IV Workshop POP-RS / Rede Tche

Serviços e Segurança na Rede Tchê
POP-RS/CERT-RS

César Loureiro

PoP-RS
Ponto de Presença da
RNP no Rio Grande do Sul

Rede Tchê

Agenda I

- Apresentação do CERT-RS
- Honeypots
- Incidentes reportados ao CERT-RS
- Detecção e Contenção de DoS/DDoS

Agenda II

- Flows
- Backup roteadores
- Servidor/Analise de logs
- Diagnostico de sites
- Medição de banda
- NTP
- Collocation
- Mirror
- Alocação de blocos IP
- DNS secundario e reverso
- Listas tche-l e tchetec-l
- Qualidade de Serviço (QoS)
  - Traffic Shape
  - QoS para VoiP e VC

Apresentação CERT-RS

- Criado em 1995

- Sediado e mantido pela equipe do PoP-RS
-
- Responde pelos incidentes da Rede Tchê

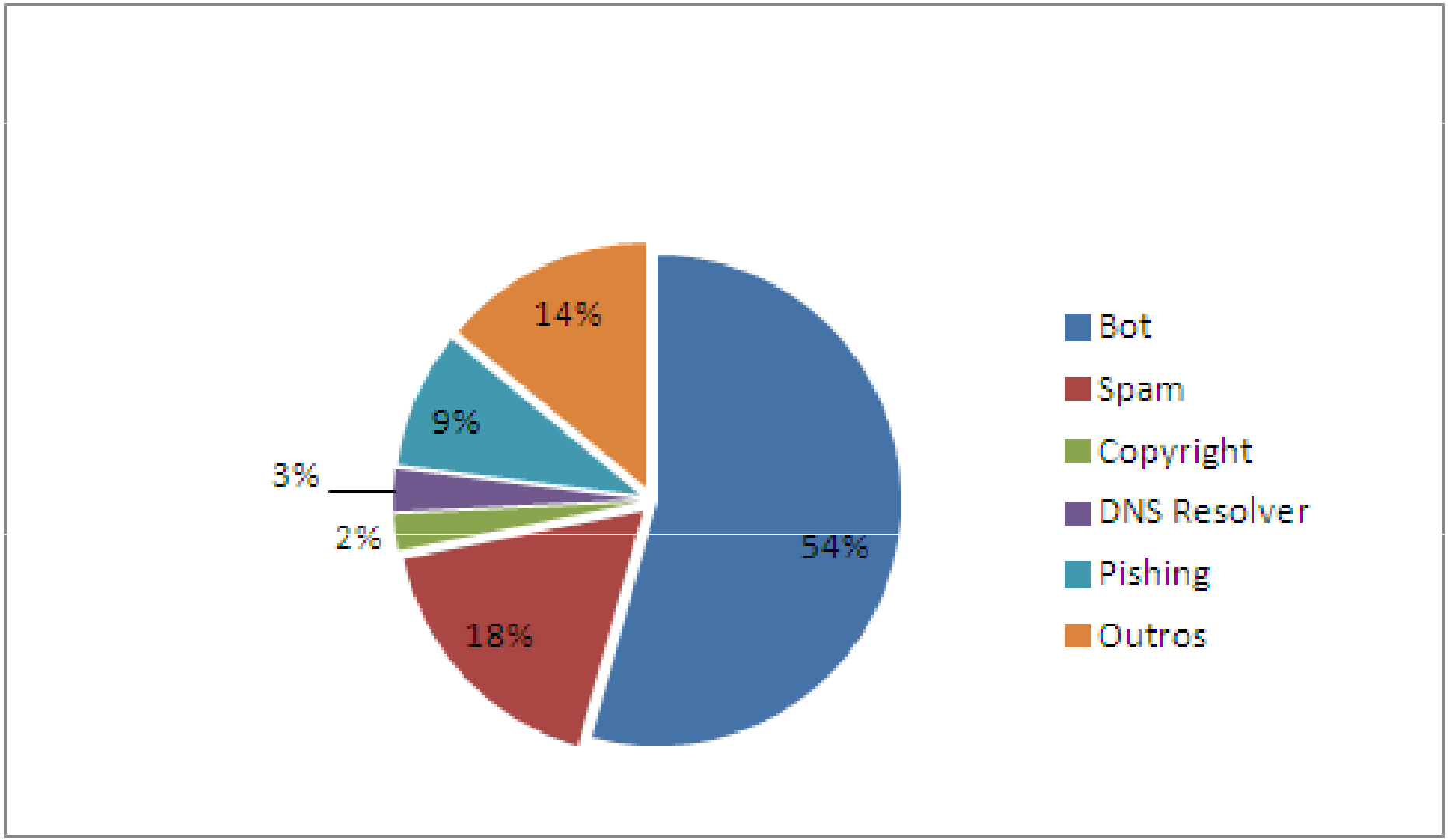
Serviços CERT-RS

- Contenção de ataques no *backbone* acadêmico.
- Notificação e tratamento de incidentes.
- Acompanhamento para que os eventos tenham o tratamento adequado!
- Auxílio aos clientes na implementação de serviços com requisitos de segurança.
- Análise de vulnerabilidades sob demanda.

Ações contra atividades maliciosas

- Cursos em conjunto com a ESR-POA/RNP
  - Introdução a segurança de redes
  - Análise Forense e Tratamento de Incidentes
- Participações no DISI da RNP
- Análise de logs e fluxo de dados apresentados
- Contensão de ataques DoS/DDoS detectados ou reportados pelos usuários

Incidentes relatados ao CERT-RS / 2012*

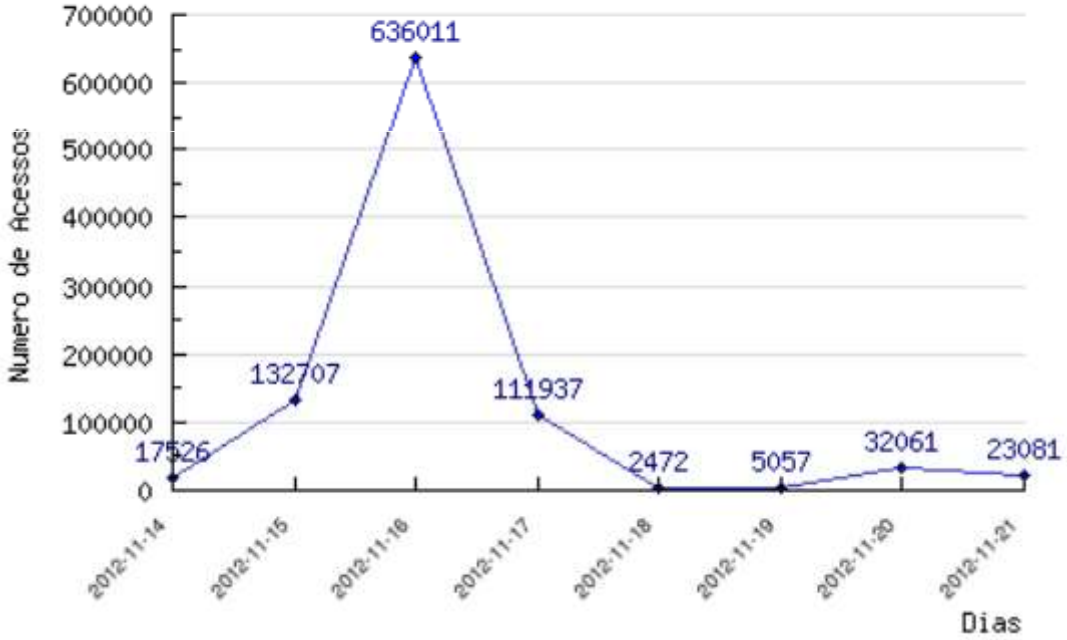


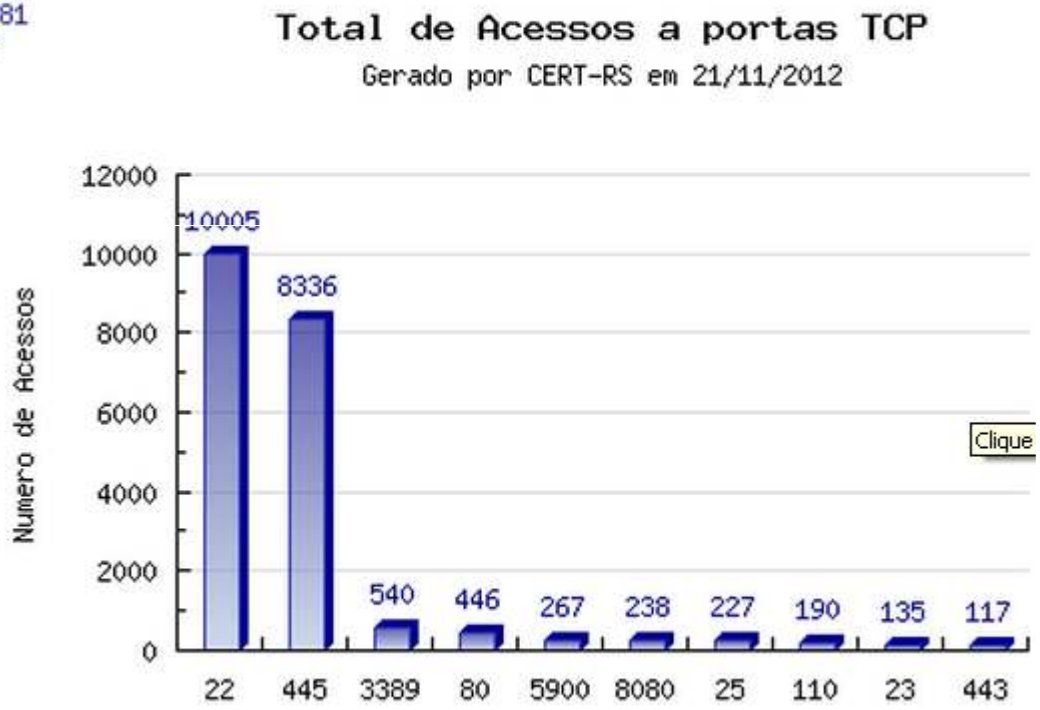
*de janeiro à outubro – 799 incidentes relatados

Honeypots

- Consórcio Brasileiro de Honeypots
- Parceria com o CERT.br
- Análise de Tendências
- Gráficos de Acessos UDP, TCP e Total

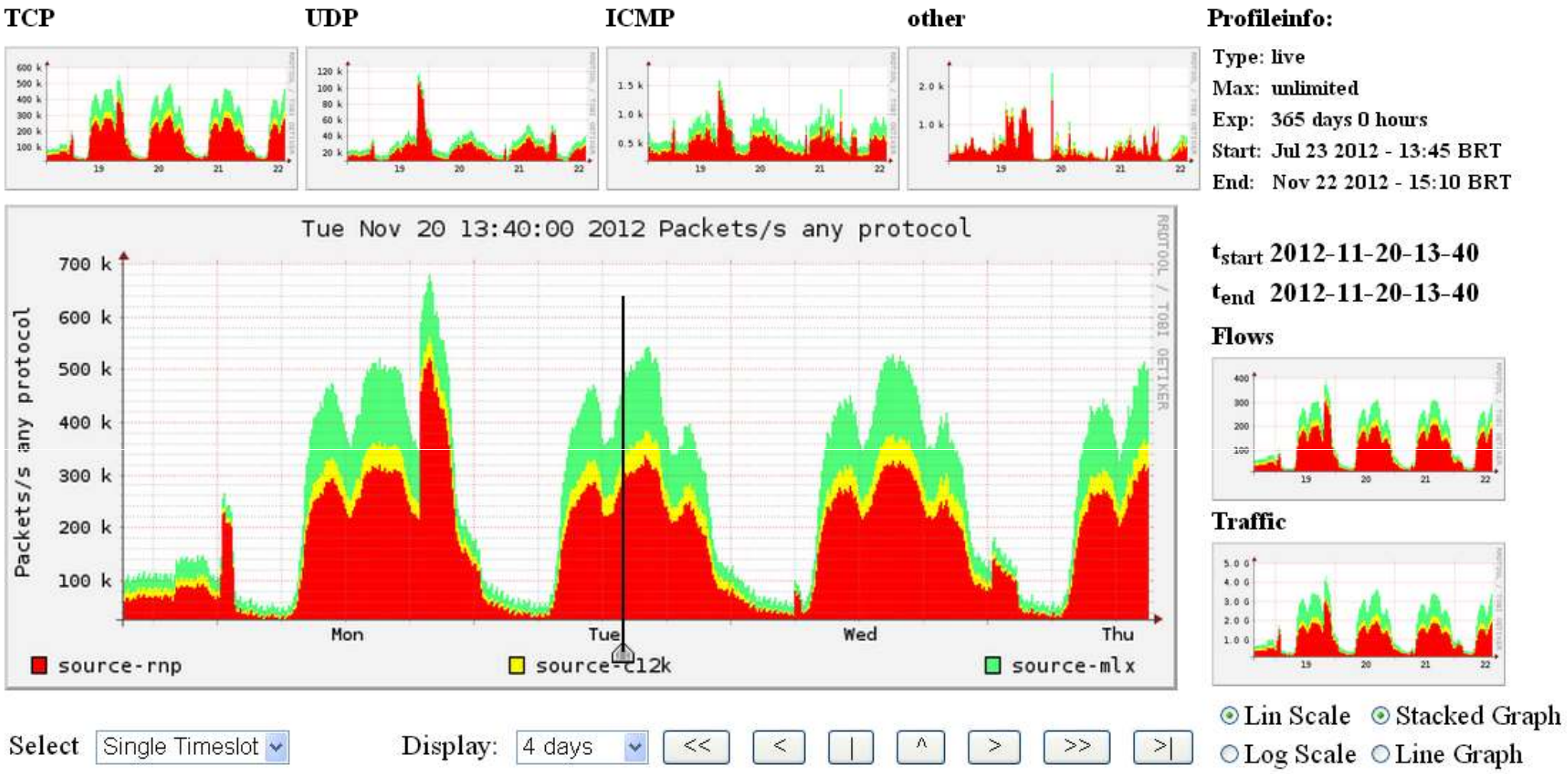
Estatísticas Honeypot





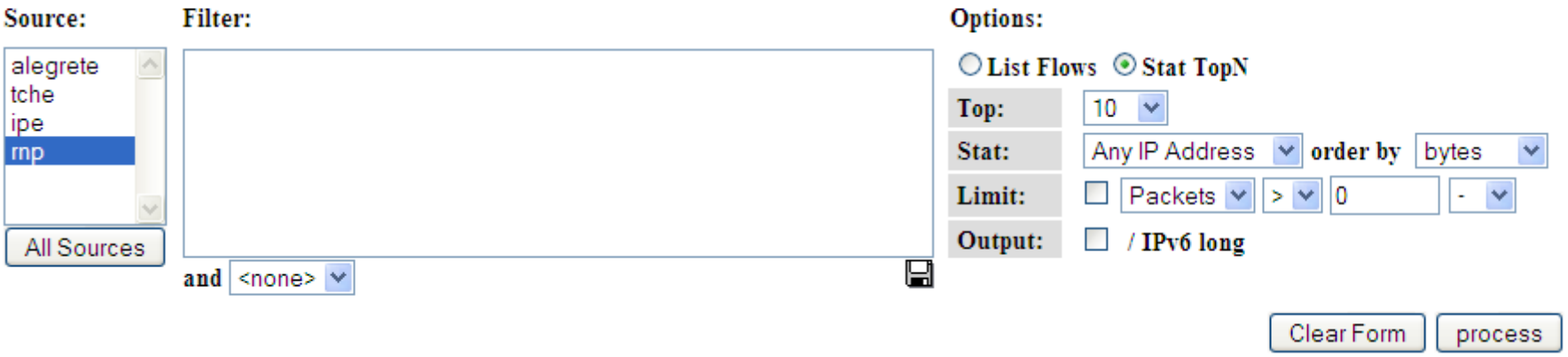
Flows

- Fluxos de dados



Flows

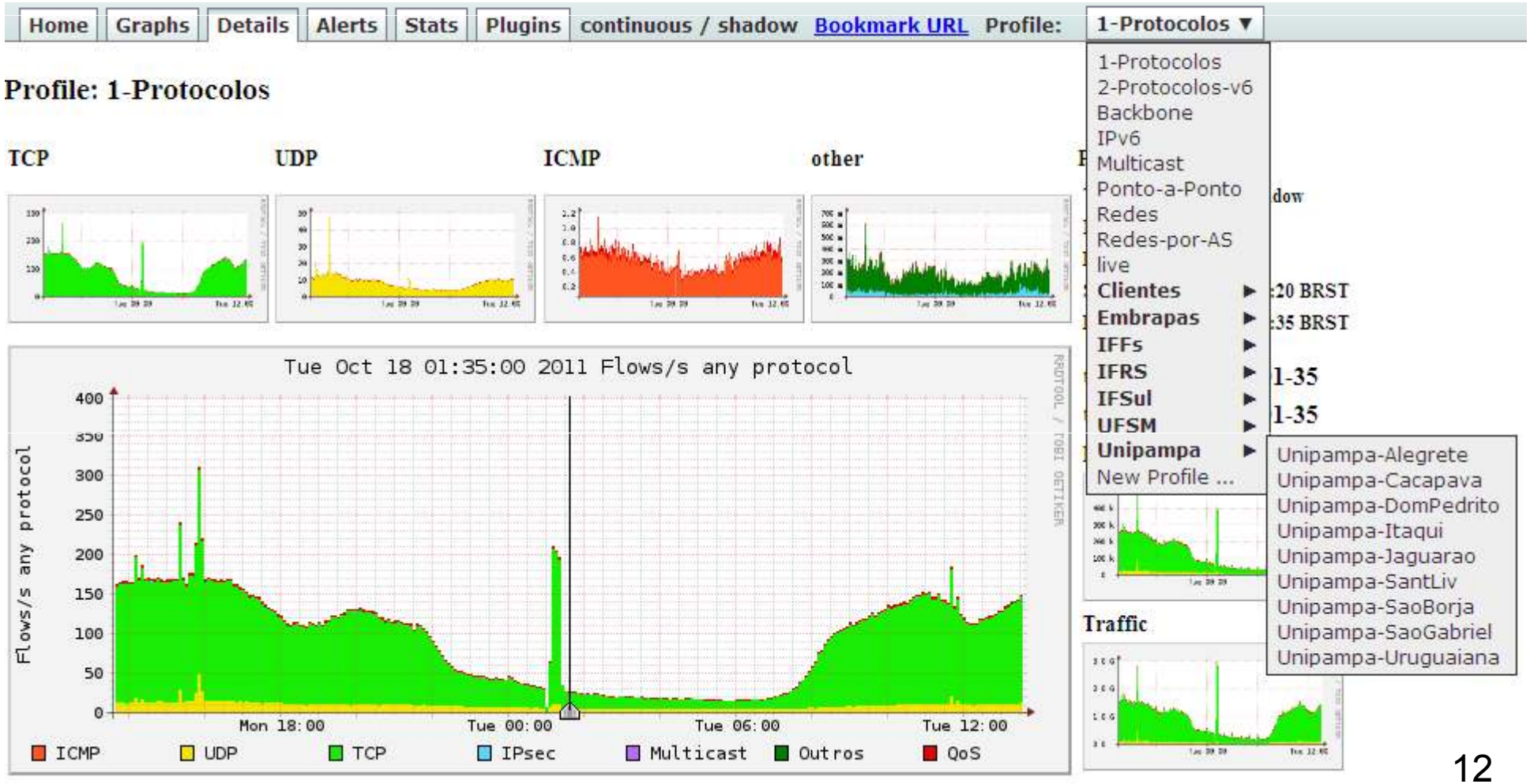
- Fluxos de dados - pesquisas




```
** nfdump -M /usr/local/var/nfsen/profiles-data/live/rnp  -T  -R nfcapd.201110180055:nfcapd.201110180130 -n 10 -s ip/bytes
nfdump filter:
any
Top 10 IP Addr ordered by bytes:
Date first seen          Duration Proto          IP Addr    Flows(%)      Packets(%)        Bytes(%)        pps      bps
2011-10-18 00:54:10.890  2386.705 any       200.236.31.7  94810(41.6)  123.1 M(27.9)  119.0 G(29.9)      51581  398.9 M
2011-10-18 00:54:08.890  2395.559 any       200.236.31.4  31017(13.6)   95.8 M(21.7)   94.1 G(23.6)      39998  314.3 M
2011-10-18 00:54:12.603  2160.974 any       200.236.31.2  13657( 6.0)   30.5 M( 6.9)   30.2 G( 7.6)      14098  111.8 M
2011-10-18 00:54:10.890  1833.711 any       200.236.31.1   3369( 1.5)   11.7 M( 2.6)   11.9 G( 3.0)       6375   51.7 M
2011-10-18 00:54:08.414  2400.180 any      200.18.33.234   5709( 2.5)   11.5 M( 2.6)   11.2 G( 2.8)       4782   37.4 M
2011-10-18 00:54:08.419  2389.778 any       200.236.31.3   1031( 0.5)   11.2 M( 2.5)    9.8 G( 2.5)       4670   32.8 M
2011-10-18 00:54:08.415  2398.226 any      200.19.252.56    378( 0.2)    9.9 M( 2.3)    8.2 G( 2.1)       4143   27.4 M
2011-10-18 01:08:16.769  1531.128 any       200.236.31.8   2504( 1.1)    8.1 M( 1.8)    8.0 G( 2.0)       5310   42.0 M
2011-10-18 01:08:19.254   982.923 any      200.17.96.190     90( 0.0)    6.5 M( 1.5)    6.3 G( 1.6)       6606   51.1 M
2011-10-18 01:08:19.254   982.923 any        193.52.82.2     90( 0.0)    6.5 M( 1.5)    6.3 G( 1.6)       6606   51.1 M
```

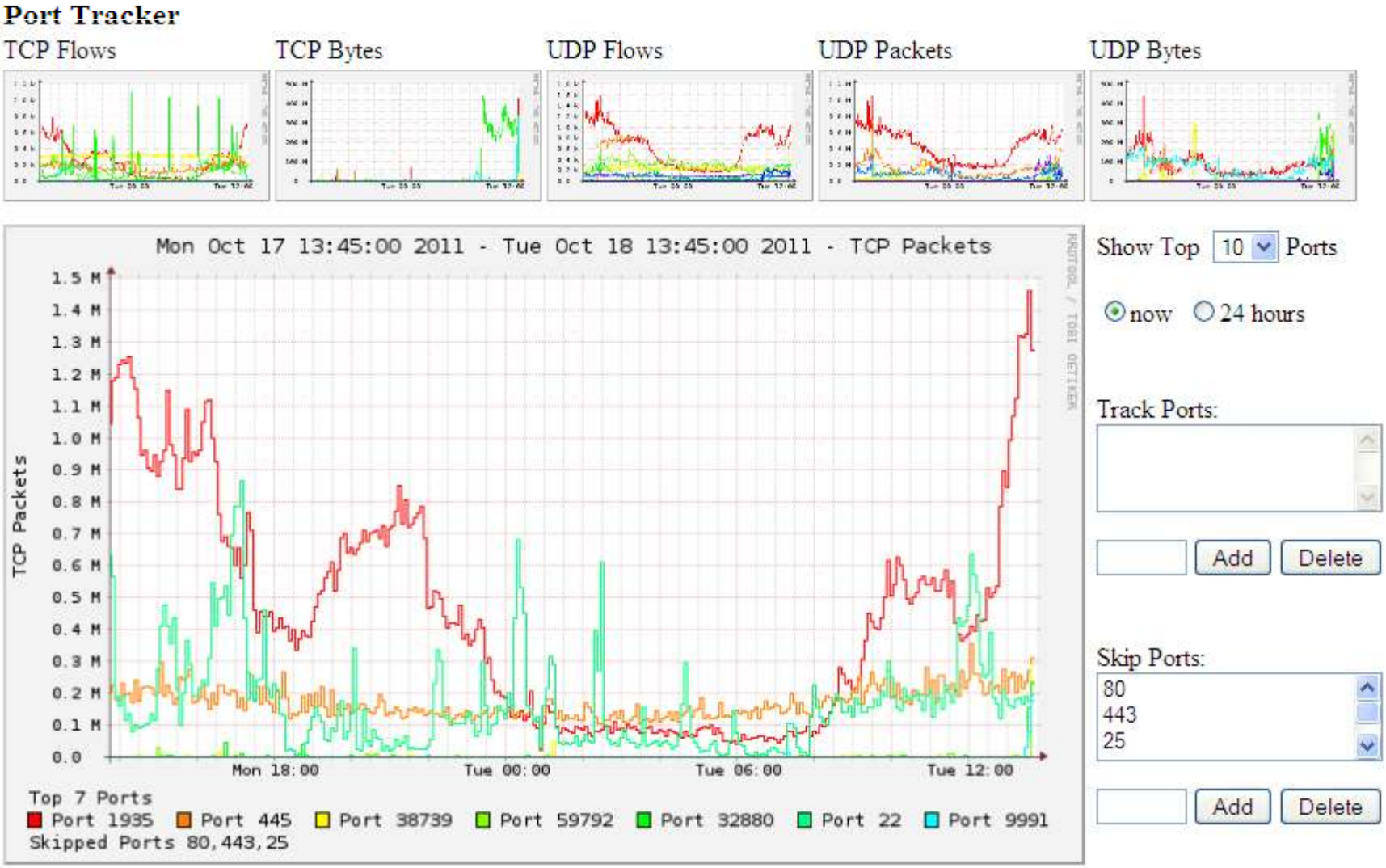
Flows

- Fluxos de dados – gráficos



Flows

- Fluxos de dados – Portas



Backup de Roteadores

A cada alteração realizadas nos roteadores, possuímos uma rotina que realiza o backup das configurações de todos, garantindo assim, um resposta ao tratamento de incidentes.

Servidor de logs centralizado

- **Análise de logs - Ossec**
  - Servidores PoP-RS
  - Roteadores da rede Tchê
  - Roteadores MetroPOA

Received From: ufpel-pos-0-2-2-3-c12k->/var/log/routers.poprs.log
Rule: 5720 fired (level 10) -> "Multiple SSHD authentication failures."
Portion of the log(s):

2012-04-24T10:53:48-03:00 ufpel-pos sshd[27097]: Failed password for ufpel from 200.17.161.8 port 48630 ssh2
2012-04-24T10:53:43-03:00 ufpel-pos sshd[27097]: Failed password for ufpel from 200.17.161.8 port 48630 ssh2
2012-04-24T10:52:35-03:00 ufpel-pos sshd[27095]: Failed password for ufpel from 200.17.161.8 port 48517 ssh2
2012-04-24T10:27:41-03:00 ufpel-pos sshd[27087]: Failed password for ufpel from 200.17.161.8 port 43284 ssh2

2012-11-14T07:49:01-02:00 alpine SYST: Port 1:7 link down
2012-11-14T07:49:08-02:00 alpine SYST: Port 1:7 link active 100Mbs FULL duplex
2012-11-22T13:04:59-02:00 MLX-4 Security: running-config was changed by gustavo from telnet client 192.168.1.225
2012-11-22T15:48:59-02:00 alpine SYST: 192.168.1.234 admin: show configuration
2012-11-23T16:24:28-02:00 ifsul-sapucaia-mu-19-c12k mcsn[1080]: task_reconfigure reinitializing done

Diagnóstico de sites

Consulta Integrada onde é possível consultar informações sobre determinado IP/domínio em uma única interface:

http://pop-rs.rnp.br/portal/

Diagnóstico de sites

PING

PING 200.132.0.132 (200.132.0.132) 56(84) bytes of data.
64 bytes from 200.132.0.132: icmp_seq=1 ttl=64 time=0.303 ms
64 bytes from 200.132.0.132: icmp_seq=2 ttl=64 time=0.310 ms
64 bytes from 200.132.0.132: icmp_seq=3 ttl=64 time=0.332 ms
64 bytes from 200.132.0.132: icmp_seq=4 ttl=64 time=0.303 ms

--- 200.132.0.132 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.303/0.312/0.332/0.011 ms

TRACEROUTE

traceroute to 200.132.0.132 (200.132.0.132), 20 hops max, 40 byte packets
1 delta.pop-rs.rnp.br (200.132.0.132) 0.491 ms 0.462 ms

REVERSO

132.0.132.200.in-addr.arpa domain name pointer delta.pop-rs.rnp.br.

SPF

132.0.132.200.in-addr.arpa domain name pointer delta.pop-rs.rnp.br.

BLACKLIST

Checando 200.132.0.132...

zen.spamhaus.org [Não Listado]
b.barracudacentral.org [Não Listado]
t1.dnsbl.net.au [Não Listado]
bl.spamcop.net [Não Listado]
cbl.abuseat.org [Não Listado]

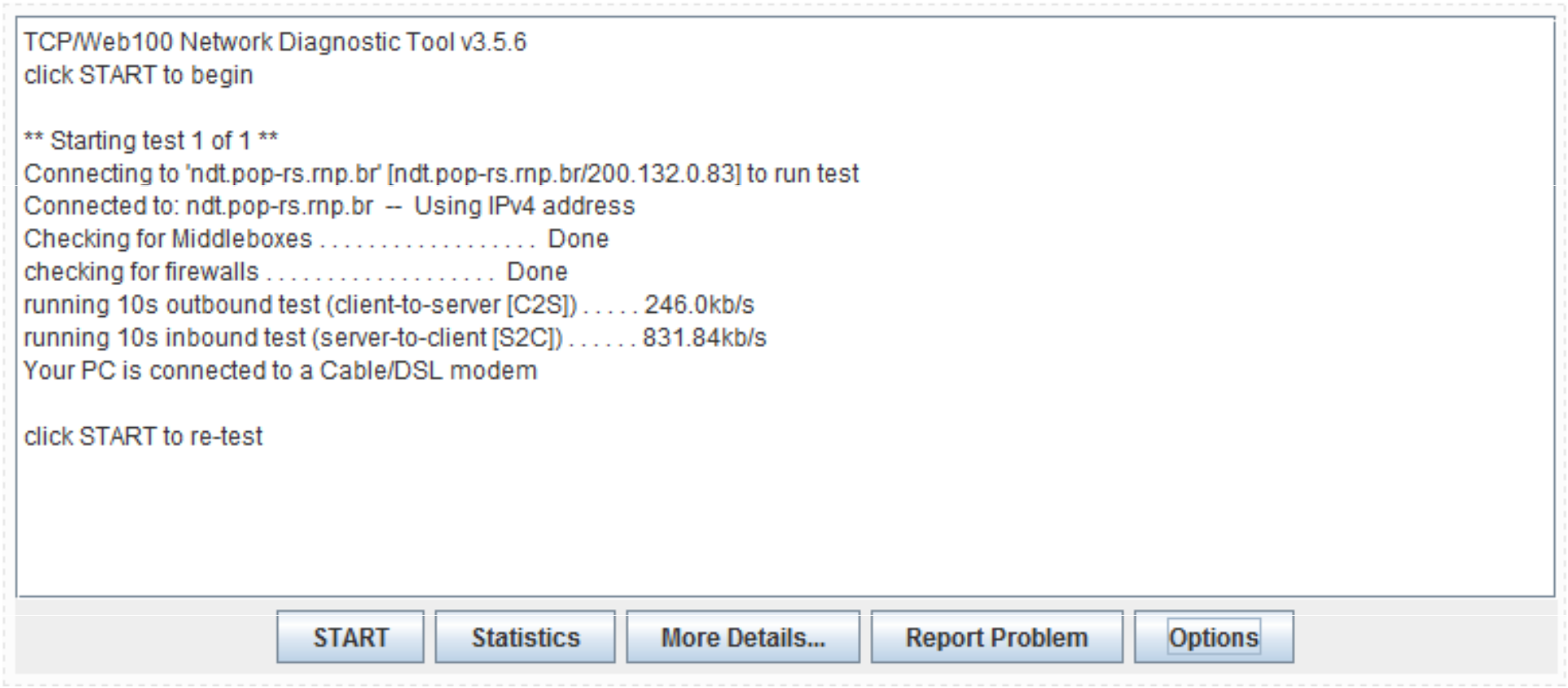
Medição de banda

- **Web100 - *network diagnostic tool* (NDT)**

Solução para medição de banda de um ponto da rede até o POP-RS (entrada e saída).

http://ndt.pop-rs.rnp.br

Medição de banda



RNP

MONIPÊ

NTP(Network Time Protocol)

Disponibilização de servidores de tempo Stratum1 para uso dos clientes da rede Tchê.

Um servidor de ordem Stratum 1, é sincronizado utilizando um receptor GPS (Stratum 0).

ntp.pop-rs.rnp.br

ntp.cert-rs.tche.br

Collocation

- Disponibilizada a rede 200.132.1.0/24 para os clientes proverem serviços nas dependências do PoP-RS/CPD.
- Maior velocidade de banda.

Para o uso do espaço físico do Datacenter é necessário realizar um convênio com a UFRGS.

Mirror

Disponibilização dos sistemas:

- FreeBSD (ftp://ftp4.br.freebsd.org)

- CTAN(Comprehensive teX Archive Network)

http://mirror.pop-rs.rnp.br

DNS Secundário e Reverso

Serviço de DNS segundário através de transferências de zonas dos clientes para o POP-RS.

Endereçamento IP (blocos)

- IPv4 -> intranet RNP, feito diretamente pelo cliente

- IPv6 -> entrar em contato com o POP

BGP Multihomed

- Cada cliente conectado a outro backbone (Oi, Embratel, GVT, etc) pode balancear seu tráfego com a Rede Tchê.
- Não necessita solicitar Sistema Autônomo próprio.
- Deve possuir um /24 da RNP(sugestão) e conexão com outra operadora.

Entrar em contato por telefone para ver outros quesitos técnicos

Listas Tche-l e Tchetec-l

Listas de discução / Canal de comunicação dos clientes da rede Tchê

- Tche-l -> Contatos administrativos
- Tchetec-l -> Contatos técnicos

Utilize estas listas para compartilhar informações com os outros participantes da rede Tchê.

"Mantenha seu e-mail atualizado"

Preencha o formulário de atualização de dados cadastrais

QoS (Quality of Services)

- Possibilidade de marcação de pacotes (DiffServ).
- Traffic Shape

  “Avise o POP ao aumentar seu canal de comunicação”
- QoS para VoiP e Video Conferência entre campi.

.