Estudo de caso: Ataques via Internet e o Ambiente de Datacenters/ISP

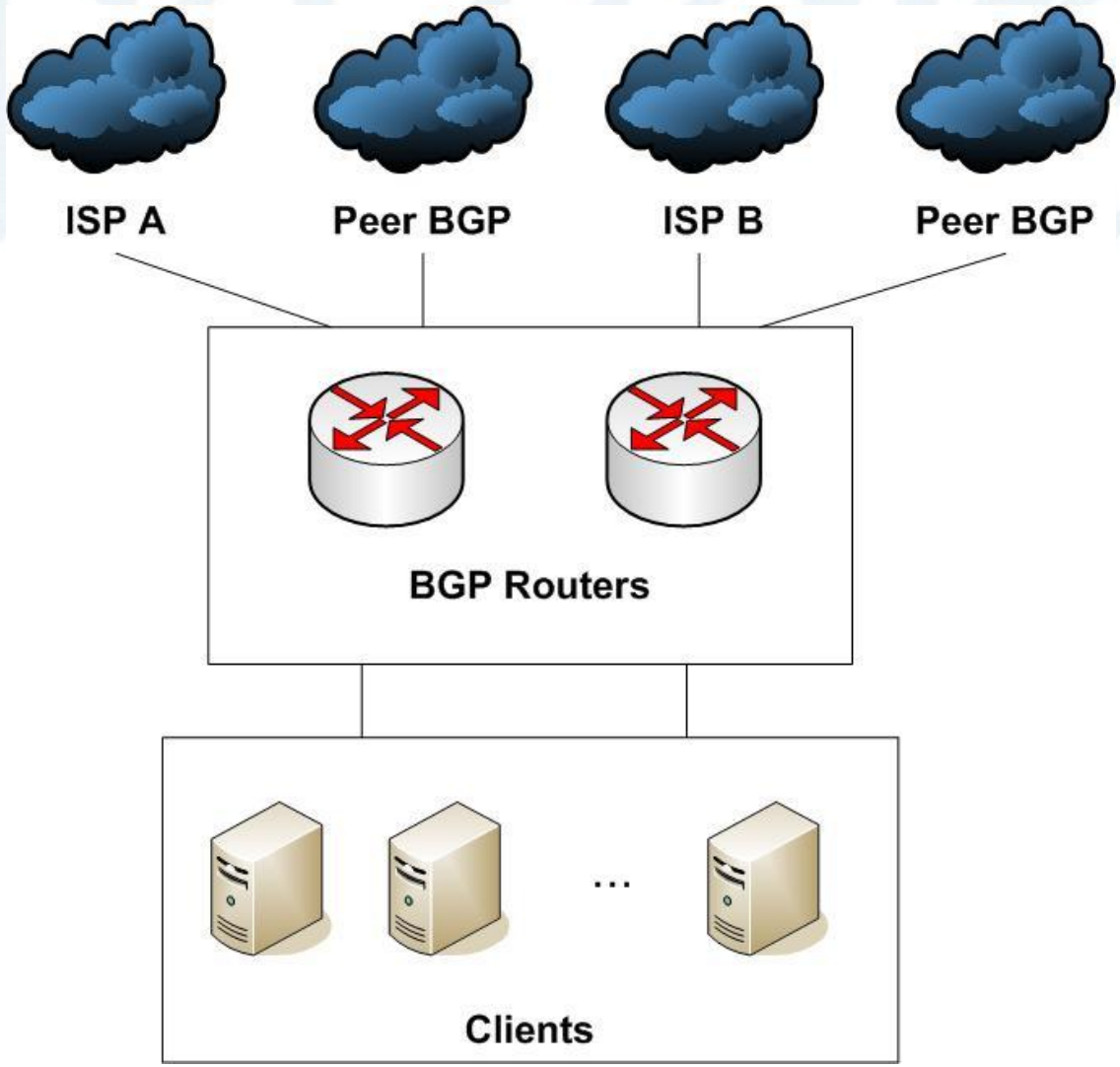
Artur Renato Araujo da Silva
DH&C Outsourccing
E-mail: artur@dh-c.com.br
PGP ID: 0xE6C1BCE0

DH&C Outsourccing

Agenda

- **O Ambiente**
- As Ameaças
- A Coleta de Dados
- Detecção de Ataques
- Métodos de bloqueio
- Tendências

- Ambiente Multi-homed
- 2 upstreams
- Vários peers
- Estrutura IP compartilhada para os clientes
- Redundância de equipamentos
- 4 blocos CIDRs (/20)



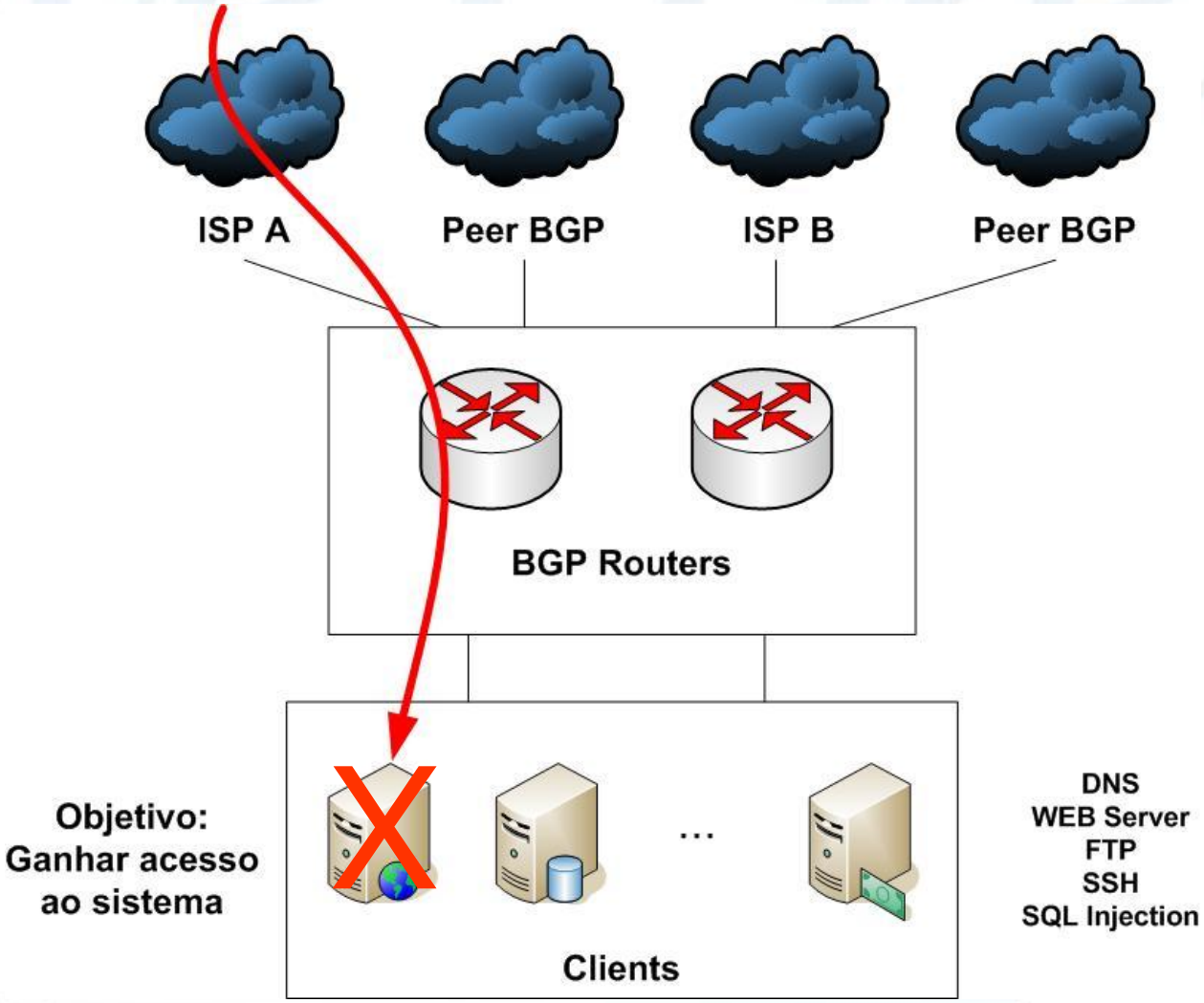
O Ambiente

DH&C Outsourcing

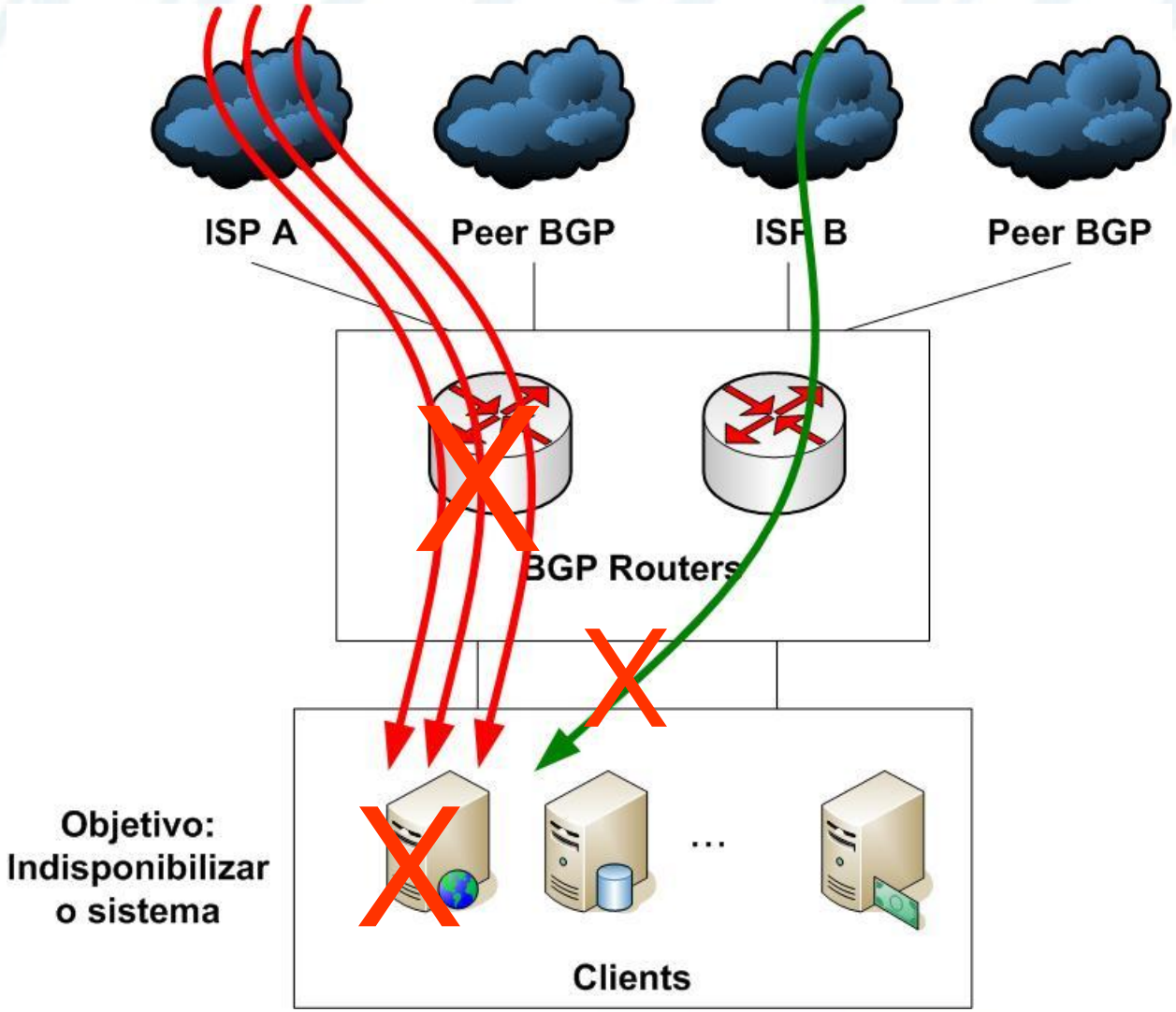
Agenda

- O Ambiente
- **As Ameaças**
- A Coleta de Dados
- Detecção de Ataques
- Métodos de bloqueio
- Tendências

Ataque à aplicação

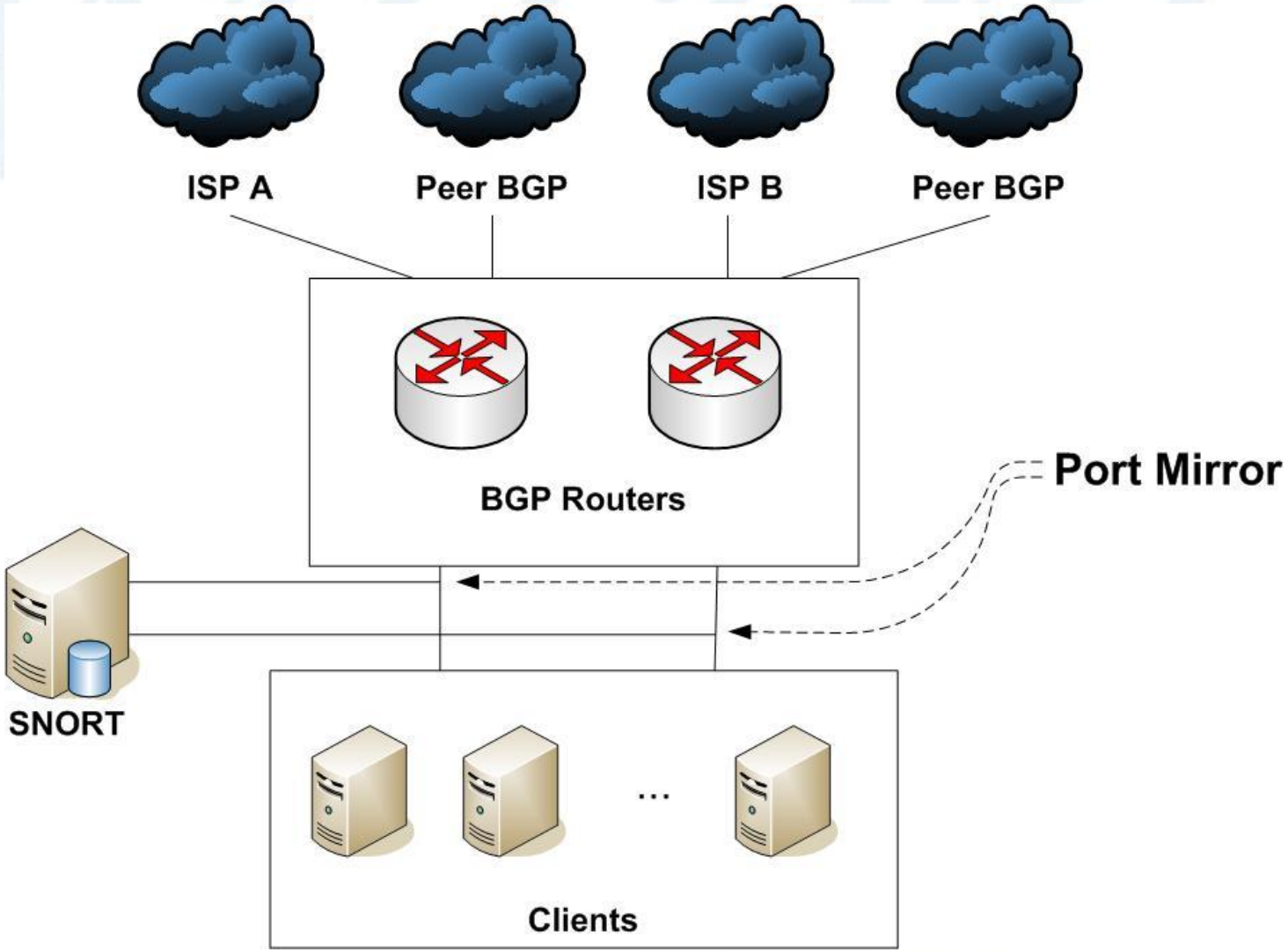


Ataque DoS - DDoS



Agenda

- O Ambiente
- As Ameaças
- **A Coleta de Dados**
- Detecção de Ataques
- Métodos de bloqueio
- Tendências



A Coleta de Dados

DH&C Outsourcing

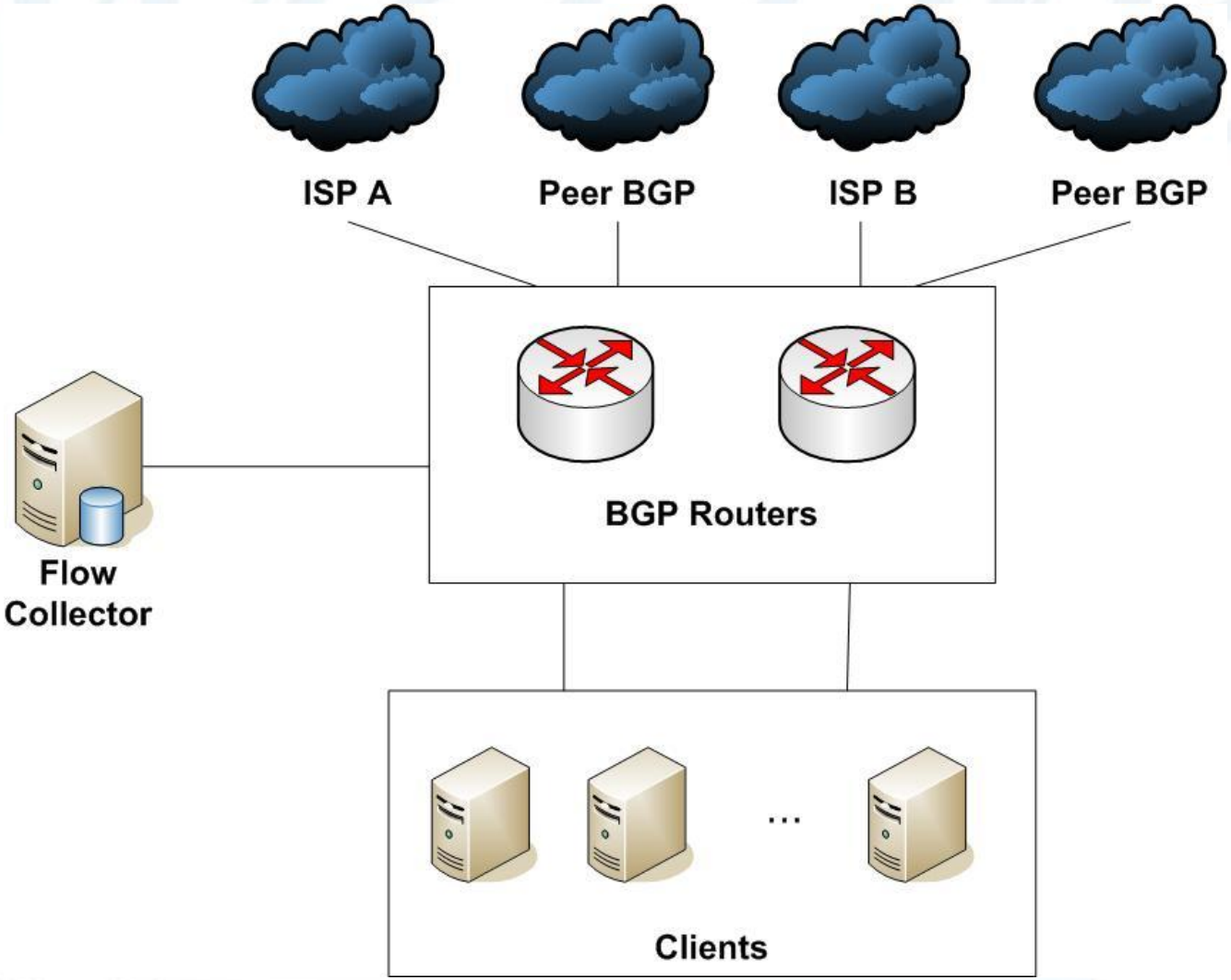
- SNORT + ACID
- Geração de relatórios On-line
  - Interface ACID – Administradores
  - Interface Própria – Clientes
    - Geração dos relatórios baseados nos dados da base Mysql
    - Relatórios individuais

Problema – Volume de Alarmes

- Conjunto default de regras
  - 1 dia 256232 alertas
  - 6 dias 1550811 alertas
- Conjunto customizado de regras
  - 1 dia aprox. 50.000 alertas
- Origem distinta de ataques por dia: 27684

Solução

- Clientes
  - Relatórios On-line diários
  - Resumos guardados como histórico permanente
- Administradores
  - Relatórios On-line por uma semana
  - Backup em disco por um mês



A Coleta de Dados

DH&C Outsourcing

- Netflow V5 - Juniper / Cisco
- Flow-tools + flowscan (JKflow)
- Rate 1:1
- Armazenados por 30 dias
- Gráficos on-line
  - Pacotes/segundo
  - Fluxos/segundo
  - Bits/segundo
  - Por cliente e por aplicação

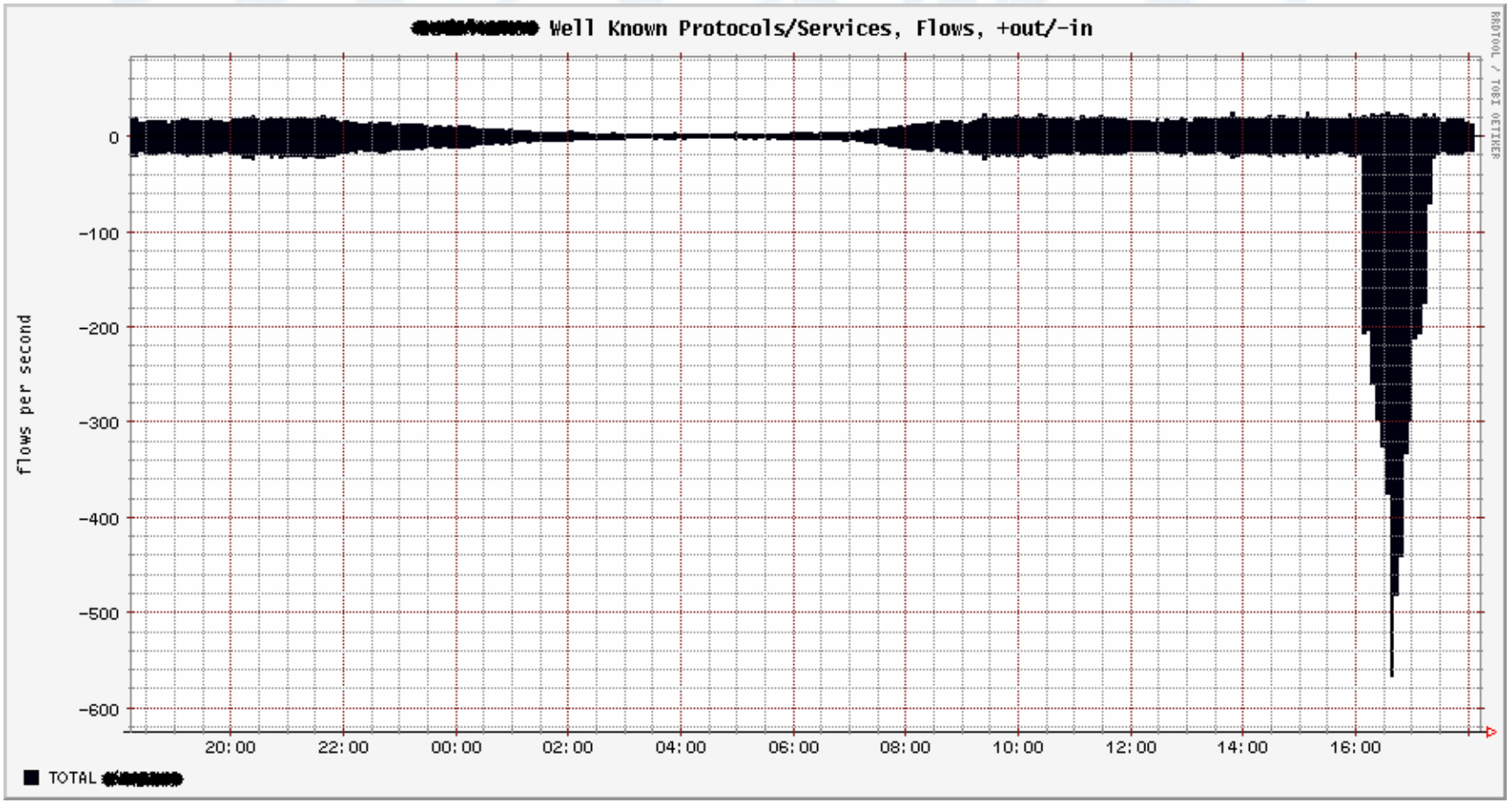
Agenda

- O Ambiente
- As Ameaças
- A Coleta de Dados
- **Detecção de Ataques**
- Métodos de bloqueio
- Tendências

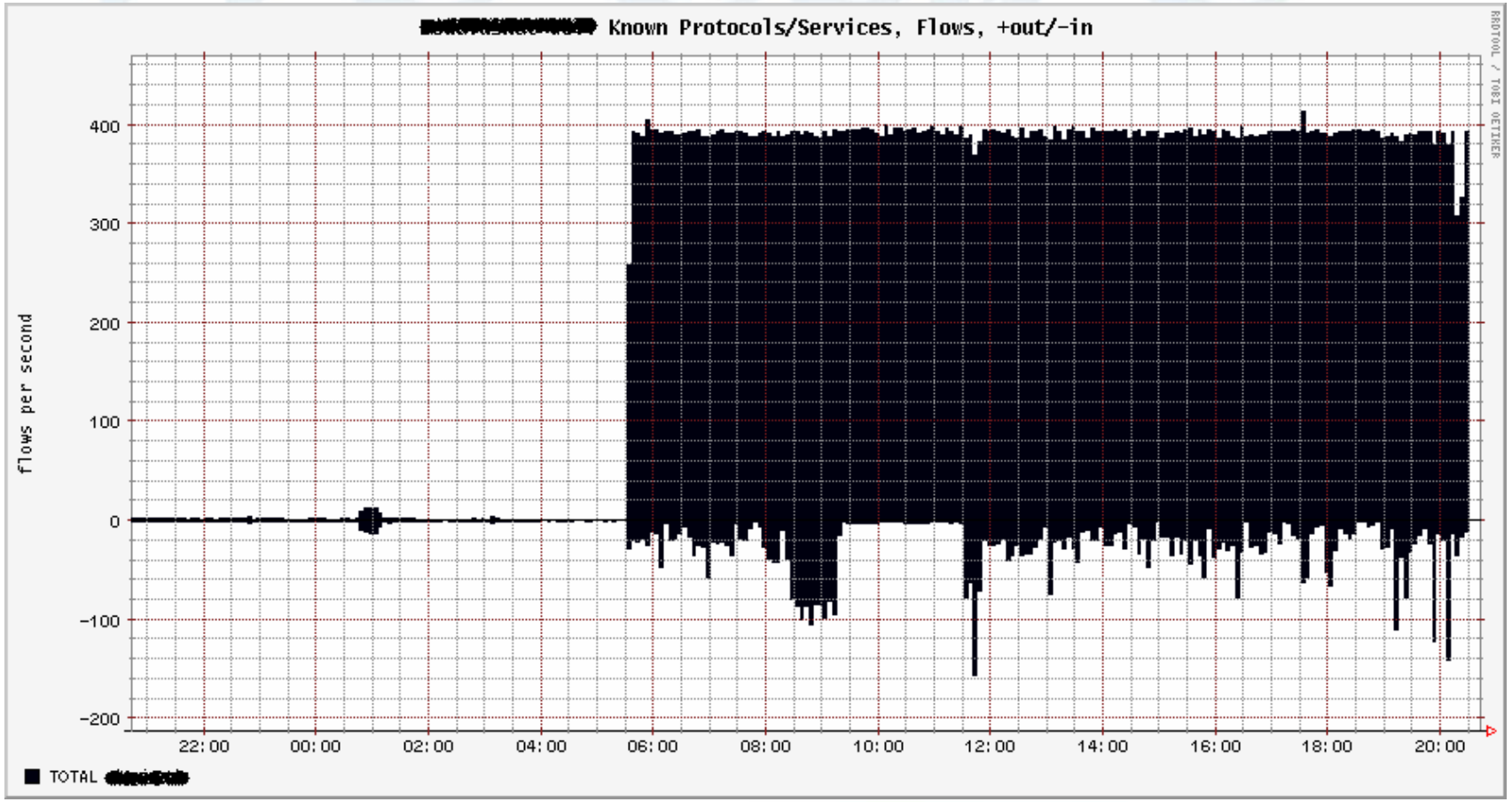
- Ataques à aplicação
  - Alertas via SNORT
- Ataques à infraestrutura (DoS e DDos)
  - Observação dos padrões (gráficos)
  - Scripts de threashold!
    - Análise do perfil de tráfego
    - Geração de alertas via e-mail
    - Detecção em 2 minutos

- Origem e destino dos ataques
- Portas e protocolos
- Registro de todas as conexões – auditoria
- TOP 10 (fluxos, bits, packets)
- 1dia = 4 Gbytes de dados

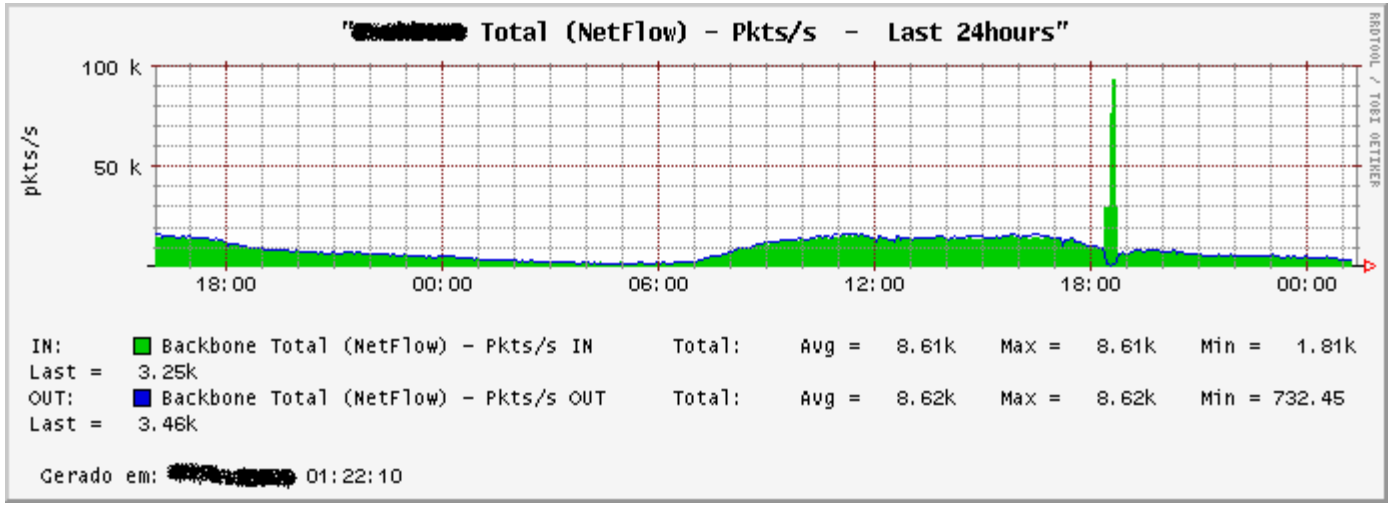
- Identifcação de scan



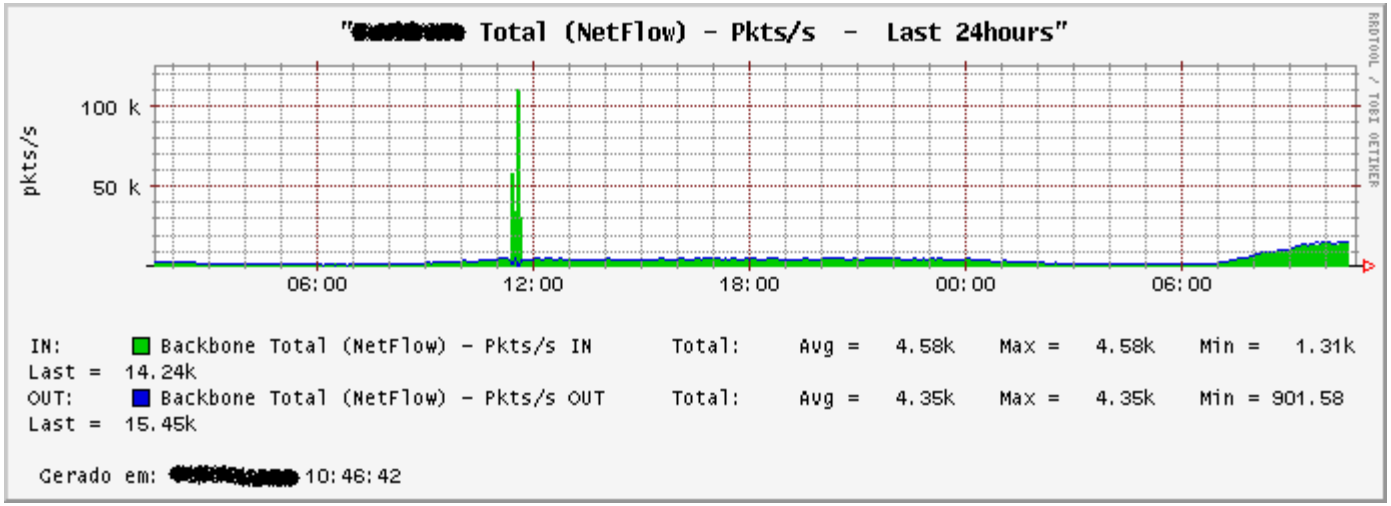
- Identifcação de worms e vírus



- Identificação de DoS



- Identificação de DDos



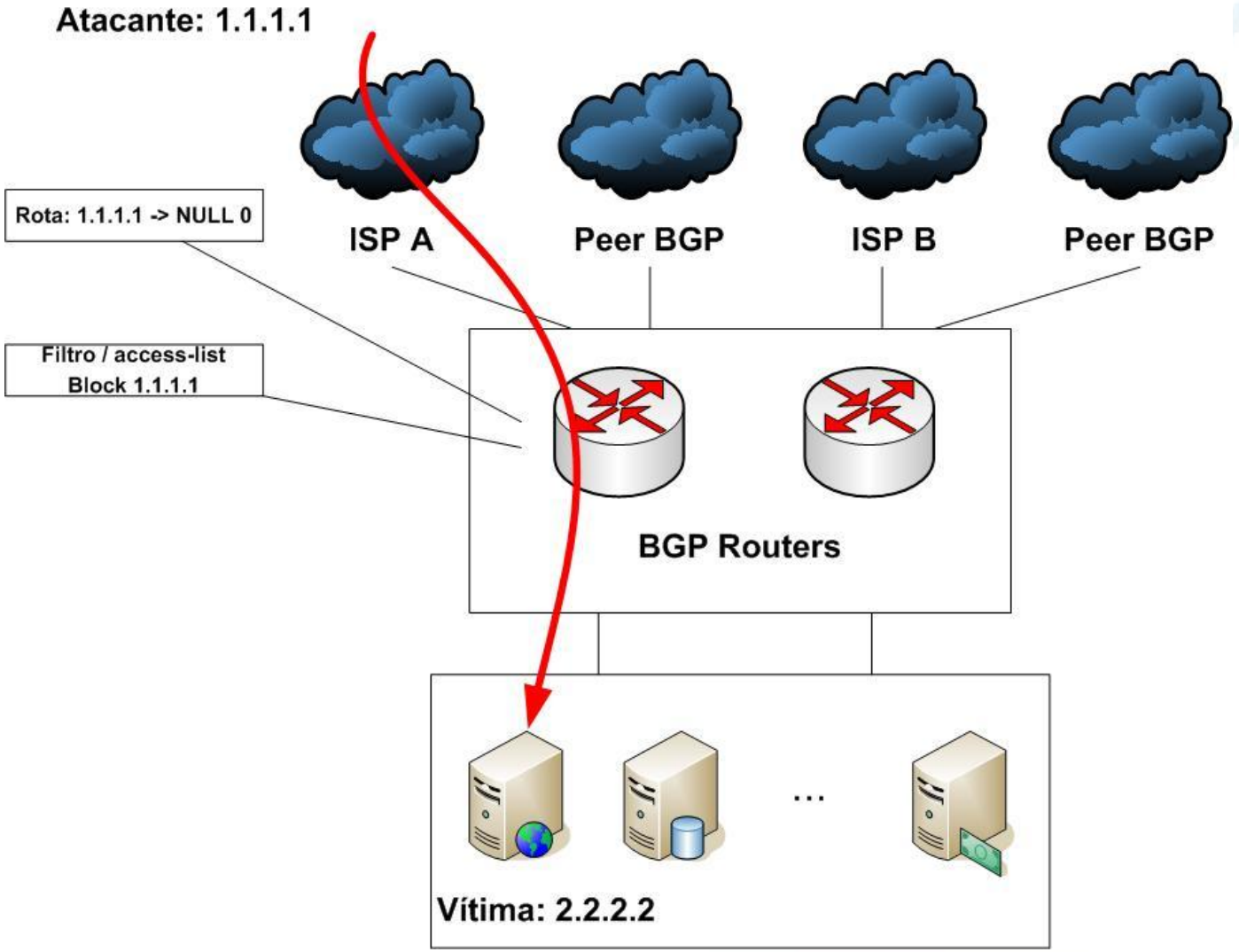
- Cisco:
  - Router# show ip cache flow | inc M|K

- Juniper
  - admin@Router> show services accounting flow-detail order bytes
  - admin@Router> show services accounting flow-detail order packets

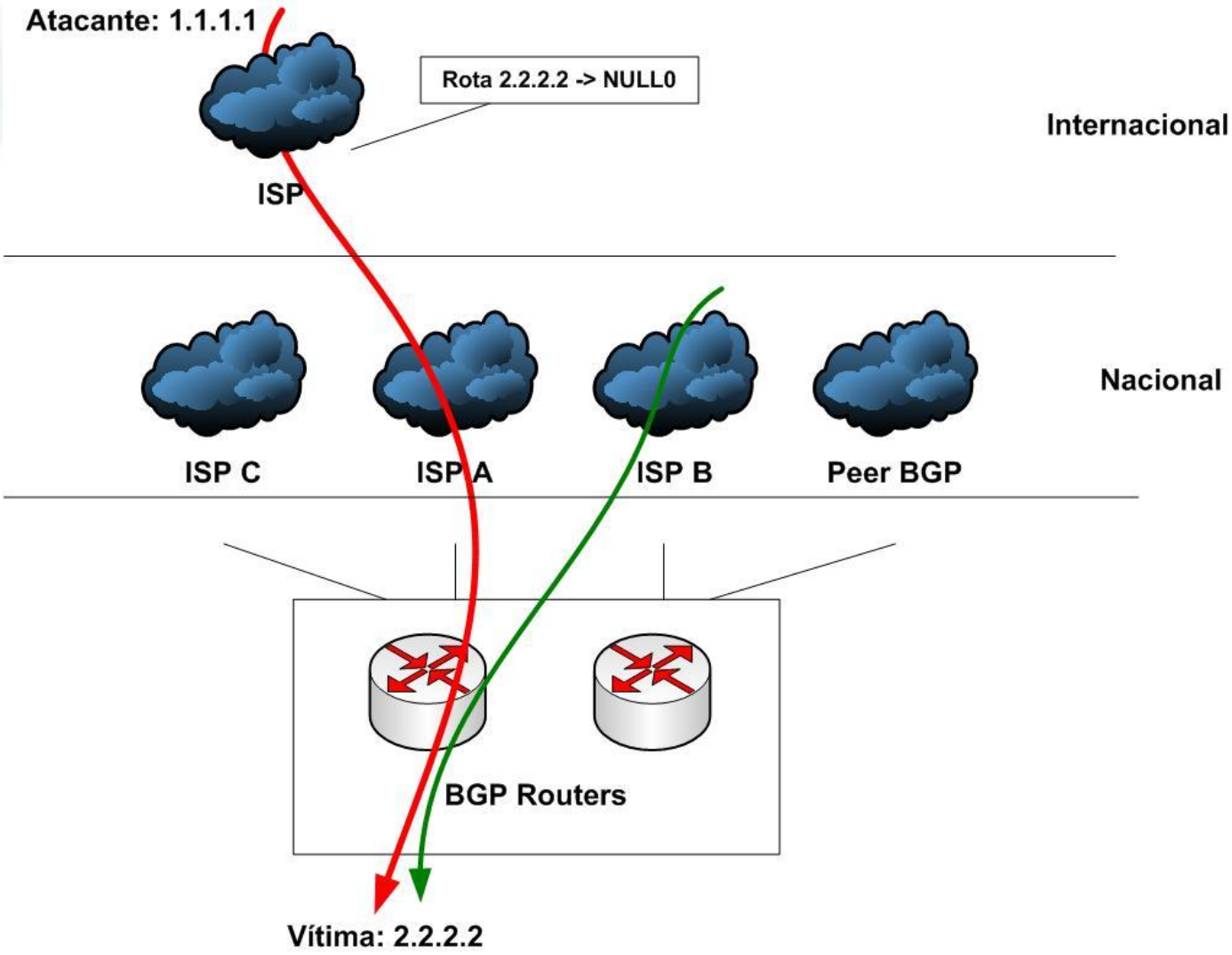
Agenda

- O Ambiente
- As Ameaças
- A Coleta de Dados
- Detecção de Ataques
- **Métodos de bloqueio**
- Tendências

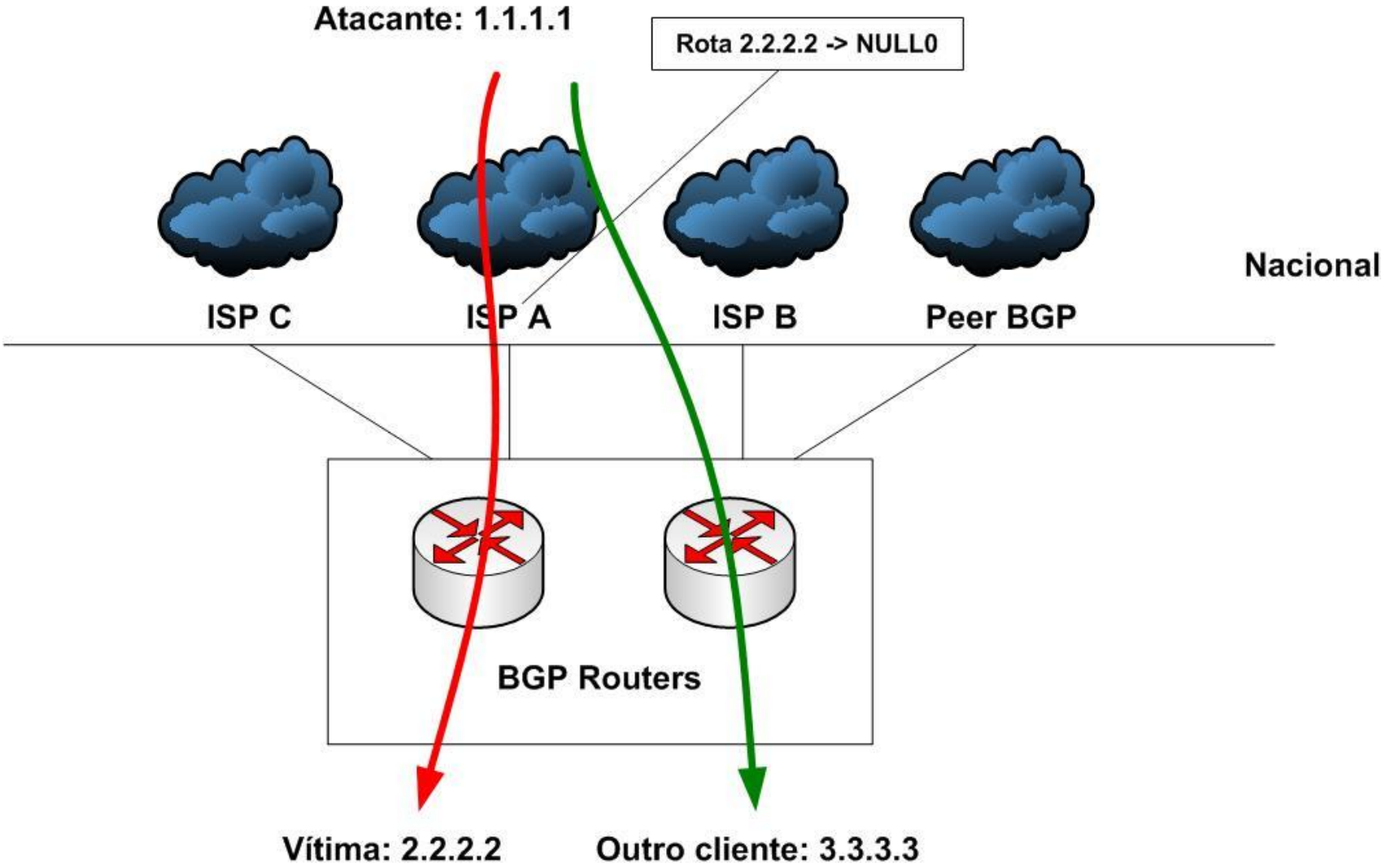
Access-list / RPF



Black Hole (1/2)



Black Hole (2/2)



Agenda

- O Ambiente
- As Ameaças
- A Coleta de Dados
- Detecção de Ataques
- Métodos de bloqueio
- **Tendências**

- Detecção por assinatura x anomalia
- Detecção por anomalia
  - Protocolos
    - Ex. Binários em header HTML
  - Perfil de rede
    - Período de aprendizagem
- IPS
  - Ataques à aplicação
  - Ataques DoS e DDoS

Agradecimento

Gustavo R. Ramos

DH&C Outsourcing

Perguntas?

artur@dh-c.com.br

DH&C Outsourcing