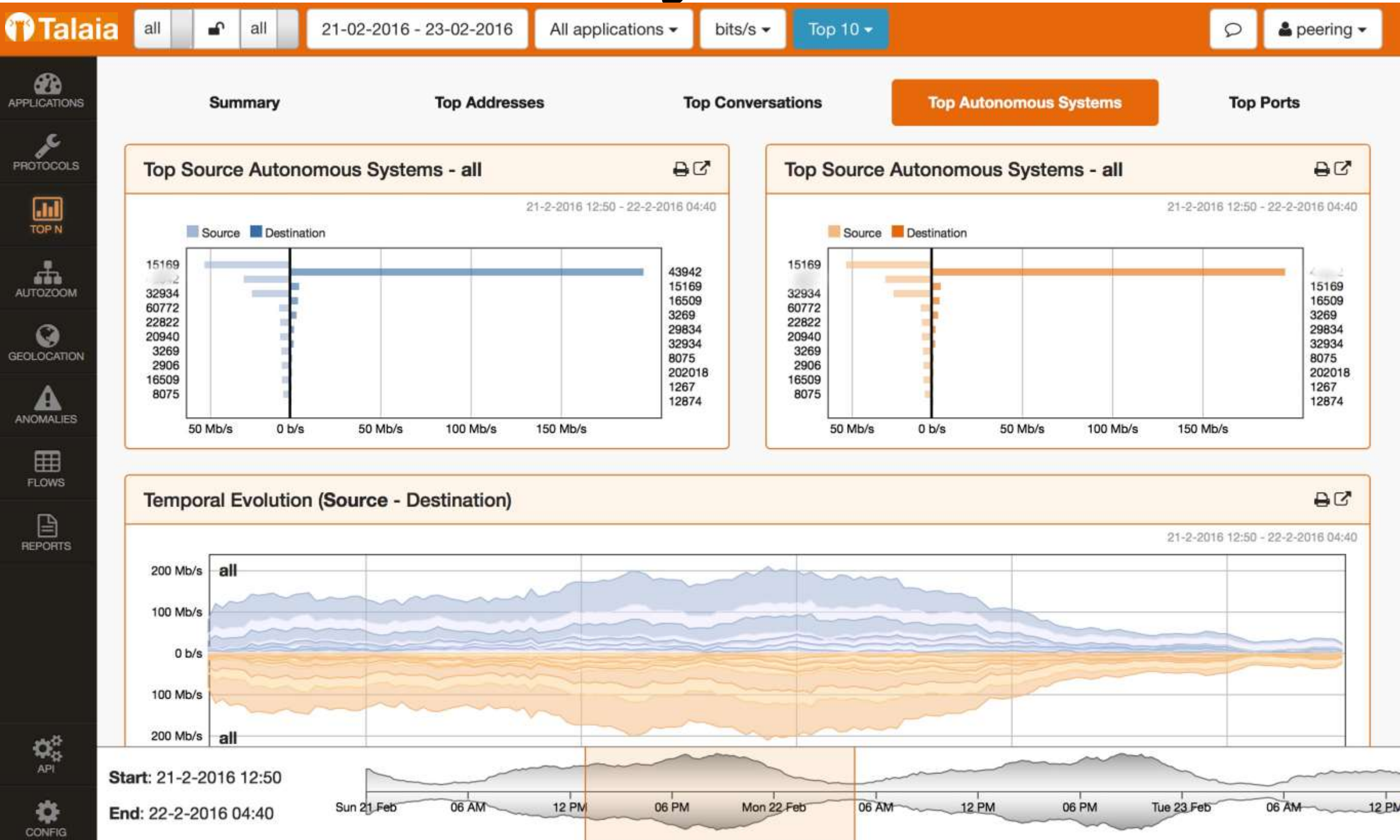
Demonstração “ao vivo”



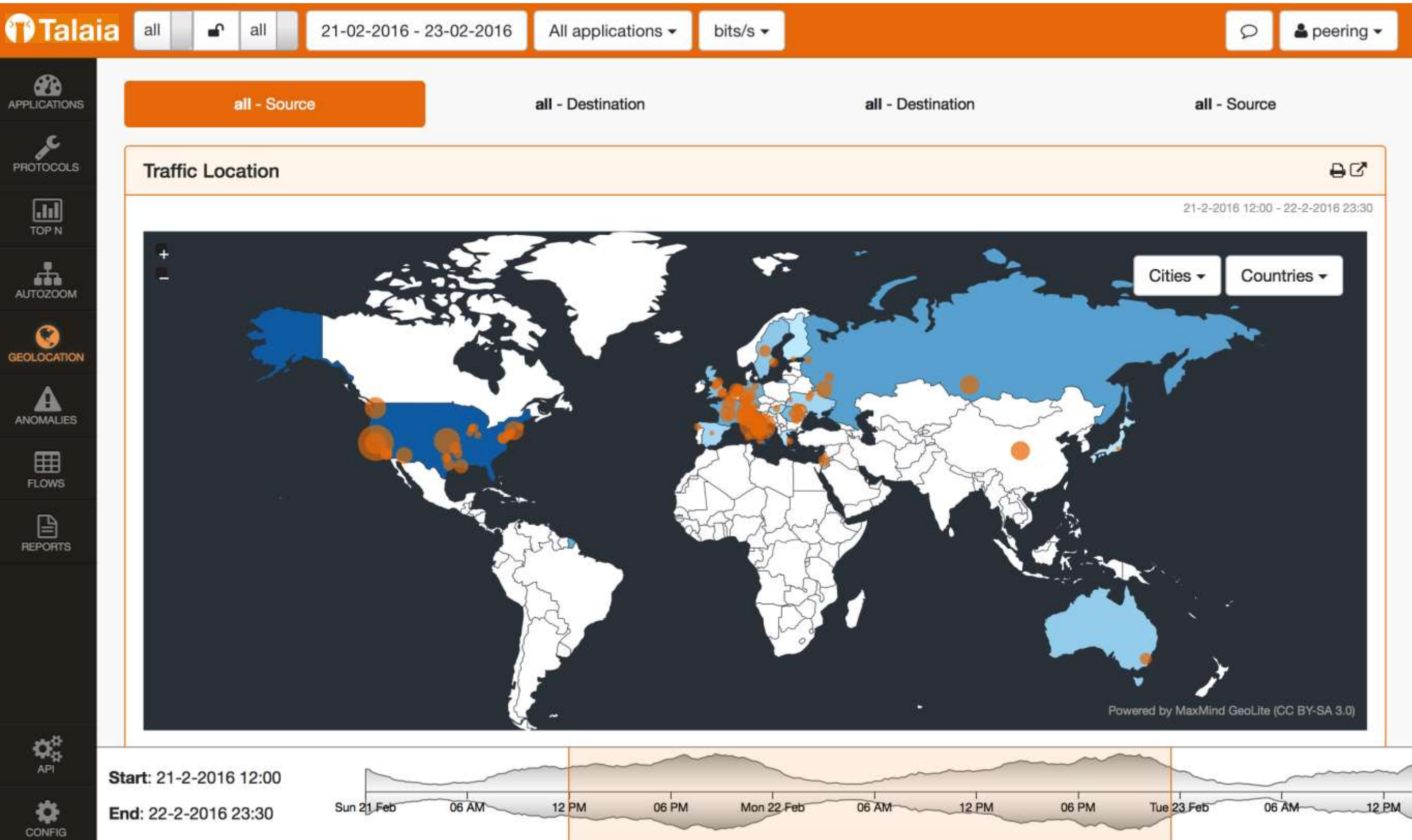
Demonstração “ao vivo”



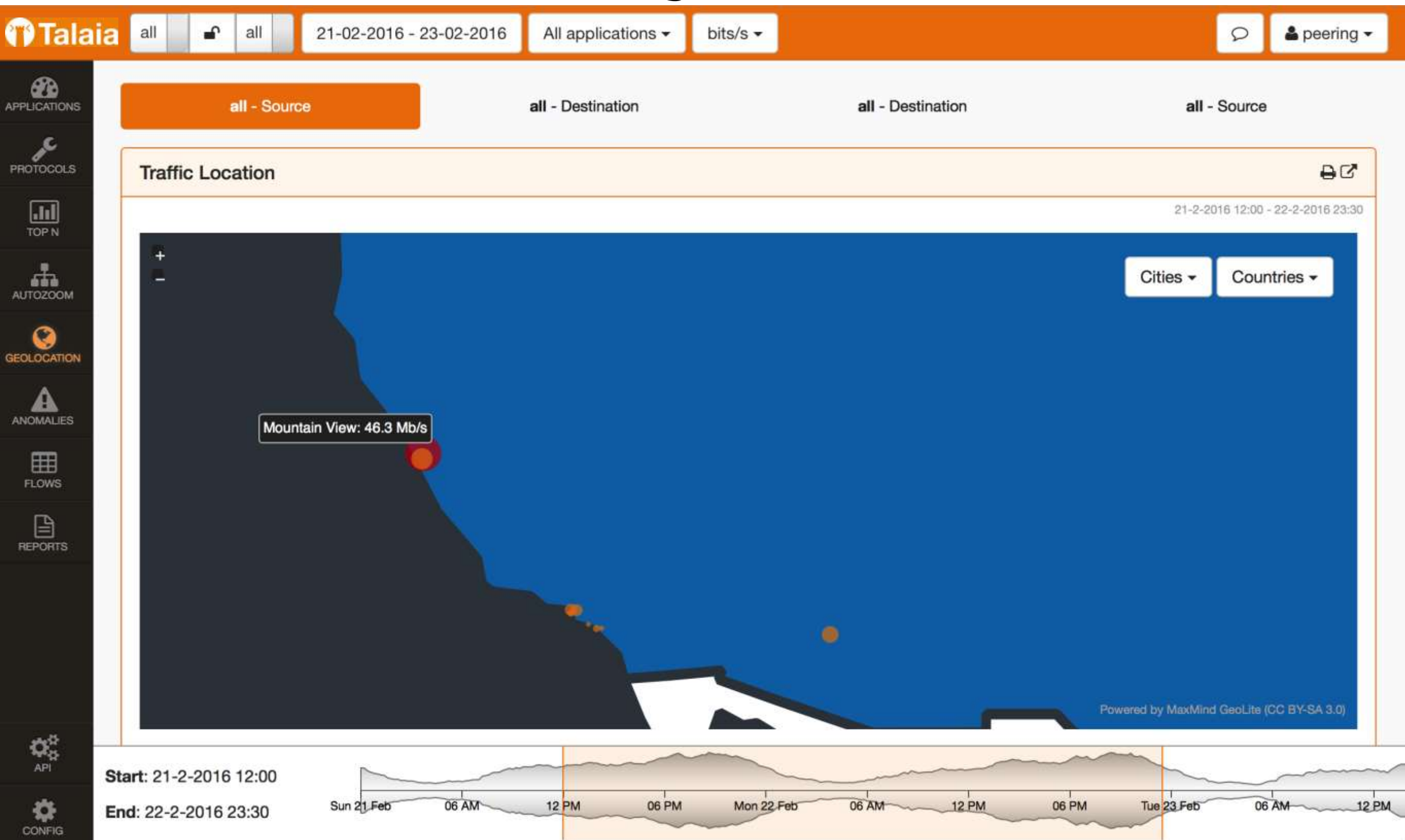
Demonstração “ao vivo”



Demonstração “ao vivo”



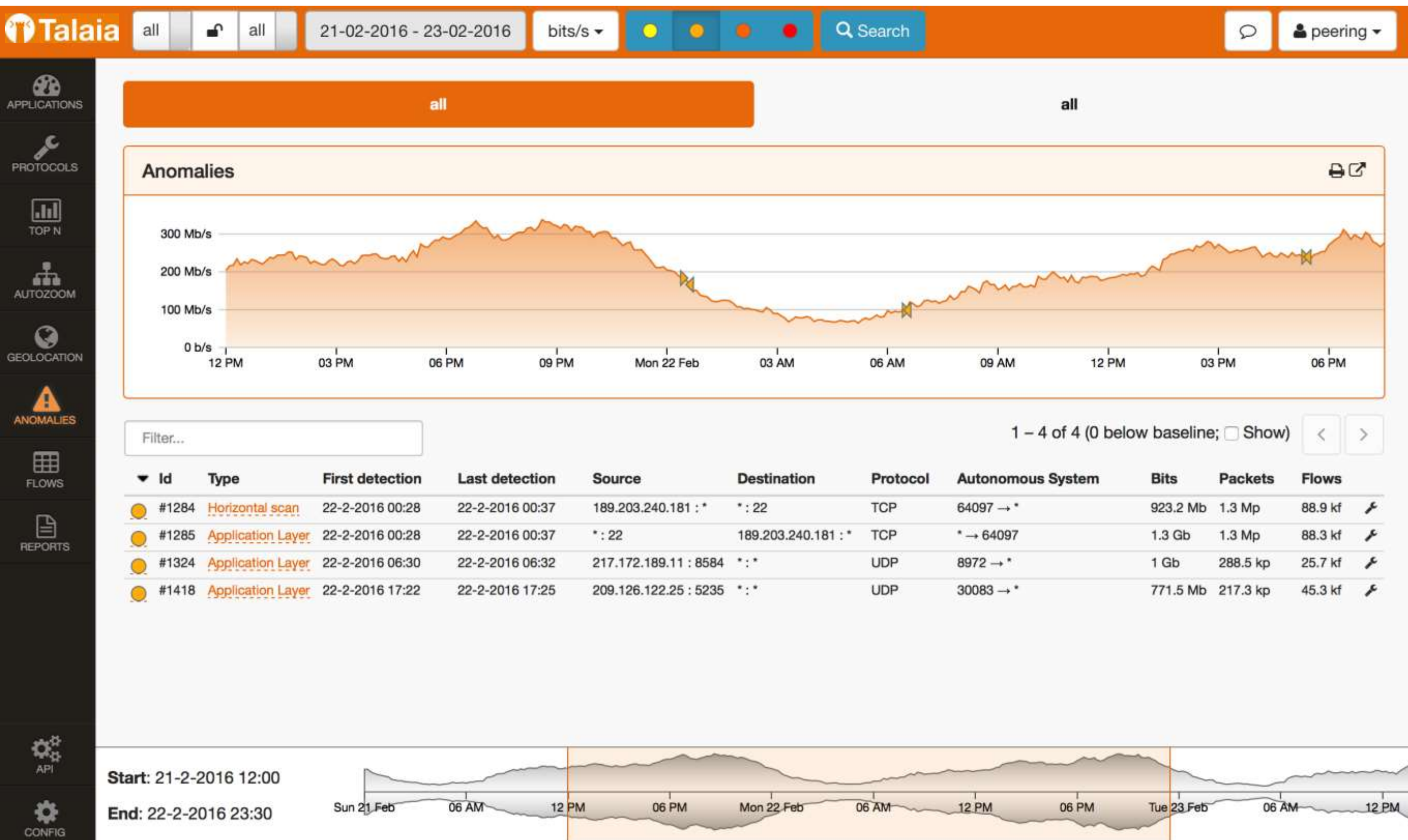
Demonstração “ao vivo”



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 privilegiado ponto de vista você pode planejar e prever diversas “coisas” para sua rede.

Conclusão

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

Obrigado!

Perguntas?

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