Anycast f.dns.br
DNSSEC updates

GTER29 - 15/05/2010 - São Paulo

Frederico A C Neves <fneves@registro.br>

Anycast f.dns.br

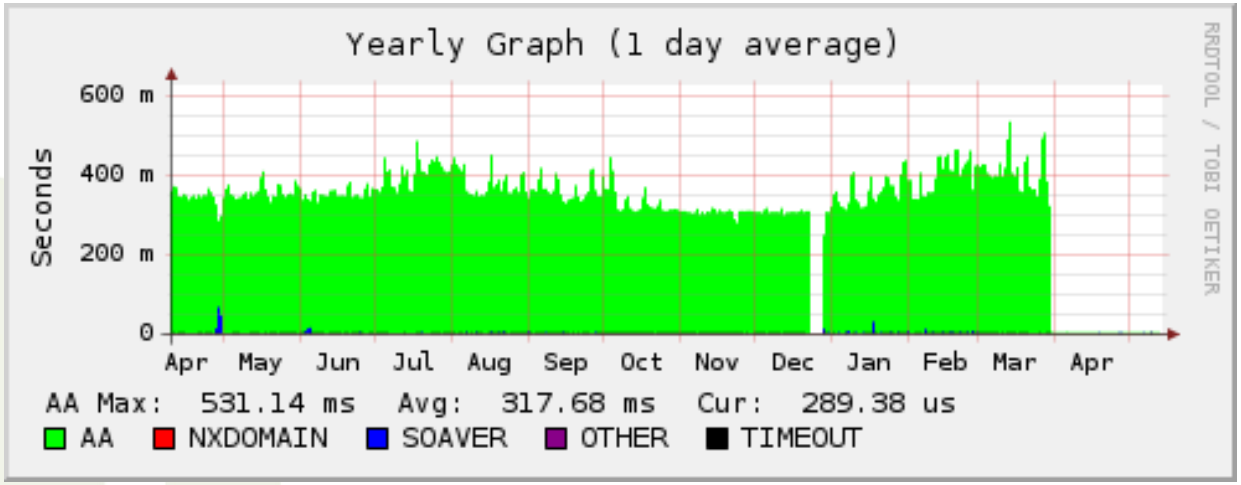
- Originalmente cluster Unicast em Seul ASN14650
- Excelente Cobertura na Asia
- RTT alto para o Brasil (~400ms)
- Propósitos
  - reduzir RTT para o público local
  - Melhor resiliência do conjunto
- Inicialmente 3 pontos no Brasil (PTTMetro ATM) e 3 pontos no exterior
- Anycast exclusivamente local - sem a necessidade de trânsito (salvo gerência)

Primeiro Servidor PTTMetro São Paulo

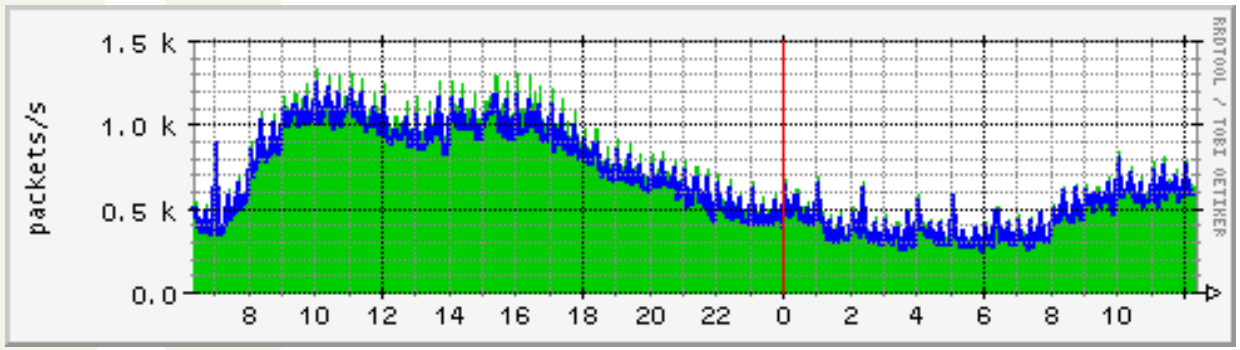
> dig @f.dns.br hostname.bind chaos txt +short
"f1.a.f.dns.br”

> dig @f.dns.br hostname.bind chaos txt | grep time
;; Query time: 0 msec

RTT

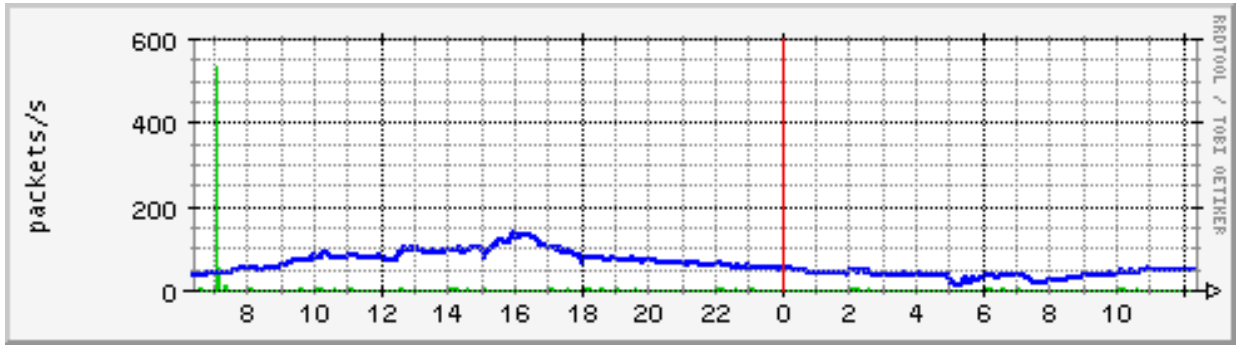


Trafego



Problema - Assimetria devido a Inexistência de PATH

Gerência

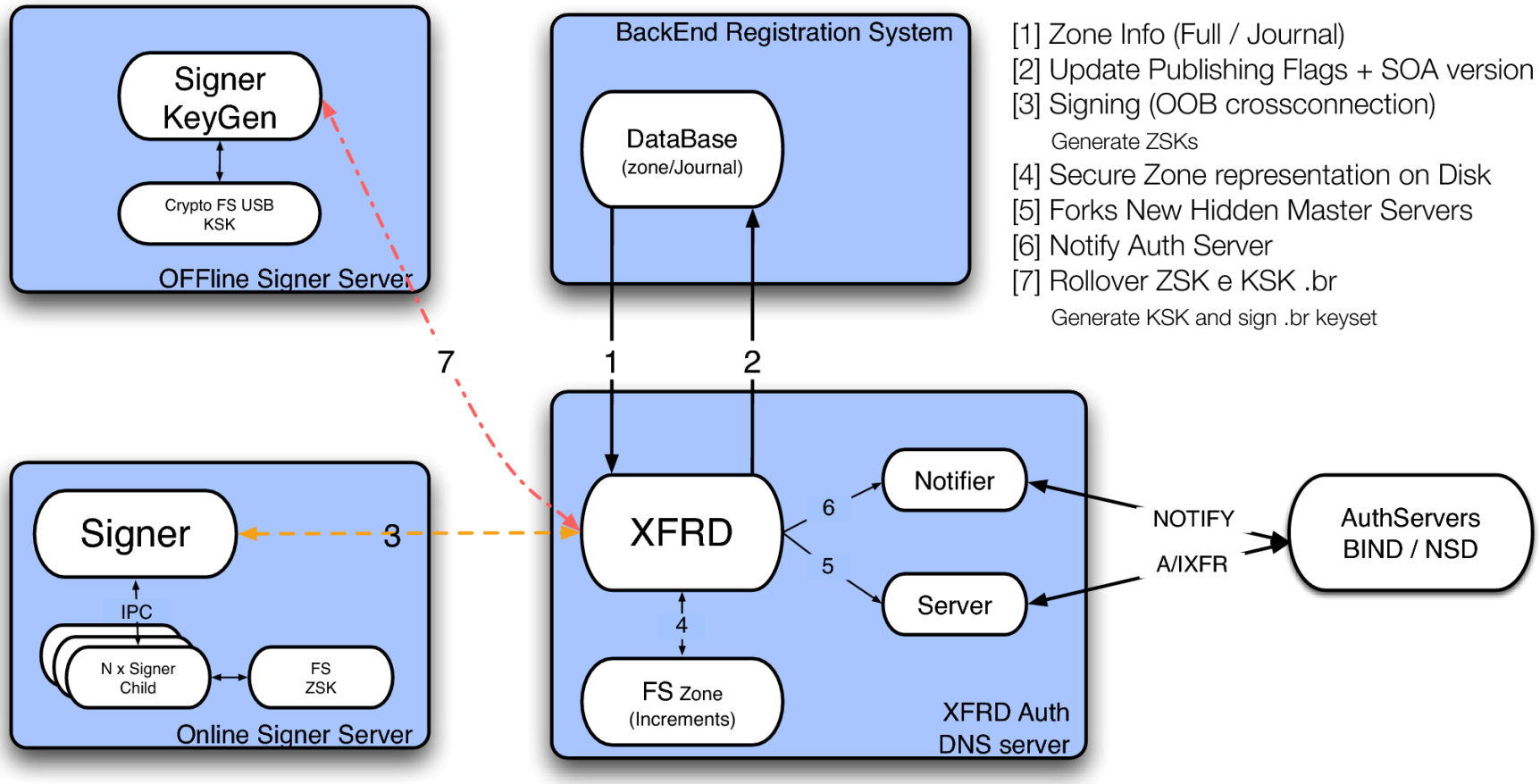


- ~100pps não sabem como retornar ao solicitante
- Complica a hospedagem do serviço
  - Filtros (p.ex. uRPF)
- Reduz a resiliência pois implica em recursos da rede que hospeda o serviço
- Assimetrias de roteamento são comuns, mas não pela inexistência do PATH
- Pode indicar problemas no iBGP e falta de BCP38
- Debug trabalhoso - Notificaremos os “Agressores” :-)

DNSSEC Updates
Política de chaves

- http://registro.br/info/dnssec-policy.html
- KSK BR
  - RSASHA1 1280 bits
  - Rollover double-signing entre 2 e 5 anos
    - Terceira semana de maio
- ZSK BR
  - RSASHA1 1152 bits
  - Rollover pre-publishing a cada 3 meses
    - Primeira semana de fev/mai/ago/nov
- ZSK *.BR
  - RSASHA1 1024 bits
  - Rollover pre-publishing mensal
    - Segunda semana do mês

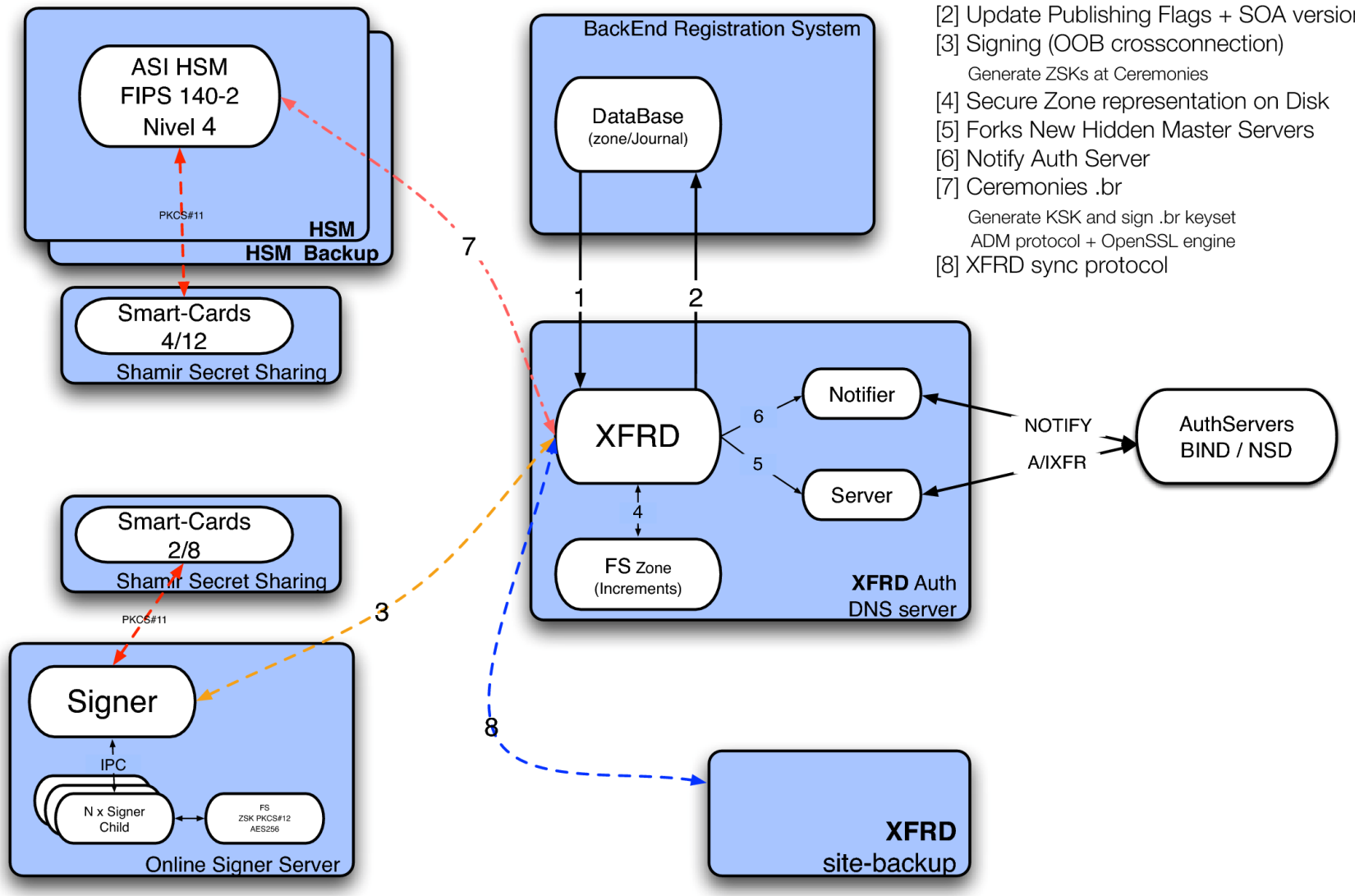
Modelo Anterior



Deficiências - Modelo Anterior

- Falta de redundância de hardware e dados
- Chaves armazenadas em aberto no Signer
- Rollovers manuais
- Manipulação da KSK BR no offline-signer

Novo Modelo



[1] Zone Info (Full / Journal)
[2] Update Publishing Flags + SOA version
[3] Signing (OOB crossconnection)
Generate ZSKs at Ceremonies
[4] Secure Zone representation on Disk
[5] Forks New Hidden Master Servers
[6] Notify Auth Server
[7] Ceremonies .br
Generate KSK and sign .br keyset
ADM protocol + OpenSSL engine
[8] XFRD sync protocol

Melhorias - Novo Modelo

- Redundância (Site backup)
- Proteção das chaves no signer
- HSM – Hardware Security Module
- Automatização de Rollovers
- Validação da zona pré-publicada

Redundância

- Site backup
  - Réplica dos elementos mantidos no site em produção
- Sincronização online
  - Túnel IPsec mantém os sites interligados de forma segura
  - Rsync cuida da replicação dos dados

Novo Signer

- Chaves criptografadas em disco
  - PKCS#12
  - AES-256
- Proteção por Smart Cards
  - Esquema 2:8 (Shamir Secret Sharing Scheme)
  - Smart Cards necessário para ativação

(decriptação das chaves)

HSM – Hardware Security Module

- Hardware criptográfico
- Substitui o offline-signer
- Responsável pela manipulação da KSK BR
- Protegida por Smart Cards (SSSS)
- Grupos: Admistradores, Auditores e Operadores
- Será manipulada apenas nas cerimônias (2 vezes ao ano)

Automatização de Rollovers

- Troca de chaves DNSKEY
- Cerimônias semestrais
- Geração de chaves para o período de um semestre
- Geração de assinaturas da KSK BR (HSM)
- Monitoração remota dos rollovers

Validação da zona pré-publicada

- Validação da cadeia de confiança DNSSEC
- Consistência dos registro da prova de não existência
- Verificação de porcentagem máxima de mudança em publicações incrementais
- Caso haja alguma inconsistência, a publicação não ocorre

Cerimônias 13/05/2010

1. Ativação da HSM

2. Cerimônia 2010 – 01 (NIC.br)

3. Cerimônia 2010 – 02 (Oi)

Primeiros resultados serão observados
24/05/2010 Início do Rollover da ZSK .br
31/05/2010 Início do Rollover da KSK .br

Perguntas ?

Obrigado