O que é DNS (e DNSSEC)

13 de outubro de 2007, 01:15

Para que você visite um site ou envie um e-mail, um servidor DNS antes assegura se você bate na porta certa. O DNSSEC vem trazer mais segurança.

Por Ricardo Vaz Monteiro

Quando você visita um site através do seu navegador ou quando envia um email, a internet precisa saber em qual servidor o site e o e-mail estão armazenados para poder responder à sua solicitação. A informação da localização destes servidores está em um servidor chamado DNS (Domain Name Server).

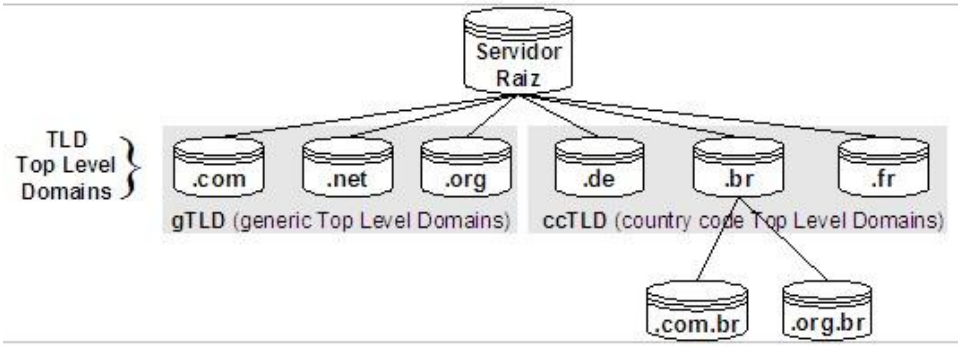
Cada domínio possui um registro no DNS que define qual o endereço IP do servidor de hospedagem e o IP do servidor de e-mail que responderão por este domínio. O processo para a descoberta dos servidores que respondem por um domínio é denominado ?resolução do nome? ou ?resolução do domínio?.

O navegadores e os sistemas clientes de e-mail solicitam que a internet faça a resolução do domínio para apresentar um site, ou enviar um e-mail. Esse processo é totalmente transparente para o usuário, que apenas digita o site que quer visitar e o navegador descobre em qual servidor o site está hospedado e em seguida solicita para o servidor de hospedagem que envie a página inicial.

Por segurança, um domínio pode definir vários servidores DNS. O DNS primário é o primeiro sistema a ser consultado no momento da resolução do nome, caso o servidor DNS primário esteja em manutenção, o servidor DNS secundário é consultado, e assim sucessivamente.

Devido ao intenso tráfego da internet e devido à segurança da rede, a estrutura do banco de dados DNS é distribuída e hierárquica. Ou seja, ao invés de um banco de dados central e único com informações de todos os domínios, a resolução ocorre consultando-se diversos servidores DNS e sua resolução é hierárquica (um servidor DNS pode apontar para outro servidor DNS e assim sucessivamente).

A estrutura hierárquica equivale a uma árvore invertida, ou seja, existe um servidor principal que aponta para um secundário que aponta para um terceiro e assim sucessivamente. O servidor DNS que está no topo da internet é o servidor raiz.



Servidor raiz

O servidor raiz da Internet possui uma tabela que indica qual DNS será responsável pela resolução dos domínios para cada extensão de domínio (Top Level Domain) diferente.

A tabela em si é muito pequena, possui apenas uma entrada para cada Top Level Domain existente. Os Top Level Domains são de dois tipos: gTLDs (Generic Top Level Domains – domínios genéricos usados no mundo todo) e ccTLDs (Country Code Top Level Domains – extensões de domínios administrados pelos países).

Por exemplo: todos os domínios terminados em .com serão respondidos pelos servidores da VeriSign; os domínios .br serão respondidos pelos servidores do Registro.br e assim sucessivamente. Cada gTLD ou ccTLD tem apenas uma entrada neste banco de dados.

Por segurança, o servidor raiz foi replicado em 13 servidores raízes diferentes espalhados pelo mundo e duas vezes ao dia seu conteúdo é automaticamente replicado.

Foi convencionado que cada servidor raiz seria chamado por uma letra do alfabeto (Servidor A, Servidor B etc…). Mesmo um determinado servidor raiz, o servidor raiz A, por exemplo, pode ser replicado em várias regiões do mundo, para assegurar que o tempo para a resolução de um domínio seja rápido (baixa latência).

Bem, então na verdade existem treze servidores raiz principais e dezenas de cópias espalhadas pelo mundo. Veja na imagem abaixo a plotagem dos servidores raizes e suas cópias em funcionamento no mundo.

Os grandes provedores de acesso e empresas de telecomunicações arquivam em seus caches (memória temporária) a tabela dos servidores raiz. Portanto, a cada e-mail enviado ou site visitado os servidores raiz não são obrigatoriamente consultados.

Na verdade, o volume de consultas a estes servidores é muito pequeno, já que sua tabela é alterada apenas quando um novo top level domain é criado. Quem realmente processa o

maior volume de queries para resolução de nomes são os servidores dos TLDs (Top Level Domains).

Por exemplo: um servidor raiz normalmente recebe 500 queries por dia e os servidores da VeriSign (responsável pela resolução dos domínios .com) recebem bilhões de queries diariamente.

DNSSEC

A estrutura hierárquica de resolução de nomes, onde um DNS aponta para outro DNS, possui um problema intrínseco de segurança. Imagine a hipótese que um provedor de acesso capture uma *querie* para resolução de um nome e inadvertidamente responda com um endereço errado de onde o site esteja hospedado. Neste exemplo, você poderia solicitar no seu navegador o endereço www.itau.com.br e o provedor fornecer por erro www.brasdeco.com.br, ou pior, um site *phishing*, que simula o site do banco Itaú.

Um dos maiores problemas desta hipótese é que realmente seria impossível identificar que o provedor de acesso fez isso. Portanto, para dar segurança a estrutura de resolução de nomes a IETF (Internet Engineering Task Force) criou uma extensão do uso atual do DNS denominado DNSSEC.

A extensão DNSSEC autentica as informações do DNS e garante que estas informações são autênticas e íntegras. Sua adoção depende de cada Top Level Domain. O Registro.br, responsável pela administração dos domínios .br já começou a permitir o registro de domínios com o DNSSEC para algumas extensões como .blog.br, .eng.br etc.

O mercado aguarda a liberação do uso do DNSSEC para a extensão .com.br, de longe a mais utilizada no país. O mercado bancário e financeiro devem ser os primeiros a aderir ao DNSSEC e devem solicitar para que as empresas responsáveis pela sua hospedagem façam esta implementação extra de segurança. **[WebInsider]**