Firewalls e DNS

Como e por que configurar corretamente

Hugo Koji Kobayashi

<koji at registro.br>

Registro.br

GTS-9 - 30 de Junho de 2007

Agenda

- Principais características do protocolo DNS original
- Extension Mechanisms for DNS (EDNS0)
- Firewalls e DNS

Parte I

Principais características do protocolo DNS original

DNS - Características originais do protocolo

- Definido nas RFCs 1034 e 1035.
- Banco de dados distribuído através de uma arquitetura hierárquica, cujo principal propósito é a resolução de nomes de domínio.
- Servidores aceitam consultas em transporte TCP/UDP, porta 53.
- Payload máximo em transporte UDP de 512 bytes.
- Payload máximo por mensagem DNS em TCP de 64 Kbytes.

Formato da mensagem DNS

ID, flags e contadores

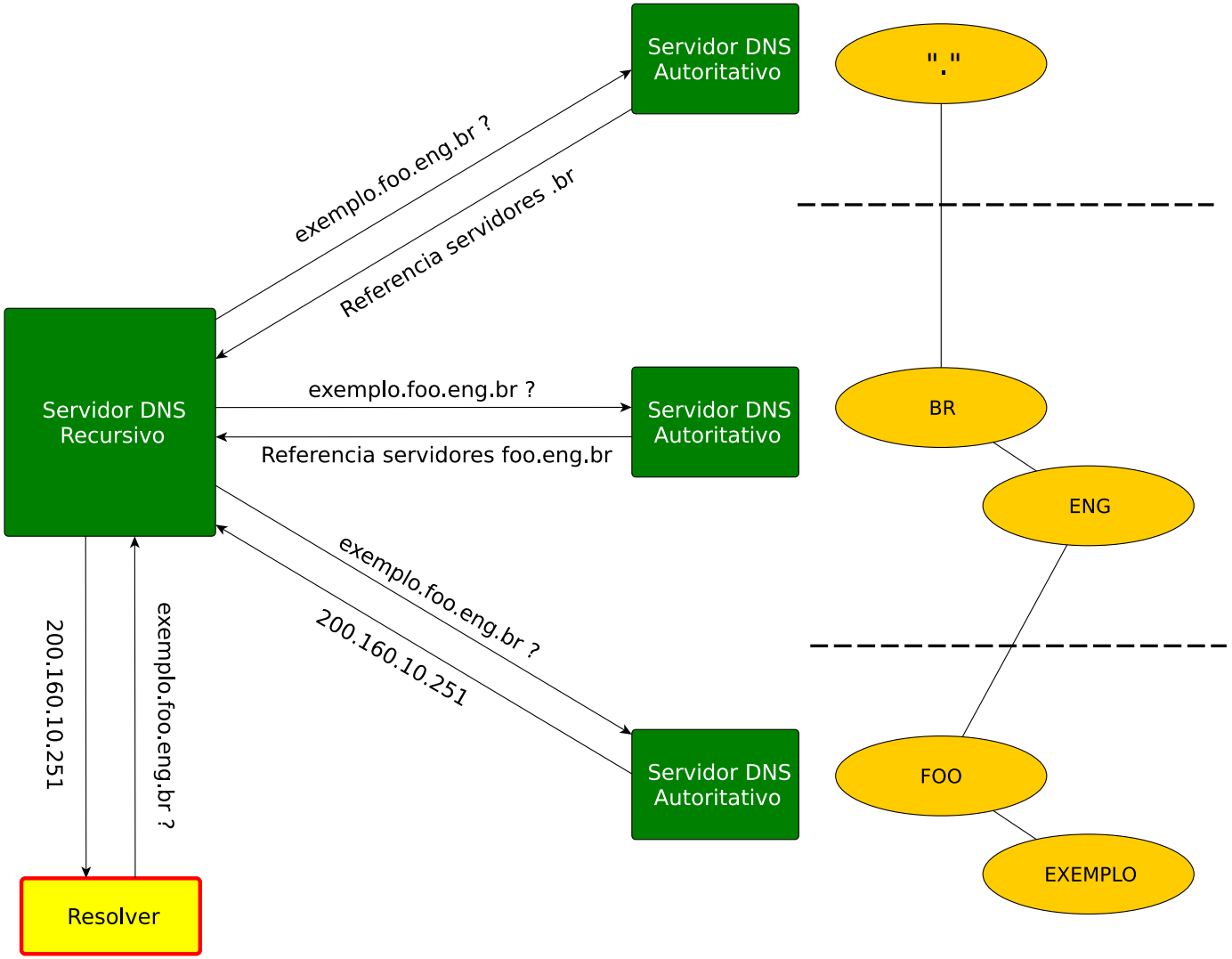
Pergunta ao servidor

RRs com resposta a pergunta

RRs indicando autoridade sobre a pergunta

RRs contendo informações adicionais

Funcionamento básico DNS



Quando TCP é utilizado

- Transferências de zona (AXFR)
- Respostas com payload maior do que 512 bytes:
  1. Consulta inicial via UDP.
  2. Resposta maior do que 512 bytes, flag TC [1] é marcado para indicar que sua resposta está truncada.
  3. Cliente refaz consulta via TCP.

[1] Servidor autoritativo procura evitar o uso do flag TC removendo RRs da seção Additional da mensagem DNS sempre que possível a fim de evitar que cliente precise refazer a consulta via TCP.

Parte II

Extension Mechanisms for DNS (EDNS0)

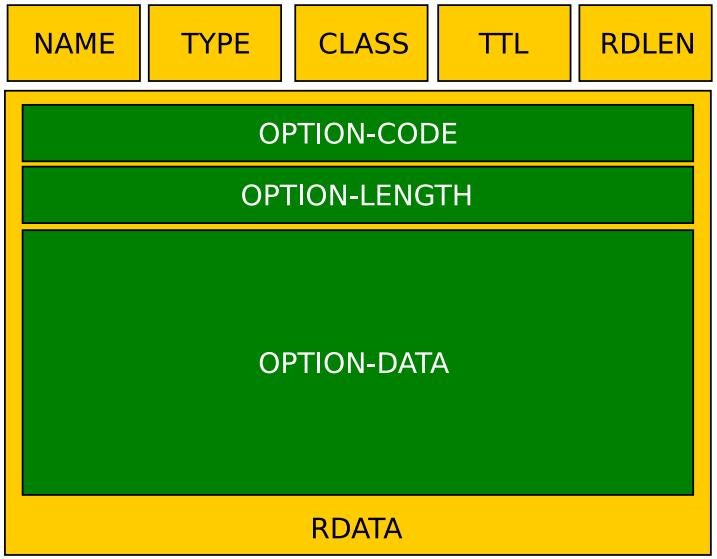
EDNS0 - Extension Mechanisms for DNS

registro.br
Registro de Domínios para a Internet no Brasil

- Definido na RFC 2671
- Extensão ao protocolo DNS original para eliminar alguns limites do protocolo.
- Permite:
  - mais flags e RCODEs ao cabeçalho DNS
  - novos tipos de labels
  - payloads maiores em transporte UDP (limitado a 64 Kbytes)
- Define um novo pseudo-RR: OPT

nic.br

EDNS0 - pseudo-RR OPT



NAME	‘‘.’’
TYPE	‘‘OPT’’
CLASS	Tamanho do pacote UDP
TTL	RCODE estendido e Flags
RDATA	Pares {atributo,valor}

Pseudo-RR OPT

- Não armazena dados de DNS como outros RRs
- Não é cacheado ou armazenado em arquivo, sendo utilizado apenas no momento da comunicação entre servidores

EDNS0 - Como funciona?

- Depende de suporte tanto no cliente como no servidor.
- Cliente envia consulta UDP com pseudo-RR OPT na seção Additional da mensagem DNS, informando qual o tamanho máximo de respostas UDP que pode processar.
- Se servidor suportar EDNS0, pode aumentar o limite para o tamanho da resposta que vai retornar ao cliente, evitando re-query via TCP.
- Se servidor não suportar EDNS0, envia resposta com até 512 bytes de payload DNS.

EDNS0 - Uso

- Transição de IPv4 para IPv6:
  Existência de records A e AAAA simultanemente, fazendo com que respostas que contêm glue records fiquem maiores.
  Por exemplo, o "priming request" (consulta aos records NS da raiz) que atualmente tem 436 bytes de payload DNS, passaria a 811 bytes de payload DNS quando houver glue IPv6 para todos os 13 servidores da raiz.
- DNSSEC:
  EDNS0 é mandatório (bit "DNSSEC OK" (DO)).
  Respostas maiores principalmente pelo tamanho de records RRSIG e DNSKEY.

EDNS0 - Suporte em servidores

Alguns exemplos de servidores que suportam EDNS0:

- Bind (desde 8.3.x - 2001)
- Microsoft DNS server (Windows 2003)
- NSD (auth only - desde 1.x - 2003)
- ANS/CNS

Parte III

Firewalls e DNS

Por que configurar corretamente?

registro.br
Registro de Domínios para a Internet no Brasil

- Garantir qualidade na resolução DNS, ou seja, evitar atrasos e, principalmente, a impossibilidade de resolução de nomes
- Evitar overhead desnecessário em servidores DNS, tanto recursivos como autoritativos

nic.br

Firewalls e DNS

- Autoritativos:
  - Consultas com destino à porta 53 UDP e TCP do servidor autoritativo e respectivas respostas devem ser permitidas.
- Recursivos:
  - Consultas do servidor recursivo com destino à porta 53 UDP e TCP de qualquer outro servidor e respectivas respostas devem ser permitidas.
  - Consultas vindas de **clientes autorizados** com destino à porta 53 UDP e TCP do servidor recursivo e respectivas respostas devem ser permitidas.
  - Bloqueio às demais consultas DNS direcionadas ao servidor recursivo.

Open Recursive Resolvers

- São servidores recursivos que aceitam consultas DNS vindas de qualquer computador na Internet.
- Problemas:
  - Ataques de envenenamento de cache, que levam o servidor recursivo a armazenar informações forjadas;
  - Ter o servidor utilizado para ataques DDoS.
- Como resolver: a solução recomendada é separar os servidores autoritativos e recursivos em computadores distintos e limitar o acesso ao servidor recursivo a clientes de sua rede.
- Mais detalhes no documento do CERT.br "Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos": http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Firewalls e DNS/UDP > 512 bytes

Se seu servidor recursivo suporta EDNS0, verifique se seu firewall permite datagramas UDP/DNS com mais de 512 bytes. Um teste pode ser feito através da seguinte consulta (935 bytes de payload DNS):

dig @a.dns.br br ns +dnssec +bufsize=1000

Se a resposta não for recebida, pode-se:

- corrigir o comportamento do firewall;
- diminuir o payload máximo enviado via record OPT na configuração EDNS0 do servidor para 512 bytes.

Firewalls e fragmentos UDP

Se seu servidor recursivo suporta EDNS0 e o firewall suporta mensagens DNS maiores que 512 bytes, verifique se seu firewall é capaz de fazer o correto reassembly de datagramas UDP fragmentados. Um teste pode ser feito através da seguinte consulta (2185 bytes de payload DNS):

```
dig @a.dns.br br dnskey +dnssec +bufsize=2500
```

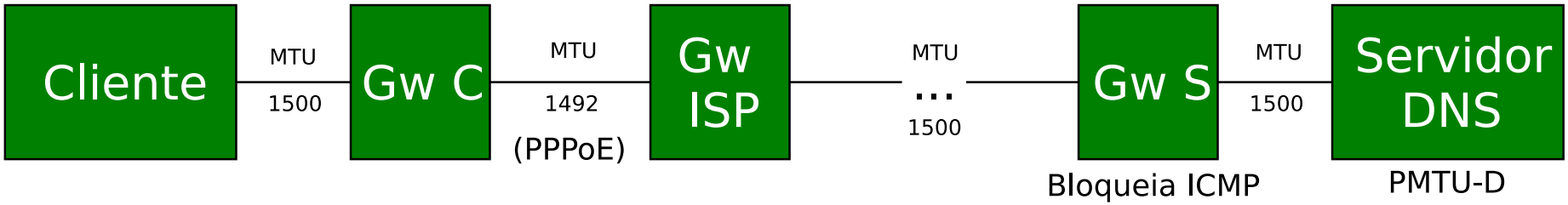
Se a resposta não for recebida, pode-se:

- corrigir o comportamento do firewall;
- diminuir o payload máximo enviado via record OPT na configuração EDNS0 do resolver. RFC EDNS0 sugere que se configure baseado em MTU de 1280 bytes.

Firewalls e PMTU-D (1)

- A medida que DNSSEC for adotado, a quantidade de mensagens DNS maiores do que o MTU da rede tende a aumentar.
- Boa parte destas mensagens poderão ser transportadas via TCP.
- Para garantir o funcionamento de PMTU-D em seus servidores, seu firewall e outros dispositivos de roteamento em sua rede **não devem descartar** mensagens ICMP do tipo 3, código 4 ("destination unreachable", "fragmentation needed but don't fragment bit set").

Firewalls e PMTU-D (2)



1. Cliente faz consulta DNS via UDP e recebe resposta com bit TC=1. Servidor quer enviar resposta com payload de 2185 bytes.
2. Cliente descarta resposta UDP e refaz a consulta usando TCP.
3. Como MTU dos segmentos de rede do Cliente e Servidor é de 1500 bytes e o servidor implementa PMTU-D, este envia primeiro pacote IP com 1500 bytes e bit DF=1 (header IP).
4. Quando pacote IP chega em GWISP, este descarta o pacote IP e retorna mensagem ICMP Can't fragment (tipo 3, código 4).
5. Porém, como GWS filtra ICMP, servidor DNS não o recebe e depois de algum tempo tenta o envio novamente do pacote de 1500 bytes e bit DF=1, até a sessão TCP expirar [2]. Resolução DNS falha!

[2] Algumas implementações de PMTU-D detectam este tipo de situação, mas ainda assim com perda de performance.

Referências

RFC 1034
DOMAIN NAMES - CONCEPTS AND FACILITIES

RFC 1035
DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

RFC 1191
Path MTU Discovery

RFC 2181
Clarifications to the DNS Specification

RFC 2671
Extension Mechanisms for DNS (EDNS0)

RFC 2923
TCP Problems with Path MTU Discovery

RFC 4472 - Apêndice B
Operational Considerations and Issues with IPv6 DNS

RFC 4821
Packetization Layer Path MTU Discovery

Referências


RFC 4033
DNS Security Introduction and Requirements


RFC 4034
Resource Records for the DNS Security Extensions


RFC 4035
Protocol Modifications for the DNS Security Extensions


Tutorial DNSSEC
ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf


Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/


Testing Firewalls for IPv6 and EDNS0 Support
http://www.icann.org/committees/security/sac016.htm


Testing Recursive Name Servers for IPv6 and EDNS0 Support
http://www.icann.org/committees/security/sac017.htm


Acommodating IPv6 Address RRs for the Root of the DNS
http://www.icann.org/committees/security/sac018.pdf

Obrigado!

Perguntas? Comentários?