



Resumo Técnico F5

DNSSEC: O Antídoto para Envenenamento e Outros Ataques ao DNS

O Sistema de Nomes de Domínios (DNS) fornece uma das funções mais fundamentais da Internet. Se o DNS não estiver funcionando, provavelmente sua empresa também não funcionará. Proteja sua empresa e sua presença na Web com as Extensões de Segurança ao Sistema de Nomes de Domínios (DNSSEC).

por Peter Silva

Gerente Técnico de Marketing

Com contribuições de

Nathan Meyer, Gerente de Produto, e Michael Falkenrath, Engenheiro Sênior de Sistema de Campo



Índice

Introdução	3
<hr/>	
Desafios	4
O DNS solto no mundo: Coisas ruins podem acontecer	4
Domando o Mundo	5
<hr/>	
Soluções	6
BIG-IP v10.1 e DNSSEC: As chaves para o sucesso	6
<hr/>	
Conclusão	9
Recursos	10



Introdução

Nós, humanos, sempre tivemos dificuldade em lembrar sequências de números. Em 1956, George Miller realizou pesquisas sobre a capacidade de se lembrar de números e descobriu que os humanos são capazes de guardar sete itens na memória, com uma variação de mais ou menos dois.¹ Ele concluiu que mesmo quando se oferecem mais informações, a memória humana é capaz de lembrar de cinco a nove blocos de informações. A maioria das pessoas tem um vocabulário de 10.000 a 30.000 palavras e alguns sugerem que 500 a 1.000 delas sejam nomes. Há uma longa tradição de se trocar números por letras, principalmente nos sistemas de telefone, que ganhou muita força com o surgimento das mensagens SMS pelo celulares.

Não é surpresa que, com a invenção da Internet, com todos seus endereços numéricos de Protocolo de Internet, os humanos precisassem de um meio de traduzir esses números em nomes mais compreensíveis. O Sistema de Nomes de Domínios (DNS) foi criado em 1983 para permitir que nós, humanos, fôssemos capazes de identificar pelo nome todos os computadores, serviços e recursos conectados à Internet. O DNS traduz nomes legíveis para os humanos em informações binárias exclusivas para os dispositivos, para que os usuários de Internet sejam capazes de encontrar as máquinas que quiserem. Pense nele como a lista telefônica da Internet.

Agora, o que aconteceria se alguém trocasse o nome da sua empresa, colocando no lugar o nome dele? A lista telefônica relacionaria "O. Crápula", um impostor que receberia todas as ligações destinadas a você e controlaria seu número. Ou, que tal se alguém excluísse todas as referências a você e ninguém mais pudesse encontrá-lo? Isso com certeza afetaria seus negócios. E se a mesma situação acontecesse com o nome do domínio ligado ao seu site público? E se fosse um site de comércio eletrônico! Ou seus clientes não poderiam encontrá-lo de forma alguma ou eles seriam redirecionados a outro site que poderia parecer exatamente igual ao seu, mas que na verdade era o site do O. Crápula. O. Crápula ficaria feliz em tomar todos os seus pedidos e pagamentos, deixando você sem receita, paralisado ou com todas as outras miríades de problemas que surgem quando uma propriedade na Web é sequestrada.

Segurança não foi um item incluído no planejamento original do DNS, já que na época o principal problema era a capacidade de se expandir, e não o comportamento mal-intencionado. Muitos acreditam que proteger o DNS seria de imensa ajuda para proteger a Internet como um todo. A Extensão de Segurança do Sistema de Nomes de Domínios (DNSSEC) pretende acrescentar segurança ao DNS sem perder a compatibilidade com o sistema antigo para poder crescer junto com a Internet. Em essência, o DNSSEC adiciona uma assinatura digital para garantir a autenticidade de certos tipos de transação com o DNS e, dessa forma, garantir a integridade da informação.



O DNSSEC fornece:

- Autenticação de origem dos dados do DNS.
- Integridade dos dados.
- Negação de existência autenticada.

Desafios

O DNS solto no mundo: Coisas ruins podem acontecer

O DNS fez um excelente trabalho desde seus primórdios, porém, como ocorre com tudo mais na Internet, pessoas mal-intencionadas descobriram como explorar o protocolo. Um dos modos é chamado de envenenamento do cache do DNS. Quando você digita uma URL no navegador, um solucionador de DNS verifica na Internet o nome/número correto da transação e localização. Geralmente, o DNS aceitará a primeira resposta ou responderá sem perguntar e enviará você ao site. Ele também guardará essa informação por um período até que ela expire, assim da próxima vez que o nome/número for requisitado, o site é fornecido imediatamente. O DNS não precisa consultar a Internet novamente e usa o endereço até ele expirar. Como os usuários supõem que estão obtendo a informação correta, a situação pode ficar crítica quando um sistema malicioso responde à primeira consulta do DNS com uma informação falsa, modificada, e assim tem-se o envenenamento do DNS. Os servidores de DNS primeiro enviam o usuário ao link errado, mas também guardam a informação falsa até ela expirar. Não é apenas um computador que é enviado ao lugar errado; se o servidor malicioso estiver respondendo ao serviço de um provedor, milhares de usuários podem ser enviados ao sistema desonesto. Isso pode durar horas ou dias, dependendo de quanto tempo o servidor armazena a informação, e todos os outros servidores de DNS que propagam a informação também são afetados. O perigo iminente oferecido por um site desonesto inclui o fornecimento de um malware, a perpetração de fraudes e o roubo de informações pessoais ou sigilosas.

Em 2009, o principal arquivo de DNS de Porto Rico sofreu um ataque². As versões locais dos sites da Google, Microsoft, Coca-Cola, Yahoo e outros como PayPal, Nike e Dell foram redirecionados para sites desfigurados ou em branco que diziam que o site requisitado havia sido alvo de hackers. Nesse incidente, os usuários estavam cientes de que eles não estavam visitando o site real, já que o grupo que se dizia responsável se fez notar. Em um incidente mais sinistro, um dos maiores bancos brasileiros sofreu um ataque que redirecionava os usuários a um site malicioso, o qual tentava instalar um malware para roubar as senhas. Nesse caso, os usuários não estavam cientes de que estavam em um site falso, já que a página fornecida se parecia exatamente com a original. Esses tipos de ataque são muito difíceis de detectar, pois os usuários digitaram o nome correto do domínio no navegador.



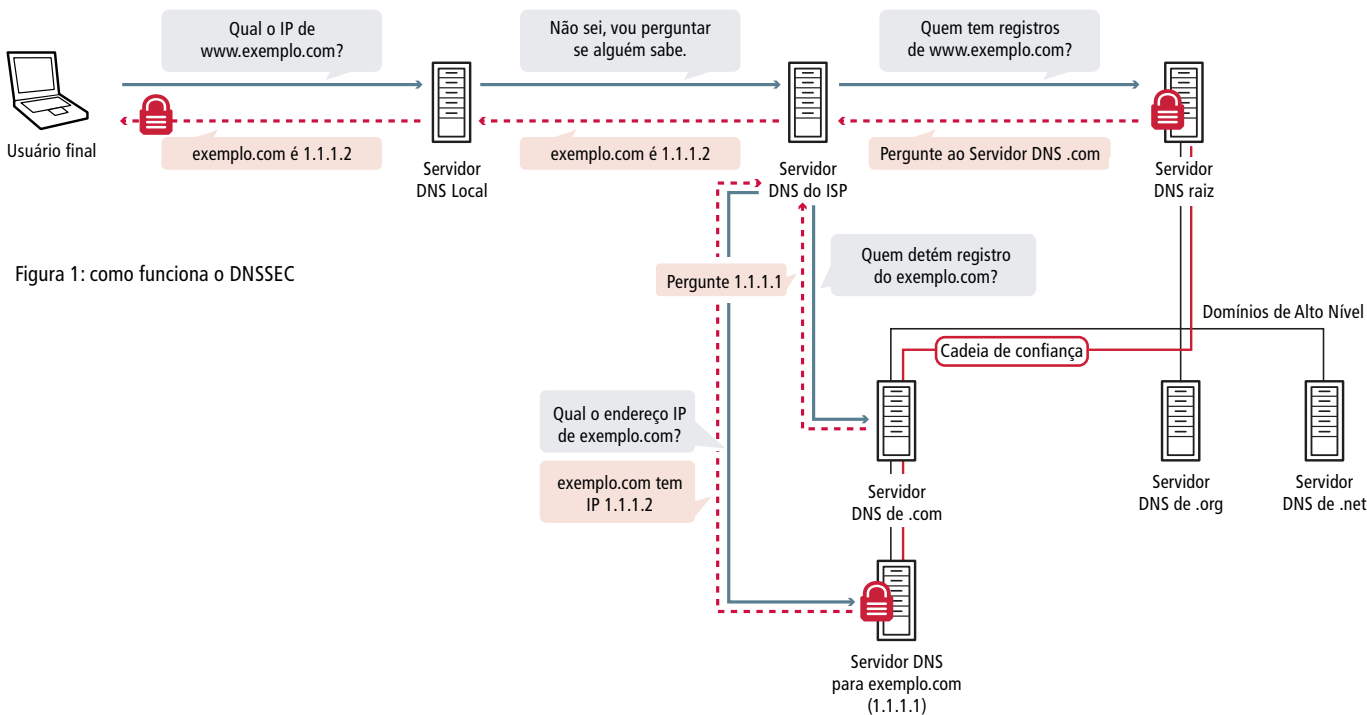
Domando o Mundo

O DNSSEC é uma série de extensões ao protocolo do DNS, definidos nas Requisições de Comentários (RFCs) 4033, 4034 e 4035, que asseguram a integridade dos dados retornados pelas consultas de nome de domínio ao incorporar uma cadeia de confiança na hierarquia de DNS. A cadeia é construída usando-se uma infraestrutura de chave pública (PKI), com cada elo na cadeia consistindo em um par de chaves pública e privada. O DNSSEC não criptografa nem fornece sigilo aos dados, mas os autentica.

O DNSSEC faz o seguinte:

- Autenticação da origem dos dados do DNS: Os solucionadores podem verificar se o dado se originou em um serviço confiável.
- Integridade dos dados: Os solucionadores podem verificar se a resposta não foi adulterada durante o envio.
- Negação de existência autenticada: Quando não houver resposta à consulta, os servidores confiáveis podem fornecer provas de que não há dados.

Implementar um DNSSEC implica autenticar zonas com criptografia pública/privada e devolver as respostas do DNS com assinaturas. (Veja a figura 1.) Um cliente confia que essas assinaturas são baseadas em uma cadeia de confiança estabelecida além das fronteiras administrativas, de zonas pai para zonas filhas, usando uma nova DNSKEY e registros de recursos com autenticador de delegação (DS). Uma implementação de DNSSEC precisa gerenciar as chaves criptográficas: geração de múltiplas chaves, autenticação de zoneamento, troca de chave, revisão e temporização de chaves e recuperação de chaves comprometidas.





Para aplicar o DNSSEC:

1. Cada zona DNSSEC cria um ou mais pares de chaves públicas/privadas com a parte pública colocada em DNSKEY tipo de registro DNSSEC.
2. As zonas autenticam todos os conjuntos de registros de recursos (RRsets) e definem a ordem pela qual múltiplos registros do mesmo tipo são devolvidos com a(s) chave(s) privada(s).
3. Os solucionadores usam a DNSKEY(s) para verificar os RRsets. Cada RRset também tem uma assinatura anexada chamada de RRSIG.

Se o solucionador tem a DNSKEY(s) da zona, ele pode verificar se os RRsets estão intactos verificando suas RRSIGs. A cadeia de confiança é importante ao DNSSEC, já que uma cadeia ininterrupta de confiança precisa ser estabelecida da raiz ao topo, dos domínios de alto nível (TLD) descendo até os registradores individuais. Todas as zonas precisam ser autenticadas por "assinatura", na qual quem publica a zona autentica a zona antes da publicação e a zona paterna publica as chaves para aquela zona. Com muitas zonas, é provável que as assinaturas expirem antes que os registros do DNS sejam atualizados. Portanto, os operadores da zona precisam de meios para reautenticar automaticamente os registros do DNS antes que a assinatura expire. Essa funcionalidade é chamada de "autenticação contínua" ou "revisão automática de chave" e ainda não é encontrada em implementações comuns de servidor de nomes.

Soluções

BIG-IP v10.1 e DNSSEC: As chaves para o sucesso

O F5® BIG-IP® v10.1 suporta o DNSSEC como recurso adicional ao BIG-IP® Global Traffic Manager™ (disponível como serviço individual ou como módulo no BIG-IP® Local Traffic Manager™). O BIG-IP Global Traffic Manager (GTM) oferece alta disponibilidade, desempenho máximo e gerenciamento centralizado para aplicações executadas entre vários data centers espalhados pelo mundo. O BIG-IP GTM distribui as requisições dos usuários finais das aplicações de acordo com as políticas corporativas, as capacidades dos data centers e as condições da rede, para garantir a maior disponibilidade possível. O recurso DNSSEC no BIG-IP GTM autentica as respostas de DNS em tempo real e fornece os meios de implementar o DNSSEC com rapidez e facilidade em um ambiente existente.



Se um cliente requer um site que está atrás do dispositivo BIG-IP mas não requer uma resposta autenticada, o recurso DNSSEC no BIG-IP GTM não faz nada e o BIG-IP GTM responde normalmente – passando pelo dispositivo BIG-IP o endereço IP virtual ao pool de servidores DNS e retornando diretamente ao cliente. Quando a autenticação for solicitada, o recurso DNSSEC no BIG-IP GTM intercepta e autentica a resposta antes de enviá-la ao computador cliente. (Veja a figura 2.) Dessa vez, a solicitação DNSSEC passa através do BIG-IP GTM para os servidores DNS. Quando a resposta é devolvida, o BIG-IP GTM autentica a resposta em tempo real para garantir a assinatura contínua. Um possível agressor não tem como forjar essa resposta sem a chave privada correspondente. A comunicação interna entre o BIG-IP GTM e o DNS server está normal e a comunicação externa do cliente está segura.



Figura 2: Interação do recurso DNSSEC no BIG-IP GTM

Essa autenticação em tempo real é fundamental nos ambientes de conteúdo dinâmico, nos quais tanto os objetos quanto os usuários podem estar vindo de vários locais ao redor do mundo. Outros dispositivos alegam fornecer DNSSEC para DNS estáticos e estarem em conformidade com os DNSSEC em geral, mas nenhum deles tem uma boa solução para o conteúdo dinâmico e nenhum até agora apresentou qualquer solução para as respostas de DNS do tipo de balanceamento de carga do servidor global (GSLB) nas quais o IP respondido pode mudar conforme o cliente que pergunta. Como o GSLB pode fornecer diferentes respostas a clientes diferentes para o mesmo nome de domínio inteiramente qualificado (FQDN), o GSLB e o DNSSEC estão basicamente em conflito com as especificações planejadas originalmente. O DNSSEC, como concebido originalmente, se concentrou somente no DNS estático tradicional e nunca considerou as exigências do GSLB ou o DNS inteligente. É relativamente simples usar BIND para fornecer DNSSEC ao DNS estático. É mais difícil fornecer DNSSEC para DNS dinâmico e há uma grande dificuldade em fornecer DNSSEC às respostas de DNS do tipo GSLB, especialmente em implementações em nuvem. O recurso DNSSEC da F5, de uso geral, fornece DNSSEC cobrindo os três cenários e é simples de implementar e de manter, além de deter baixos custos de manutenção.



A exclusiva solução da F5, em patenteamento, para o problema do DNSSEC em GSLB, o resolve autenticando a resposta no momento em que o dispositivo GSLB decide qual será ela.

Essa é uma solução de DNSSEC em tempo real e, com ela, a F5 é o único fornecedor de GSLB a ter uma solução de DNSSEC funcionando de verdade. Embora outros tenham proposto um sistema no qual todas as possíveis respostas são pré-autenticadas, a maioria concluiu que essa não é uma abordagem viável.

Assumindo que o BIG-IP GTM já esteja implantado, configurado e em funcionamento – incluindo DCs, servidores, escutadores, WIPS, assim por diante – a lista de chave DNSSEC (veja figura 3) é onde os administradores configuram as chaves de autenticação de zonas (ZSKs) e as chaves de autenticação de chave (KSKs). As KSKs são usadas para autenticar outros registros DNSKEY e registros DS, enquanto as ZSKs são usadas para autenticar as RRSIG. É prática nomear as chaves com o nome da zona e/ou com a ZSK ou a KSK no final para facilitar a identificação. A KSK pode ser fortalecida usando mais bits no conteúdo da chave. Isso tem um impacto operacional pequeno, pois ela é usada somente para uma pequena parte dos dados da zona e para verificar o conjunto de chaves da zona, e não para outros RRsets na zona. A KSK deve ser alterada a cada 12 meses, e as ZSK a cada um ou dois meses. Nenhuma interação pai/filho é necessária quando as ZSKs são atualizadas.

As configurações padrões do recurso DNSSEC no BIG-IP GTM seguem as diretrizes do instituto norte-americano de padrões e tecnologia (NIST), fornecendo meios simples e prontos para usar na implementação dessa poderosa solução.

General Properties	
Name	xyz.com_ZSK
Algorithm	RSA/SHA1
Bit Width	1024
Use FIPS	Disabled
Type	Zone Signing Key
State	Zone Signing Key
TTL	86400 seconds
Rollover Period	0 seconds
Expiration Period	0 seconds
Signature Validity Period	604800 seconds
Signature Publication Period	403200 seconds

Figura 3: A GUI do sistema BIG-IP da F5 simplifica e agiliza a configuração e a segurança da sua infraestrutura de DNS.

Como a KSK só é usada para autenticar um conjunto de chaves, que provavelmente são atualizadas com menos frequência do que os outros dados da zona, ela pode ser armazenada separadamente em um local mais seguro do que a ZSK. A KSK pode ter um período de efetividade de chave maior. Na maioria dos métodos de gerenciamento de chave e autenticação de zona, a KSK é usada com menos frequência do que a ZSK. Assim que um conjunto de chaves é autenticado com a KSK, todas as chaves no conjunto podem ser usadas como ZSKs. Se uma ZSK for comprometida, ela pode ser simplesmente retirada do conjunto e um novo conjunto é então reautenticado com a KSK.



Se uma KSK for derrubada, haverá interações com outras partes além do administrador da zona. Isso pode incluir o registro na zona paterna ou administradores verificando os solucionadores que tenham a chave envolvida configurada como pontos seguros de entrada. Portanto, o período de efetividade da chave pode e deve ser bem mais longo.

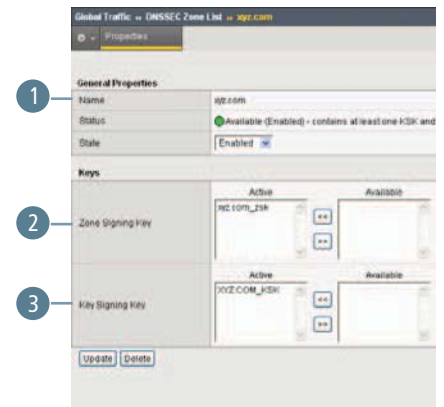
A chave pública permite que um cliente valide a integridade de algo autenticado com a chave privada e o uso do hash permite ao cliente confirmar se o conteúdo não foi adulterado. Como a chave privada do par de chaves pública/privada pode ser usada para representar um autenticador válido, é fundamental mantê-la em segurança. A F5 emprega duas técnicas destacadas no setor para realizar essa tarefa de segurança. Primeiro, para as requisições não-FIPS, a F5 emprega o Secure Vault, um sistema de armazenagem super seguro criptografado por SSL usado nos dispositivos BIG-IP. Mesmo se o disco rígido for removido do sistema e minuciosamente examinado, é quase impossível recuperar o conteúdo do Secure Vault.

Para segurança de nível militar, a F5 suporta a armazenagem FIPS das chaves privadas e esse é um fator exclusivo que o diferencia de muitos outros provedores de DNSSEC no mercado. Também exclusiva da F5 é a habilidade de sincronizar com segurança as chaves entre múltiplos dispositivos FIPS. Além disso, muitos modelos de hardware da F5 (BIG-IP 1500, 3400, 6400, 6800, 8400 e 8800) dão um passo além, utilizando um chip de armazenagem criptografada na placa mãe para proteger uma chave de hardware exclusiva como parte do processo de criptografia em múltiplas camadas.

Conclusão

O DNSSEC garante que a resposta que você recebe quando pede a resolução de um nome veio de um servidor de nomes confiável. Como o DNSSEC está longe de ser implementado globalmente e muitos solucionadores ainda não foram atualizados ou não suportam o DNSSEC, implementar o recurso DNSSEC no BIG-IP GTM pode aumentar enormemente e de modo imediato a segurança do seu DNS. Ele ajuda a cumprir os decretos federais do DNSSEC e ajuda a proteger seus valiosos nome de domínio e propriedades na web contra os servidores desonestos que enviam respostas inválidas.

O BIG-IP V10.1 da F5 agora fornece autenticação DNSSEC para os registros de DNS e autenticação DNSSEC em tempo real conforme solicitado pelos clientes. A combinação de BIG-IP Local Traffic Manager + BIG-IP GTM + DNSSEC em um único produto fornece uma solução de DNSSEC instantânea para as implementações existentes de DNS, dando a você maior controle e segurança sobre a infraestrutura de DNS, além de atender aos decretos do governo norte-americano a respeito da conformidade com o DNSSEC.



Quando criar as zonas DNSSEC, use os mais específicos FQDN no seu nome. O BIG-IP GTM procurará o conjunto e zonas DNSSEC para encontrar o mais específico e o usará como nome, mesmo se houver vários candidatos.

- (1) Nome da zona DNSSEC.
- (2) Escolha a chave de autenticação.
- (3) Escolha a chave de autenticação de chave.

Em vez de desmontar e substituir a infraestrutura atual de DNS, você pode simplesmente colocar o BIG-IP GTM na frente dos seus servidores de DSN e reduzir seus custos de gerenciamento com implementação e manutenção, tudo na mesma appliance.

Recursos

[DNSSEC.net](#)

[DNSSEC Resource Center](#)

[National Institute of Standards and Technology](#)

[Tech Republic](#)

[Public Interest Registry](#)

¹ Miller, G. A. (1956). The magical number seven plus or minus two: Some limitations on our capacity for processing information. *Psychological Review*, 63, 81-97.

² Puerto Rico sites redirected in DNS attack, CNET News, Apr. 27, 2009. ; Cache-poisoning attack snares top Brazilian bank, *The Register*, Apr. 22, 2009.

