Implementação do DNSSEC

Wilson Rogério Lopes
wlopes@ig.com
http://tisora.com.br

GTER 32 - 12/2011

DNSSEC no iG

- Domínio ig.com.br assinado em 14 de maio de 2011
- **Primeiro portal brasileiro a ter o domínio assinado**

domínio:ig.com.br
entidade: Internet Group do Brasil SA
servidor DNS: dnssec1.ig.com.br
status DNS: 26/11/2011 AA
último AA: 26/11/2011
servidor DNS: dnssec2.ig.com.br
status DNS: 26/11/2011 AA
último AA: 26/11/2011
record DS: 56476 RSA/SHA-1FFC9F99278B14E76733A85...
status DS: 24/11/2011 DSOK

Agenda

- **Premissas**
- **DNS Autoritativo**
  - Política de chaves e assinaturas
  - Infraestrutura, ferramentas e operação
  - Estatísticas
- **DNS Recursivo**
  - Infraestrutura
  - Estatísticas
- **Considerações Finais**

Premissas

- **Operação**
  DNSSEC não pode ser um problema operacional
- **Processo alinhado com a gerência de mudanças**
- **Confiabilidade e Monitoração**
  Manter a confiabilidade da infra de DNS
- **Reassinatura/Rollover automatizados**
- **Escalabilidade**

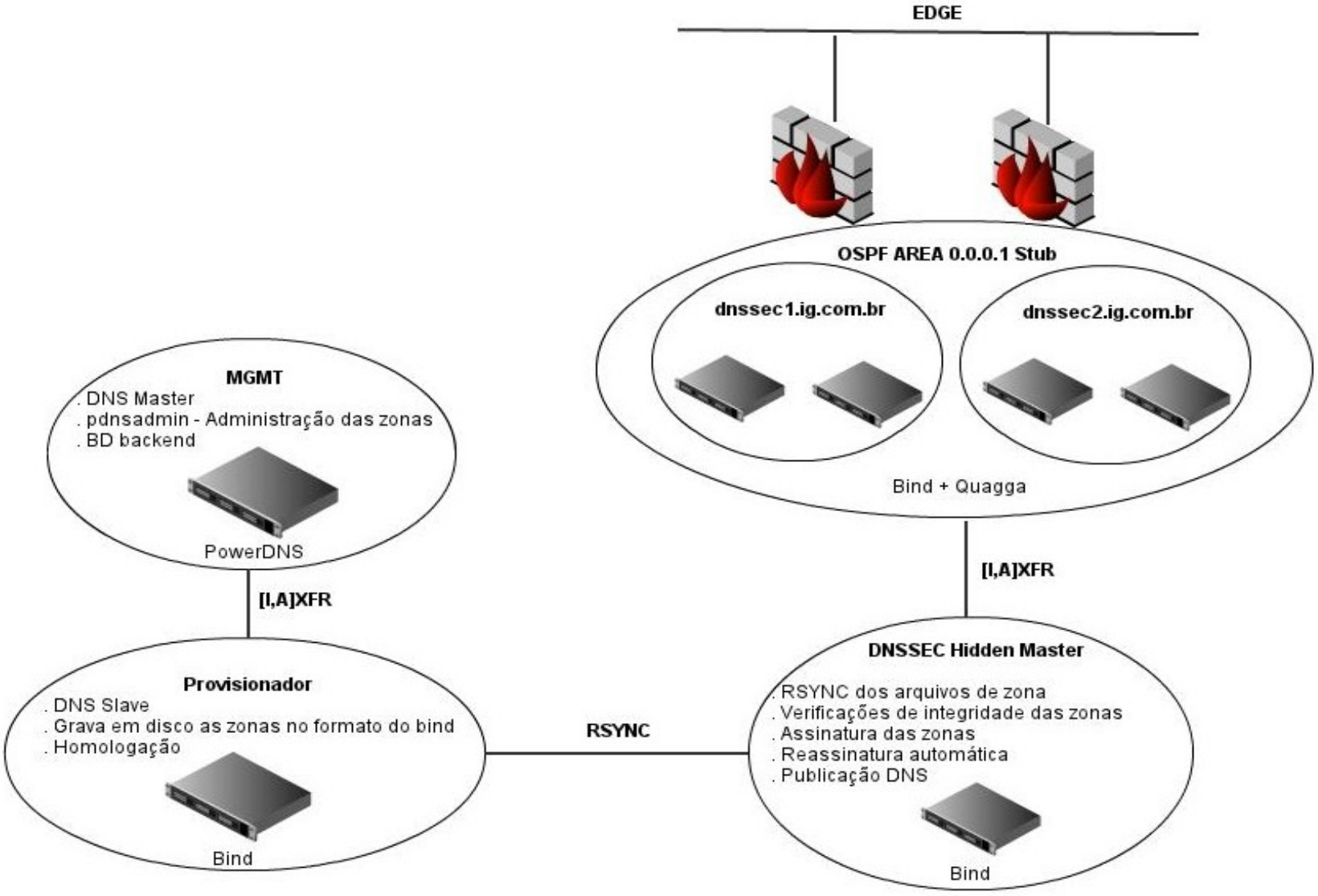
Política de chaves e assinaturas

- **KSK RSASHA1 1024 bits**
  Assina todo o conteúdo da zona
  Rollover a cada 12 meses - método double-sign

- **RRSIG's – assinaturas válidas por 30 dias**

- **Reassinatura automática**

Autoritativo - Infraestrutura



Autoritativo - Ferramentas

- ***Pdnsadmin* – Desenvolvimento interno**
  - Administração de zonas/registros
  - Validação
  - Provisionamento de zonas via rndc
  - Email notificando as alterações

- **Validações antes de cada publicação**
  - Integridade da zona
  - Número de registros alterados
  - Existência de registros importantes

- ***DSC – DNS Statistics Collector***
  - Clara visualização do uso do DNSSEC

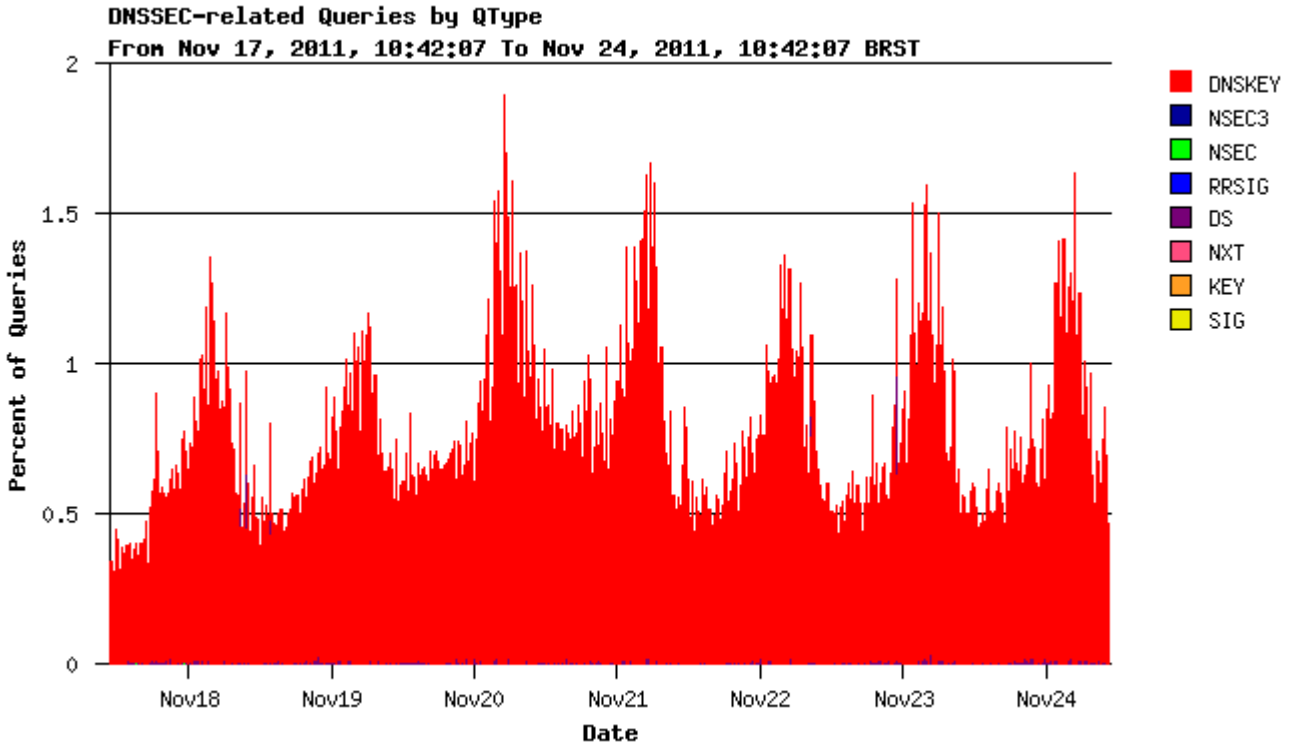
Autoritativo - Ferramentas

Analyzing DNSSEC problems for ig.com.br

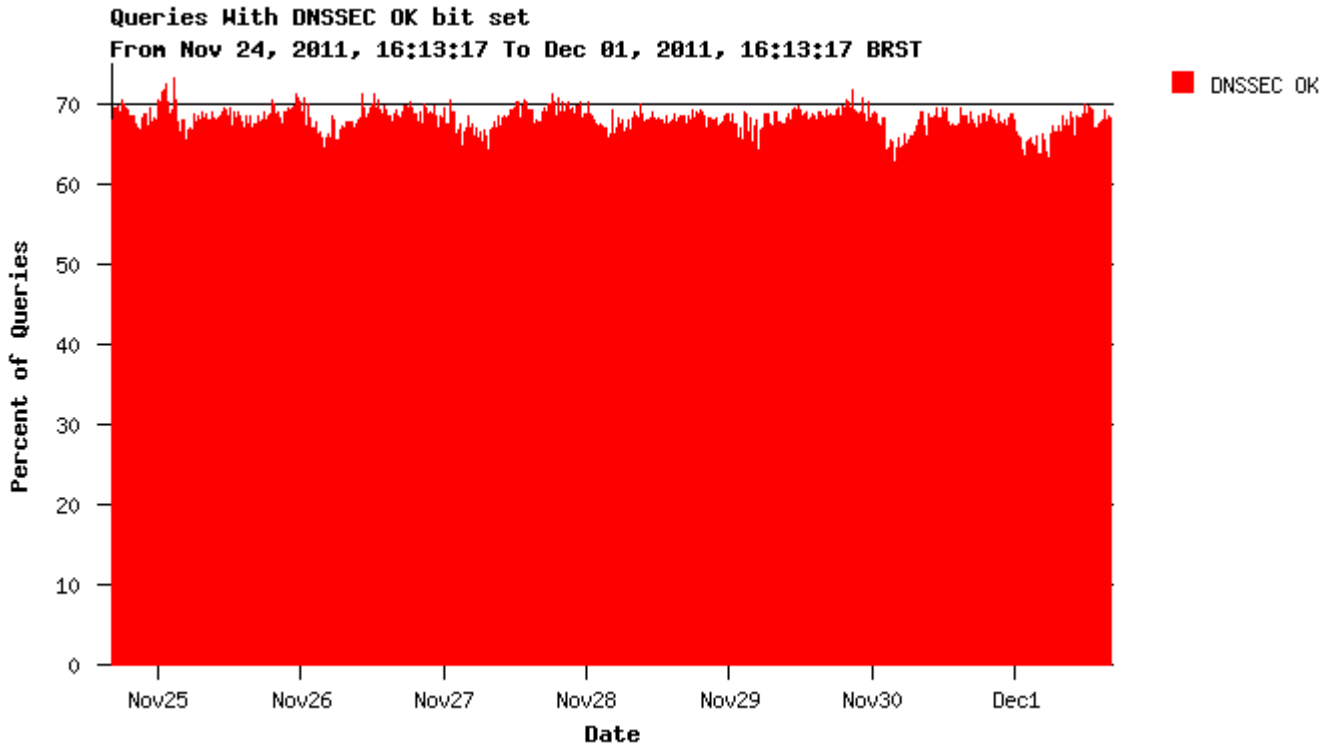
.	Found 2 DNSKEY records for . DS=19036/SHA1 verifies DNSKEY=19036/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
br	Found 1 DS records for br in the . zone Found 1 RRSIGs over DS RRset RRSIG=55231 and DNSKEY=55231 verifies the DS RRset Found 2 DNSKEY records for br DS=41674/SHA1 verifies DNSKEY=41674/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=41674 and DNSKEY=41674/SEP verifies the DNSKEY RRset
com.br	Found 1 DS records for com.br in the br zone Found 1 RRSIGs over DS RRset RRSIG=25230 and DNSKEY=25230 verifies the DS RRset Found 1 DNSKEY records for com.br DS=31554/SHA1 verifies DNSKEY=31554/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=31554 and DNSKEY=31554/SEP verifies the DNSKEY RRset
ig.com.br	Found 1 DS records for ig.com.br in the com.br zone Found 1 RRSIGs over DS RRset RRSIG=31554 and DNSKEY=31554/SEP verifies the DS RRset Found 1 DNSKEY records for ig.com.br DS=56476/SHA1 verifies DNSKEY=56476/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=56476 and DNSKEY=56476/SEP verifies the DNSKEY RRset ig.com.br A RR has value 187.31.64.25 Found 1 RRSIGs over A RRset RRSIG=56476 and DNSKEY=56476/SEP verifies the A RRset

- **Verisign DNSSEC Analyzer**
  http://dnssec-debugger.verisignlabs.com

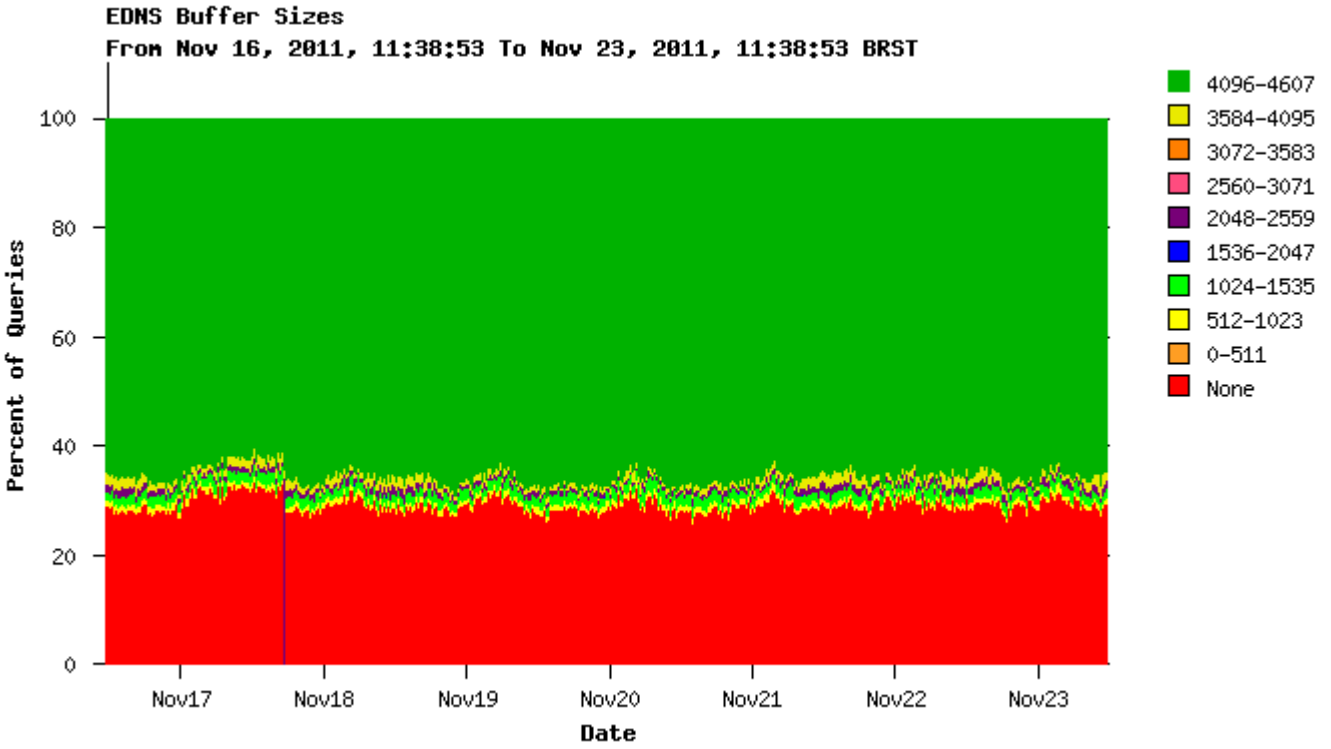
Autoritativo - Estatísticas



Autoritativo - Estatísticas



Autoritativo - Estatísticas



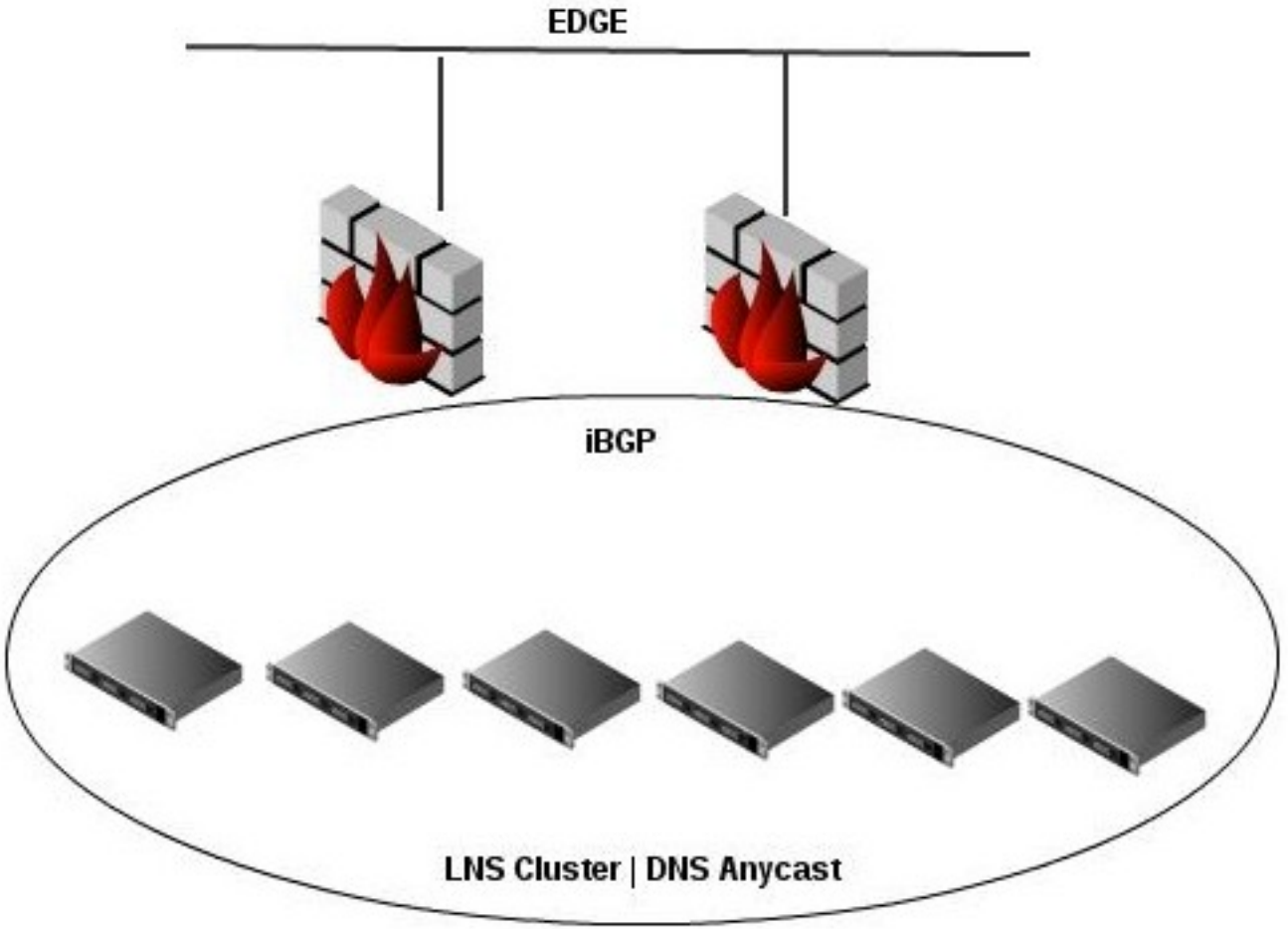
Recursivo - Infraestrutura

- **Atende aos clientes do dial iG**
  Alguns milhares de clientes simultâneos
- **Ancorada chave da raiz - Rollover automático**
- **Preocupações**

  Servidores
  CPU - Custo da criptografia
  Memória - RRSET + RRSIG
  EDNS0 – Evitar aumento de consultas via TCP

  Clientes
  Latência nas respostas
  MTU – Clientes via túnel L2TP

Recursivo - Infraestrutura



Recursivo - Estatísticas

- **CPU**

  Aumento de consumo não relevante **neste ambiente**

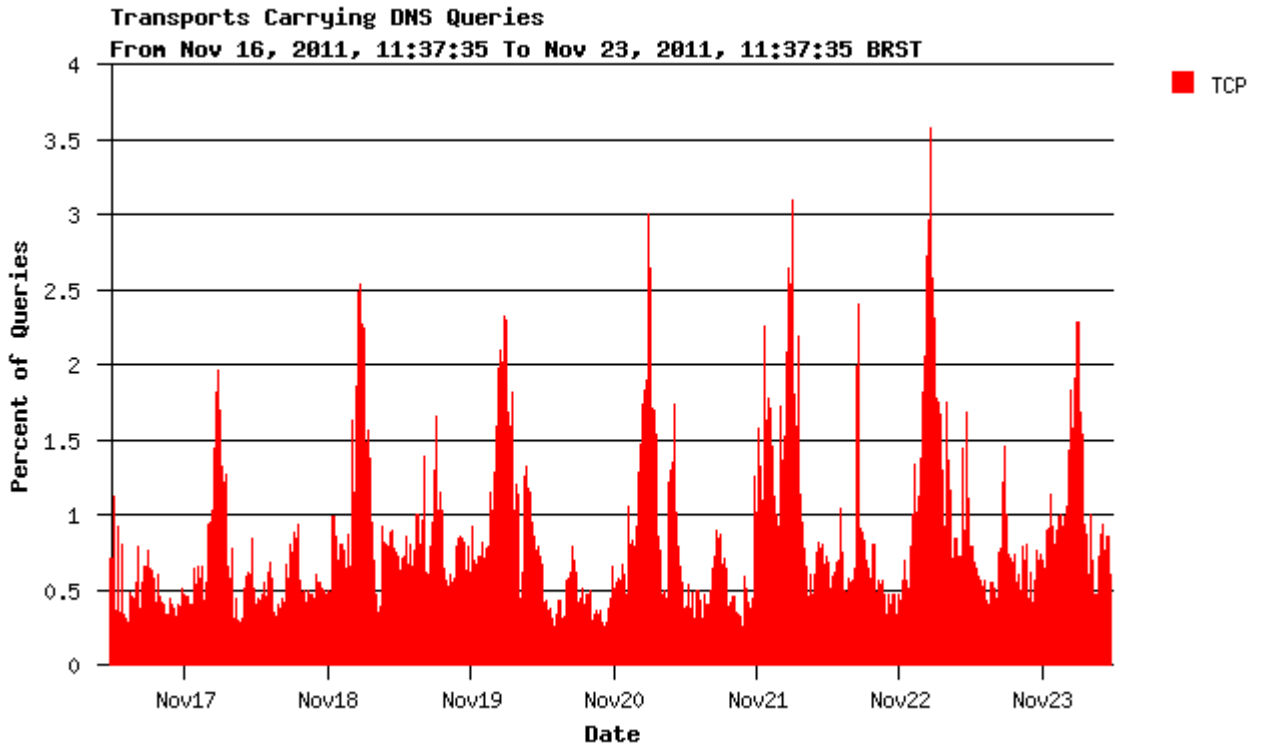
  Devido à...

  90% das queries em cache
  Os domínios mais consultados não estão assinados
  Cache dos registros já validados – DS, DNSKEY, RRSIG

- **ENDS0 – edns-udp-size**

- **MTU - max-udp-size**

Recursivo - Estatísticas



OBRIGADO !

Wilson Rogério Lopes
Gerência de Datacenter
wlopes@ig.com
noc@ig.com