O que é um registro DNS SPF?

Registros SPF são um tipo de registo DNS TXT usados geralmente para autenticação de e-mails. Os registros SPF incluem uma lista de endereços de IP e de domínios autorizados a enviar e-mails desse domínio.

Registros DNS

Copiar o link do artigo

O que é um registro DNS SPF?

Um Sender Policy Framework (SPF) é um tipo de registro DNS TXT que lista todos os servidores autorizados a enviar e-mails de um determinado domínio.

Um registro DNS TXT (“texto”) permite que o administrador de um domínio insira um texto aleatório no Domain Name System (DNS). Registros do tipo TXT foram criados inicialmente com o objetivo de incluir avisos importantes relativos ao domínio, mas evoluíram desde então para atender a outras finalidades.

Os registros SPF foram criados originalmente porque o protocolo padrão utilizado para envio de e-mails — o Simple Mail Transfer Protocol (SMTP) — não autentica, por si só, o endereço do "remetente" de um e-mail. Isso significa que sem o SPF ou sem outros registros de autenticação, um invasor pode facilmente se fazer passar por um remetente e enganar o destinatário realizando alguma ação ou compartilhando informações, coisas que de outra forma o destinatário não faria.

Pense no registro SPF como uma lista de convidados controlada por um porteiro. Se o nome de alguém não estiver na lista, o porteiro não o deixará entrar. Da mesma forma, se um registro SPF não possui o endereço de IP de um remetente ou domínio em sua lista, o servidor de recebimento (porteiro) não entregará esses e-mails ou irá marcá-los como spam.

Os registros SPF constituem apenas um dos muitos mecanismos de DNS que podem ajudar os servidores de e-mail a confirmar se um e-mail foi enviado de uma fonte confiável. Domain-based Message Authentication Reporting and Conformance (DMARC) e DomainKeys Identified Mail (DKIM) são dois outros mecanismos utilizados para autenticação de e-mails.

Vale notar que, em determinado momento, os registros SPF tiveram um tipo de registro de DNS dedicado. Desde então, o tipo de registro dedicado foi descontinuado e apenas os registros TXT devem ser utilizados.

Como um servidor de e-mail verifica um registro SPF?

Os servidores de e-mail realizam um processo relativamente simples para verificar um registro SPF:

- O Servidor Um envia um e-mail. Seu endereço de IP é *192.0.2.0* e o return path utilizado pelo e-mail é email@returnpath.com. (Um endereço de return path é diferente do endereço do "de" e é utilizado especificamente para coletar e processar mensagens devolvidas).

- O servidor de e-mail que está recebendo a mensagem (Servidor Dois) usa o domínio do return path recebido e procura por seu registro SPF.

- Se o Servidor Dois encontrar um registro SPF para o domínio do return path, irá procurar o registro SPF do endereço de IP do Servidor Um em sua lista de remetentes autorizados. Se o endereço de IP estiver listado no registro SPF, o SPF é aprovado e o e-mail encaminhado. Se o endereço de IP não estiver listado no registro SPF, o SPF não é aprovado. Nesse caso, o e-mail será recusado ou marcado como spam.

Como é um registro SPF?

Os registros SPF devem seguir determinados padrões para que o servidor entenda como interpretar seu conteúdo. Abaixo um exemplo dos principais componentes de um registro SPF:

```
v=spf1 ip4=192.0.2.0 ip4=192.0.2.1 include:examplesender.email -all
```

Esse exemplo permite que o servidor saiba qual é o tipo do registro, estabelece os endereços de IP aprovados e um terceirizado para este domínio, além de dizer ao servidor o que fazer com os e-mails que não satisfizerem os requisitos. Vejamos como cada componente faz isso:

- `v=spf1` diz ao servidor que isso contém um registro SPF. Todo registro SPF deve começar com essa string.

- Em seguida vem a parte da "lista de convidados" do registro SPF, isto é, a lista de endereços de IP autorizados. Nesse exemplo, o registro SPF está dizendo ao servidor que `ip4=192.0.2.0` e `ip4=192.0.2.1` estão autorizados a enviar e-mails em nome do domínio.

- `include:examplesender.net` é um exemplo da tag "include" (incluir), que diz ao servidor que organizações terceirizadas estão autorizadas a enviar e-mails em nome do domínio. Essa tag indica que o conteúdo do registro SPF para o domínio incluído (examplesender.net) deve ser verificado e que os endereços de IP que este contém também devem ser considerados como autorizados. Vários domínios podem ser incluídos em um registro SPF, mas essa tag só funciona para domínios válidos.

- Por último, `-all` diz ao servidor que os endereços que não estiverem listados no registro SPF não estão autorizados a enviar e-mails e devem ser recusados.

- Outras opções aqui incluem `~all`, que estabelece que os e-mails que não estiverem listados serão marcados como perigosos ou como spam, mas ainda serão aceitos e, mais raramente, `+all`, que significa que qualquer servidor pode enviar e-mails em nome do seu domínio.

Embora o exemplo usado neste artigo seja bem fácil de entender, os registros SPF seguramente podem ser mais complexos. Aqui estão apenas algumas coisas que não se deve esquecer para garantir que os registros SPF sejam válidos:

- Não pode haver mais de um registro SPF associado a um domínio.

- O registro deve terminar com o componente `all` ou incluir um componente `redirect:` (que indica que o registro SPF é hospedado por outro domínio).

- Um registro SPF não pode conter caracteres em letras maiúsculas.

Verifique a documentação oficial do registro SPF para obter mais informações.

Por que são usados registros SPF?

Existem muitos motivos para os operadores de domínio usarem registros SPF:

- **Evitar ataques:** Se os e-mails não forem autenticados, as empresas e destinatários de e-mail correm risco de sofrer ataques de phishing, de e-mail spoofing e de receber e-mails de spam. Com os registros SPF, é mais difícil para os invasores imitar um domínio, reduzindo a probabilidade desses ataques.

- **Melhorar a capacidade de entrega de e-mails:** Domínios sem um registro SPF publicado podem ter seus e-mails devolvidos ou marcados como spam. Com o tempo, e-mails devolvidos ou marcados como spam podem prejudicar a capacidade de um domínio de chegar às caixas de entrada de seu público, comprometendo os esforços de comunicação com clientes, funcionários e outras entidades.

- **conformidade com o DMARC:** DMARC é um sistema de validação de e-mails que ajuda a garantir que os e-mails sejam enviados apenas por usuários autorizados. As políticas DMARC estipulam o que os servidores devem fazer com e-mails que não são aprovados nas verificações de SPF e DKIM. Com base nas instruções da política DMARC, esses e-mails serão marcados como spam, recusados ou enviados normalmente. Os administradores de domínio recebem relatórios sobre as atividades de seu e-mail que os ajudam a ajustar sua política.

O Assistente de Segurança de DNS para E-mail da Cloudflare simplifica a configuração dos registros de DNS TXT corretos e impede os spammers de usarem um domínio. Leia mais sobre o Assistente aqui.

Saiba mais sobre registros de DNS para e-mail:

- Registro DMARC
- Registro DNS DKIM
- Registro DNS MX
- Registro DNS TXT