Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos

Cristine Hoepers, Klaus Steding-Jessen, Nelson Murilo, Rafael R. Obelheiro
Versão: 1.1 – 16/02/2007

Sumário

1 Descrição do Problema

Dois tipos bastante utilizados de servidores DNS (*Domain Name System*) são o autoritativo e o recursivo, que embora possam ser executados em uma mesma máquina, possuem características distintas:

- O autoritativo é responsável por manter os mapas referentes a uma zona local e responder a requisições vindas de máquinas de todo o mundo, que precisarem resolver nomes de domínio da zona sobre a qual este servidor tem autoridade;
- O recursivo é responsável por receber as consultas DNS dos clientes locais e consultar os servidores externos, de modo a obter respostas às consultas efetuadas.

Um problema bastante comum de configuração é permitir que qualquer máquina na Internet faça consultas ao servidor DNS recursivo de uma determinada rede. Servidores com esse problema são comumente chamados de servidores DNS recursivos abertos, pois apenas o servidor autoritativo é que deve responder a consultas vindas de máquinas externas.

1.1 Possíveis Riscos

Qualquer organização que possua um servidor DNS recursivo aberto corre o risco de ter esse servidor envolvido nos seguintes ataques:

- Ser vítima de ataques de envenenamento de *cache* (*cache poisoning*), que levam o servidor recursivo a armazenar informações forjadas. Tais informações podem ser usadas para comprometer a segurança de clientes que façam consultas a esse servidor.
- Ter esse servidor abusado por atacantes e utilizado para desferir ataques de negação de serviço distribuídos (DDoS), que podem implicar nas seguintes conseqüências:
  - o grande número de consultas DNS forjadas recebidas e, principalmente, a quantidade de respostas grandes enviadas para a vítima, podem consumir uma quantidade considerável de banda da rede com um servidor DNS recursivo aberto;
  - dependendo do contrato do provedor de conectividade, a rede com o DNS aberto sendo abusado pode ser co-responsabilizada em caso de ataque de negação de serviço contra terceiros.

  Para detalhes técnicos sobre este tipo de ataque, consulte a seção “Características do Ataque de Negação de Serviço Abusando de Servidores DNS Recursivos Abertos”.

Importante: caso a rede onde está instalado o servidor DNS recursivo, mesmo que configurado corretamente, não possua regras de *ingress filtering*, um atacante pode forjar o IP dos clientes desse servidor e realizar consultas DNS em grande quantidade, causando uma negação de serviço interna à rede.

2 Soluções para o Problema

Para solucionar o problema dos servidores DNS recursivos abertos é necessário separar os servidores autoritativo e recursivo e atribuir políticas de acesso diferentes a cada um. Isto pode ser feito de duas maneiras:

- Colocando os servidores DNS em computadores diferentes, com configurações e políticas de acesso diferentes; ou
- Utilizando o conceito de *views* (visões ou vistas) do BIND 9 (*Berkeley Internet Name Domain* versão 9).

Importante: Caso seja implementada a solução utilizando computadores diferentes para os servidores recursivos e autoritativos, os registros NS das zonas servidas devem apontar apenas para os servidores autoritativos.

Ao longo desta seção serão apresentadas sugestões de configuração para os servidores BIND 9 e Microsoft DNS.

2.1 Sistemas Unix com BIND 9

Se você utiliza BIND 9 é possível solucionar o problema de duas maneiras:

- executando os servidores DNS autoritativo e recursivo em um único computador, com a utilização de *views*;
- executando cada um dos servidores DNS em computadores diferentes.

2.1.1 Configuração Usando *Views*

Nesta solução definem-se pelo menos duas *views* possíveis para o servidor DNS, uma para acesso de clientes específicos e outra para acesso por parte da Internet como um todo. A ordem em que são definidas as *views* é importante: as *views* devem ser definidas da mais específica para a mais geral.

No exemplo abaixo foram definidas duas *views*: interna e externa. Na *view* interna foi definido que somente algumas máquinas podem fazer consultas recursivas. Na *view* externa foi explicitamente definido que não se faz recursão e não será enviada nenhuma resposta para as consultas recursivas, através das seguintes diretivas:

```
        recursion no;
        additional-from-auth no;
        additional-from-cache no;
```

Segue abaixo um exemplo de configuração para o arquivo `named.conf`:

```
// lista de redes ou maquinas que podem fazer consultas recursivas
acl clientes {
        localhost;
        192.0.2.64/26;
        192.0.2.192/28;
};
```

```
// definicao da view interna -- deve vir antes da view externa
// esta view permite recursao para as redes da acl clientes
view "interna" {
        match-clients { clientes; };
        recursion yes;

        // dentro desta view sao colocadas as zonas padrao:
        // ".", localhost, etc, e qualquer outra zona que
        // seja somente interna para a rede em questao
};

// definicao da view externa -- deve ser a ultima view definida
// esta view permite consultas de qualquer rede, mas nao permite
// consultas recursivas
view "externa" {
        match-clients { any; };
        recursion no;
        additional-from-auth no;
        additional-from-cache no;

        // aqui sao colocadas as zonas master
        //
        // zone "exemplo.com.br" {
        //       type master;
        //       file "master/exemplo.com.br";
        // };

        // aqui sao colocadas as zonas slave
        //
        // zone "exemplo.net.br" {
        //       type slave;
        //       file "slave/exemplo.net.br";
        //       masters { 192.0.2.1; [...;] };
        // };
};
```

2.1.2 Configuração Usando Servidores Distintos

Servidor Autoritativo

As configurações abaixo devem ser colocadas no arquivo `named.conf` do servidor DNS autoritativo:

```
// adicionar as diretivas abaixo dentro da clausula options
// para desabilitar recursao no servidor autoritativo
options {
        recursion no;
        additional-from-auth no;
        additional-from-cache no;
};
```

Servidor Recursivo

Para o servidor recursivo é necessário combinar regras de filtragem em um *firewall*, idealmente *stateful*, com configurações no arquivo `named.conf`.

- Configuração do *Firewall*:
  Para garantir que sejam atendidos apenas clientes de redes permitidas e que o servidor recursivo possa fazer as consultas aos servidores DNS externos, é necessário ter o seguinte conjunto de regras no *firewall*:
  1. Permissão de consultas ao servidor recursivo somente para os clientes autorizados:
     Tráfego vindo dos clientes autorizados, com destino às portas 53/UDP e 53/TCP do servidor recursivo, deve ser liberado;
  2. Permissão para o servidor recursivo consultar servidores DNS externos e receber as respostas:
     Permitir tráfego originado do servidor recursivo com destino às portas 53/UDP e 53/TCP de qualquer máquina, permitindo também o retorno das respostas. Nesse caso a melhor solução é a utilização de um *firewall stateful*.
  3. Bloquear quaisquer outras conexões externas ao servidor DNS recursivo.
- Configuração do `named.conf`:
  As opções abaixo devem ser colocadas no arquivo `named.conf` do servidor DNS recursivo:

```
// colocar a seguinte diretiva na clausula options
// permitindo recursao
// IMPORTANTE: Esta opcao deve ser usada em conjunto com
// regras de firewall
options {
        recursion yes;
};
```

2.2 Servidores Microsoft

2.2.1 Microsoft DNS

Servidores Microsoft que estejam utilizando o servidor DNS nativo precisam, necessariamente, ter seus servidores autoritativos e recursivos separados em máquinas distintas, de acordo com as seguintes recomendações:

Servidor Recursivo

Deve ser colocado em uma máquina que seja acessível somente pelas redes internas ou outras máquinas que tenham permissão para fazer consultas recursivas. Essa restrição deve ser feita através de um *firewall* no próprio servidor ou por outro *firewall*, colocado entre esta máquina e as redes externas.

- Configuração do *Firewall*:
  Para garantir que sejam atendidos apenas clientes de redes permitidas e que o servidor recursivo possa fazer as consultas aos servidores DNS externos, é necessário ter o seguinte conjunto de regras no *firewall*:
  1. Permissão de consultas ao servidor recursivo somente para os clientes autorizados:
     Tráfego vindo dos clientes autorizados, com destino às portas 53/UDP e 53/TCP do servidor recursivo, deve ser liberado;
  2. Permissão para o servidor recursivo consultar servidores DNS externos e receber as respostas:

Permitir tráfego originado do servidor recursivo com destino às portas 53/UDP e 53/TCP de qualquer máquina, permitindo também o retorno das respostas. Nesse caso a melhor solução é a utilização de um *firewall stateful*.

3. Bloquear quaisquer outras conexões externas ao servidor DNS recursivo.

Servidor Autoritativo

Deve ter a recursão desligada e ser colocado em uma máquina diferente daquela que possuir o servidor recursivo. Vale lembrar que ao utilizar computadores diferentes para os servidores recursivos e autoritativos, os registros NS das zonas servidas devem apontar apenas para os servidores autoritativos. Os seguintes documentos possuem instruções sobre como desligar a recursão em servidores DNS Microsoft:

- *Securing DNS for Windows 2003 – Disabling Recursion*
  `http://technet2.microsoft.com/WindowsServer/en/library/e01d4b07-21a9-4952-a13a-6a9e0e17cb851033.mspx`
- *Windows Server 2003 Product Help – Disable recursion on the DNS server*
  `http://technet2.microsoft.com/windowsserver/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx`
- *Fixing Open DNS Servers – Windows NT, 2000 and 2003*
  `http://www.dnsstuff.com/info/opendns.htm`
- *The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0)*
  `http://www.uscert.gov/reading_room/DNS-recursion033006.pdf`

2.2.2 BIND 9

Em servidores Windows, uma alternativa à utilização de servidores nativos Microsoft é a utilização de BIND 9 para Windows.

Com a utilização do BIND 9 é possível a implementação da solução com *views*, discutida na seção “Sistemas Unix com BIND 9”, que permite a utilização de um único servidor, porém com uma separação entre o recursivo e o autoritativo.

Na página do BIND (`http://www.isc.org/sw/bind/`), na seção *Current Release*, estão disponíveis versões para Windows.

A configuração é igual à dos sistemas Unix. Recomenda-se a leitura da seção “Sistemas Unix com BIND 9” para instruções mais detalhadas.

2.3 Mac OS X 10.3 ou Posterior

Segundo o guia de Administração de Serviços de Rede do Mac OS X Server (*Mac OS X Server Network Services Administration*), o sistema utiliza o BIND 9, e recomenda que seja editado o arquivo `/etc/named.conf`, seguindo as orientações do próprio BIND 9 para configuração das restrições de consultas ao servidor recursivo.

Os seguintes documentos disponibilizados pela Apple servem de referência para administração de servidores Mac OS X e podem auxiliar no processo de configuração do BIND:

- *Mac OS X Server Network Services Administration – for Version 10.3 or Later*
  `http://www.apple.com/server/pdfs/Network_Services.pdf`
- *Mac OS X Server Command-Line Administration – for Version 10.3 or Later*
  `http://www.apple.com/server/pdfs/Command_Line.pdf`

3 Sugestões para Mitigação do Problema

Caso não seja possível implementar as técnicas apresentadas na seção anterior por alguma característica do seu ambiente, existem para o servidor BIND algumas técnicas que permitem minimizar o problema de servidores DNS recursivos abertos. No caso do servidor Microsoft DNS não existem técnicas de mitigação, apenas as soluções apontadas na seção anterior.

Importante: as configurações apresentadas nesta seção não solucionam totalmente o problema, pois permitem:

- que sejam respondidas consultas recursivas a informações que já estão no *cache* do servidor;
- que o servidor retorne informações sobre os servidores que podem responder à consulta, gerando sempre algum fator de amplificação nas respostas – nas configurações discutidas na seção anterior a resposta será apenas "REFUSED".

3.1 BIND 9 sem Utilização de *Views* e BIND 8

As configurações abaixo devem ser colocadas no arquivo `named.conf`:

```
// lista de redes ou maquinas que podem fazer consultas recursivas
acl clientes {
        localhost;
        192.0.2.64/26;
        192.0.2.192/28;
};

// adicionar a opcao allow-recursion dentro da clausula options
// permitindo recursao apenas para a acl clientes
options {
        allow-recursion { clientes; };
};
```

3.2 Mac OS X 10.3 ou Posterior

Como o sistema utiliza o BIND versão 9, recomenda-se seguir as orientações descritas para a mitigação do problema em servidores BIND 9 ou, preferencialmente, as orientações da seção "Soluções para o Problema".

4 Testando seus Servidores

Para checar se as configurações estão funcionando é necessário fazer dois tipos de verificação:

- testar se as redes ou máquinas permitidas continuam podendo realizar consultas recursivas;
- testar se o servidor DNS está recusando consultas recursivas para IPs externos em geral.

Para facilitar o segundo teste existem diversos *sites* que permitem que você verifique se o seu servidor é ou não um servidor DNS recursivo aberto. Uma lista de alguns destes *sites* segue abaixo:

- DNSreport.com (no resultado do teste, checar em particular o item "*Open DNS servers*")
  `http://www.dnsreport.com/`
- *DNS Validation Tools*
  `http://dns.measurement-factory.com/tools/third-party-validation-tools/`
- *Measurement Factory Open Resolver Test*
  A *Measurement Factory* é uma organização que conduz diversas pesquisas na área de DNS, entre outras. Uma delas é um mapeamento dos servidores DNS recursivos abertos na Internet. Os servidores já testados pelo projeto podem ser consultados via Web ou via DNS, como descrito a seguir.

  Interface Web

  `http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl`

  Consulta DNS

  Para consultar, por exemplo, se o IP `192.0.2.1` está listado, basta executar na linha de comando:

  ```
  $ dig +short 1.2.0.192.dnsbl.openresolvers.org
  ```

  Se a resposta for `127.0.0.2`, significa que é um DNS recursivo aberto. Se a resposta for `NXDomain`, significa que o servidor não é aberto ou não foi testado.
  Se o comando `dig` não estiver disponível no sistema, uma consulta semelhante pode ser feita via `nslookup` ou `host`.

5 Comentários Adicionais

1. As configurações apresentadas na seção “Sugestões para Mitigação do Problema” não foram apontadas como soluções para o problema pelos seguintes fatores:

   - No BIND 9, caso não sejam utilizadas *views*, a configuração com a utilização da diretiva “`allow-recursion { clientes; };`” faz com que o servidor, ao receber uma consulta recursiva de uma rede externa, responda com o conteúdo do *cache* ou com os endereços dos servidores onde a resposta à consulta pode ser obtida. Em alguns casos essa resposta chega a 500 bytes, tendo potencial para ser abusada para negação de serviço, pois poderia gerar uma amplificação de até 10 vezes;
   - O BIND 8 também possui o comportamento discutido no item anterior.

2. Este documento não aborda BIND 4, pois esta versão foi descontinuada (*deprecated*). Sugere-se que aqueles que ainda utilizam BIND 4 considerem mudar seus servidores para BIND 9 ou BIND 8.

3. Recomenda-se que, adicionalmente, seus servidores DNS sigam outras boas práticas de configuração segura deste serviço, como as apresentadas nestes documentos:

   - Práticas de Segurança para Administradores de Redes Internet Versão 1.2, Seção 4.5: DNS
     `http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#subsec4.5`
   - *Secure BIND Template*
     `http://www.cymru.com/Documents/secure-bind-template.html`

4. Outra medida muito importante, para evitar que sua rede participe deste ou de outros ataques DDoS que utilizem endereços de origem forjados, é a implementação de mecanismos de *egress filtering*. Este tipo de filtragem impede que saiam de sua rede pacotes:

   - com endereço de origem pertencente a uma rede reservada;
   - com endereço de origem que não faça parte de um dos blocos de endereços da rede interna.

   Detalhes sobre esse tipo de filtragem como mecanismo de prevenção ao abuso de redes em ataques de negação de serviço, podem ser encontrados nos seguintes documentos:

   - BCP 38, RFC 2827: *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*
     `http://www.ietf.org/rfc/rfc2827.txt`
   - BCP 84, RFC 3704: *Ingress Filtering for Multihomed Networks*
     `http://www.ietf.org/rfc/rfc3704.txt`

5. É recomendável que qualquer mudança em sua infra-estrutura de DNS seja implementada primeiro em um ambiente de testes.

6 Características do Ataque de Negação de Serviço Abusando de Servidores DNS Recursivos Abertos

Uma das técnicas de DDoS utilizadas atualmente envolve a exploração de servidores DNS recursivos abertos, para gerar grandes quantidades de tráfego de resposta DNS para uma vítima cujo endereço IP está sendo forjado.

Um dos problemas fundamentais explorado nesses ataques é o fato do sistema de DNS utilizar UDP (*Internet User Datagram Protocol*) como protocolo principal de comunicação. Como este protocolo não requer o estabelecimento de uma sessão entre o cliente e o servidor e não possui métodos de autenticação, fica facilitada a ação de forjar a origem de uma consulta DNS.

A Figura 1 apresenta graficamente o fluxo dos ataques de negação de serviço envolvendo o abuso de servidores DNS recursivos abertos, que consiste nos seguintes passos:

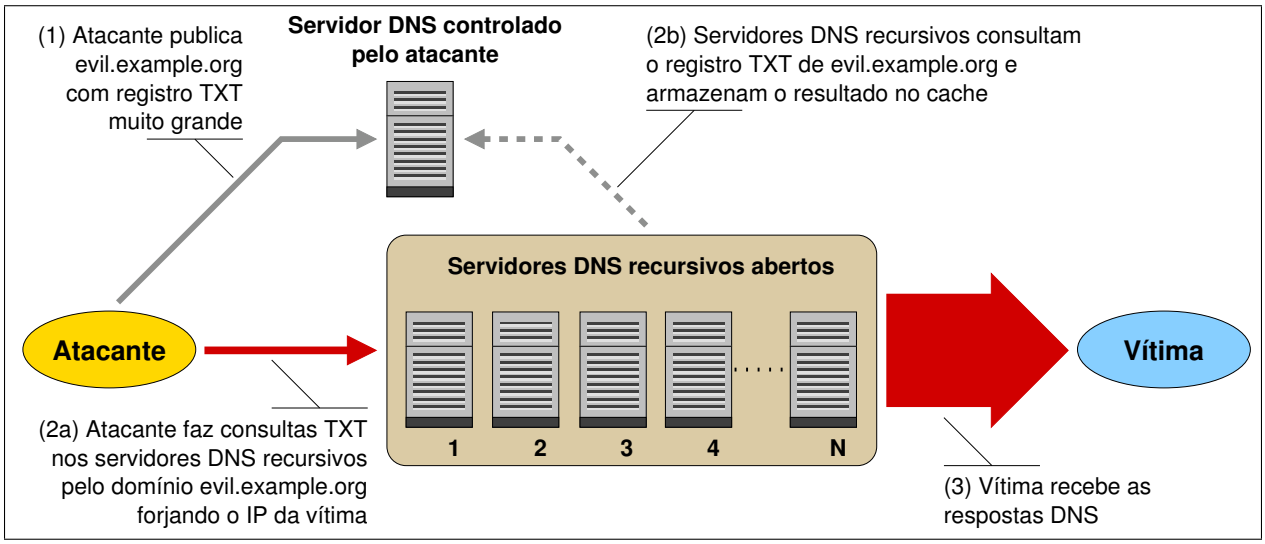

Figura 1: Visão geral do ataque de negação de serviço utilizando servidores DNS recursivos abertos.

1. O atacante publica um registro muito grande, em geral TXT, em um servidor DNS sob seu controle (muitas vezes esse pode ser um servidor previamente comprometido pelo atacante).

2. O atacante, de posse de uma lista de servidores DNS recursivos abertos, envia a estes servidores centenas ou milhares de consultas pelo registro publicado no passo 1, forjando o endereço IP da vítima, ou seja, colocando o endereço IP da vítima como endereço de origem da consulta (2a). Deste modo, o atacante faz com que as respostas sejam enviadas para a vítima e não para a máquina que fez as consultas. Na primeira consulta recebida por um servidor recursivo, este vai buscar a resposta no servidor controlado pelo atacante (2b), nas demais consultas a resposta será enviada diretamente do *cache* do servidor recursivo aberto.
   Em diversos casos documentados as consultas feitas à lista de servidores abertos foram realizadas por uma grande quantidade de *bots*, o que em geral aumenta ainda mais o volume de tráfego sendo enviado para a vítima.

3. A vítima recebe as respostas DNS, que costumam gerar uma amplificação de aproximadamente 10 a 80 vezes o tráfego inicial de consultas, pois, para uma consulta média de aproximadamente 50 bytes, podem ser retornados cerca de 4.000 bytes de resposta para a vítima.

7 Referências

Segue uma lista de documentos que foram utilizados como referência para a produção deste documento. Recomendamos a sua leitura como modo de complementar os conceitos aqui tratados.

- Práticas de Segurança para Administradores de Redes Internet Versão 1.2, Seção 4.5: DNS
  http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#subsec4.5
- *SSAC Advisory SAC008 DNS Distributed Denial of Service (DDoS) Attacks*
  http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf
- *The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0)*
  http://www.uscert.gov/reading_room/DNS-recursion033006.pdf
- *Anatomy of Recent DNS Reflector Attacks from the Victim and Reflector Point of View*
  http://www.verisign.com/static/037903.pdf
- *Measurement Factory - DNS Survey: Open Resolvers*
  http://dns.measurement-factory.com/surveys/openresolvers.html
- *Secure BIND Template*
  http://www.cymru.com/Documents/secure-bind-template.html
- *OpenBSD example file for a simple named configuration*
  http://www.openbsd.org/cgi-bin/cvsweb/~checkout~/src/etc/bind/named-simple.conf
- *OpenBSD example file for a named configuration with dual views*
  http://www.openbsd.org/cgi-bin/cvsweb/~checkout~/src/etc/bind/named-dual.conf
- *Mac OS X Server Network Services Administration – for Version 10.3 or Later*
  http://www.apple.com/server/pdfs/Network_Services.pdf
- *Mac OS X Server Command-Line Administration – for Version 10.3 or Later*
  http://www.apple.com/server/pdfs/Command_Line.pdf
- *BIND 9 Administrator Reference Manual*
  http://www.isc.org/sw/bind/arm93/

8 Agradecimentos

Gostaríamos de agradecer a André Gerhard, Aritana Pinheiro Falconi, Frederico Neves, Luiz Eduardo R. Cordeiro, Marcelo Chaves, Miriam von Zuben, Oripide Cilento Filho, Ricardo Patara e Sandro Süffert pela revisão e por sugestões para o desenvolvimento deste documento. Também gostaríamos de agradecer a Marcelo Chaves pelo desenvolvimento da Figura 1.

9 Histórico de Revisões

Versão 1.0 Versão Inicial, 07/02/2007

Versão 1.1 Complementadas as seções “Configuração Usando *Views*”, “Microsoft DNS”, “Testando seus Servidores” e “Comentários Adicionais”, 16/02/2007