Jak nastavit Sender Policy Framework (SPF): Kompletní průvodce

dmarcly.com/blog/how-to-set-up-sender-policy-framework-spf-the-complete-guide

31. ledna 2023 SPF

Sender Policy Framework (SPF) hraje důležitou roli v moderní autentizaci e-mailů spolu s DMARC a DKIM. Pomáhá zabránit tomu, aby e-maily od neoprávněných odesílatelů přistávaly do doručené pošty.

V tomto článku vám představíme komplexního průvodce SPF. Probereme různé koncepty SPF, jak to funguje, praktické pokyny k nastavení v typických scénářích a další. Na základě tohoto průvodce SPF budete moci implementovat SPF ve vaší organizaci.

Co je Sender Policy Framework (SPF)

Sender Policy Framework (SPF) je mechanismus pro ověřování e-mailů, který umožňuje odesílat jménem domény pouze autorizovaným odesílatelům a zabraňuje v tom všem neoprávněným

uživatelům. SPF umožňuje přijímajícímu e-mailovému serveru zkontrolovat, zda e-mail, který tvrdí, že pochází z konkrétní domény, skutečně pochází z IP adresy autorizované správcem této domény.

SPF je definován v RFC 7208 a více informací lze nalézt na www.open-spf.org.

Historie SPF

Koncept SPF byl poprvé zmíněn v roce 2000. Později byly IETF Anti-Spam Research Group (ASRG) předloženy návrhy jako „Reverse MX“ (RMX) od Hadmuta Danische a „Designated Mailer Protocol“ (DMP) od Gordona Fecyka. .

V roce 2003 Meng Weng Wong sloučil specifikace RMX a DMP a vytvořil to, co se nakonec stalo SPF.

Na začátku roku 2004 se IETF pokusila použít SPF a návrh CallerID společnosti Microsoft jako základ pro to, co je nyní známé jako Sender ID; ale nikam to nevedlo kvůli technickým a licenčním konfliktům. Komunita se poté vrátila k původní verzi SPF. V roce 2006 byl SPF RFC publikován jako experimentální RFC 4408.

V roce 2014 IETF zveřejnila SPF jako „navrhovaný standard“ v RFC 7208.

Proč SPF

E-mail nebyl navržen jako zabezpečená komunikační platforma – kdokoli může posílat e-maily, které vypadají, že pocházejí z jakékoli konkrétní domény. To umožňuje kyberzločincům podvodně získat citlivé informace příjemce, jako jsou údaje o kreditní kartě a/nebo heslo.

SPF bylo navrženo tak, aby konkrétně řešilo tento problém: když je SPF správně implementováno v doméně, poskytovatel e-mailových služeb kompatibilní s SPF zkontroluje každou příchozí e-mailovou zprávu, aby zjistil, zda pochází ze zadaného seznamu hostitelů, kteří mají povoleno odesílat e-maily jménem domény. doména. Pokud

ano, e-mail je označen jako ověřený SPF a přistane ve složce doručené pošty; jinak e-mail podléhá jiným typům kontrol a může skončit v karanténě nebo odmítnut v závislosti na vašem nastavení DMARC.

Výhody SPF

SPF poskytuje mechanismus pro ověřování odesílatelů e-mailů – to zajišťuje, že odesílatelé mimo zadaný seznam povolených nemají povoleno odesílat e-maily pro doménu. To eliminuje širokou škálu podvodných útoků.

Ve zkratce:

- bez SPF: kdokoli může posílat e-maily pro doménu;
- s SPF: pouze hostitelé uvedení na seznamu povolených mohou odesílat e-maily pro doménu.

Co SPF nedělá

V e-mailu jsou 2 typy adres odesílatele: adresa odesílatele obálky a adresa odesílatele záhlaví. SPF pouze ověřuje adresu odesílatele obálky, přičemž hlavička Adresa odesílatele zůstává nezaškrtnutá. DMARC zavádí koncept „zarovnání identifikátorů SPF“ k vyřešení tohoto problému.

Další informace o tomto tématu naleznete v části: Od adres v e-mailu .

SPF se přeruší, když e-mail prochází nepřímým tokem pošty, například když je přeposlán. Protože IP adresa zprostředkujícího hostitele je jiná než IP adresa původního hostitele a nemusí být na seznamu povolených, může u cílového hostitele selhat ověření SPF. Naštěstí tento problém řeší relativně nový protokol nazvaný ARC (Authentated Reced Chain): Co je to ARC (Authentified Recked Chain) . ARC zachová výsledek autentizace SPF a předá jej downstream přeskokům, aby jej mohl hostitel terminálu vyzvednout.

Konečně, SPF postrádá možnosti hlášení/zpětné vazby. To ztěžuje implementaci a údržbu.

SPF VS DKIM VS DMARC

Moderní e-mailová autentizace obvykle zahrnuje kromě SPF také velké hráče včetně DKIM a DMARC. Společně nabízejí kompletní ochranu proti falšování firemních e-mailů, která při správné implementaci minimalizuje rizika e-mailových spoofingových útoků.

DKIM je zkratka pro DomainKeys Identified Mail. Jedná se o metodu ověřování e-mailů navrženou tak, aby detekovala podvržená pole záhlaví a obsah v e-mailech. DKIM umožňuje příjemci zkontrolovat, zda záhlaví a obsah e-mailů nebyly při přenosu změněny. Další informace naleznete v části: Co je DKIM .

DMARC je zkratka pro Domain-based Message Authentication, Reporting & Conformance. Je to způsob, jak zjistit, zda e-mailová zpráva skutečně pochází od odesílatele nebo ne. Staví na SPF a DKIM a přidává možnosti kontroly zarovnání domén a hlášení určeným příjemcům. Další informace naleznete v části: Co je DMARC .

Jak je popsáno výše, SPF, DKIM a DMARC slouží k různým účelům při ověřování e-mailů. Mezitím poskytují úplnou ochranu e-mailu při společné práci. Abych to shrnul: SPF ověřuje odesílatele e-mailů; DKIM zajišťuje, že záhlaví a obsah e-mailů nebyly zmanipulovány; a DMARC ověřuje e-mailové zprávy na základě výsledků ověřování SPF a DKIM.

Zatímco DMARCLY používá všechny SPF, DKIM a DMARC, lze začít částečnou implementací, jako je SPF a DMARC, a poté přejít k úplné implementaci SPF, DKIM a DMARC.

Jak SPF funguje: Vysvětlení SPF

Aby SPF fungovalo, musí administrátor domény spolupracovat s poskytovatelem e-mailových služeb. Na straně administrátora domény zveřejňuje v DNS záznam SPF, který specifikuje whitelist

odesílatelů, tj. kteří hostitelé mohou odesílat jménem této domény; vynucení probíhá na straně poskytovatele e-mailových služeb: pro každý příchozí e-mail načte záznam SPF z DNS a zkontroluje, zda je odesílatel na seznamu.

Zvažte tento scénář:

- doménou vaší firmy je business.com; budete posílat e-maily svým zaměstnancům a zákazníkům z support@business.com ;
- váš hostitel pro doručování e-mailů, který za vás odesílá e-maily, má IP adresu 192.168.0.1;
- nějaký útočník používá hostitele podvodného e-mailu na IP adrese 1.2.3.4, aby se pokusil odeslat falešné e-maily.

Když se služba doručování e-mailů připojí k e-mailovému serveru obsluhujícímu poštovní schránku příjemce:

- e-mailový server extrahuje název domény z obálky z adresy; v tomto případě je to business.com;
- e-mailový server zkontroluje IP adresu připojujícího hostitele, aby zjistil, zda je uvedena v záznamu SPF na business.com publikovaném v DNS. Pokud je IP adresa uvedena, kontrola SPF projde, jinak ne.

Řekněme například, že váš záznam SPF vypadá takto:

```
v=spf1 ip4:192.168.0.1 -all
```

to znamená, že pouze e-maily z IP adresy 192.168.0.1 mohou projít kontrolou SPF, zatímco všechny e-maily z jakékoli jiné IP adresy než 192.168.0.1 selžou. Proto žádný e-mail od podvodného hostitele na IP adrese 1.2.3.4 nikdy neprojde kontrolou SPF.

Představte si SPF záznam jako whitelist legitimních IP adres a pouze když je příchozí e-mail z jedné z IP adres, SPF dává zelenou. Žádný jiný hostitel nemůže odesílat e-maily pomocí vaší domény. Výsledek autentizace SPF se poté použije pro autentizaci DMARC později.

Pokud používáte Gmail, je snadné zjistit, zda kontrola SPF prošla nebo selhala. Jednoduše se přihlaste do webového Gmailu, klikněte na příslušnou zprávu a pomocí funkce „Zobrazit originál“ prozkoumejte podrobnosti e-mailové zprávy. Jeden příklad zprávy je uveden níže:

Original Message

Message ID	<KmX9Uj6PT3KGlm7czJqu8g@ismtpd0007p1sjc2.sendgrid.net>
Created at:	Mon, Mar 18, 2019 at 6:59 PM (Delivered after 2 seconds)
From:	DMARCLY Report <report@dmarcly.com>
To:	"gangcailin@gmail.com" <gangcailin@gmail.com>
Subject:	DMARCLY daily report.
SPF:	PASS with IP 198.21.6.101 Learn more
DKIM:	'PASS' with domain dmarcly.com Learn more
DMARC:	'PASS' Learn more

Ve výše uvedeném příkladu zpráva prošla kontrolou SPF, jak je zvýrazněno.

Co je záznam SPF TXT

Záznam SPF je záznam Sender Policy Framework, typu záznamu prostředku TXT, publikovaný v DNS, v určené doméně. Celým účelem je specifikovat seznam povolených odesílatelů jménem domény.

Všimněte si, že dříve existoval typ záznamu prostředku SPF, ale jeho podpora byla v roce 2014 ukončena. Záznam SPF musí být publikován jako záznam TXT v DNS.

SPF záznam zveřejňuje správce domény a je vynucován poskytovateli e-mailových služeb.

Syntaxe záznamu SPF TXT

Volně řečeno, každý záznam SPF začíná číslem verze `v=spf1`, po které následuje skupina mechanismů s volitelnými kvalifikátory a modifikátory. Mechanismy SPF, kvalifikátory a modifikátory společně umožňují flexibilní způsob definování seznamu IP adres.

SPF mechanismy

Mechanismus je způsob, jak specifikovat rozsah IP adres. Je definováno osm mechanismů:

- `IP4` : Pokud je odesílatel v daném rozsahu adres IPv4, shodu;
- `IP6` : Pokud je odesílatel v daném rozsahu adres IPv6, shodujte se:
- `A` : Pokud má doménové jméno záznam adresy (A nebo AAAA), který lze přeložit na adresu odesílatele, bude se shodovat;
- `MX` : Pokud má doménové jméno záznam MX překládaný na adresu odesílatele, bude se shodovat (tj. pošta přichází od jednoho z hostitelů příchozí pošty domény);
- `PTR` : Pokud je název domény (záznam PTR) pro adresu klienta v dané doméně a tento název domény se překládá na adresu klienta (reverzní DNS potvrzené předáním), shodujte se. Tento mechanismus je zastaralý a neměl by se nadále používat;
- `EXISTS` : Pokud se zadaný název domény překládá na jakoukoli adresu, shodujte se (bez ohledu na adresu, na kterou se překládá). To se používá zřídka. Spolu s jazykem maker SPF nabízí složitější shody, jako jsou dotazy DNSBL;

- `INCLUDE` : Odkazuje na zásady jiné domény. Pokud zásady dané domény projdou, tento mechanismus projde. Pokud však zahrnutá zásada selže, zpracování pokračuje. Chcete-li plně delegovat zásady jiné domény, je nutné použít rozšíření přesměrování;
- `ALL` : Vždy se shoduje; používá se pro výchozí výsledek, jako je -all pro všechny adresy IP, které neodpovídají předchozím mechanismům.

Kvalifikátory SPF

Kvalifikátor specifikuje výsledek vyhodnocení mechanismu. Každý kvalifikátor lze kombinovat s kterýmkoli z výše popsaných mechanismů.

- `+` pro PASS, tj. kontrola SPF projde. To lze vynechat; např. +mx je totéž jako mx;
- `?` pro NEUTRÁLNÍ výsledek interpretovaný jako NONE (žádná politika);
- `~` (tilda) pro SOFTFAIL, pomoc při ladění mezi NEUTRAL a FAIL. Zprávy, které vracejí SOFTFAIL, jsou obvykle přijaty, ale označeny;
- `-` pro FAIL, tj. kontrola SPF selže.

SPF modifikátory

Existují dva široce používané modifikátory:

- `exp=some.example.com` udává název domény se záznamem DNS TXT (interpretovaný pomocí makrojazyka SPF), aby získal vysvětlení výsledků FAIL. Málo používané.
- `redirect=some.example.com` lze použít místo `all` mechanismu k propojení se záznamem zásad jiné domény.
- Modifikátory SPF umožňují budoucí rozšíření rámce.

Všimněte si, že to `redirect` funguje jiným způsobem než `include` :

- `include` je mechanismus, a pokud selže při ověření, bude zkontrolován další mechanismus ve stejném záznamu SPF;
- `redirect` je modifikátor a výsledek je zcela založen na vyhodnocení SPF záznamu zadané domény.

Příklady záznamů SPF

Zde je typický SPF záznam:

```
v=spf1 a mx include:_spf.example.com -all
```

Tento záznam umožňuje následujícím IP adresám odesílat e-maily jménem vaší domény business.com:

- pokud business.com má záznam adresy (A nebo AAAA), který lze vyřešit, je hodnota vyřešená povolena (mechanismus a);
- pokud má business.com záznam MX, který lze vyřešit, je hodnota vyřešená povolena (mechanismus mx);
- jakákoli IP adresa procházející autentizací SPF pomocí záznamu SPF jiné domény na adrese _spf.example.com je povolena (mechanismus include:_spf.example.com); Všimněte si, že pokud používáte služby doručování e-mailů třetích stran, obvykle vás požádají o přidání jejich seznamu SPF do vašeho záznamu SPF pomocí mechanismu zahrnutí. SendGrid vás například požádá o přidání include:sendgrid.net do vašeho záznamu SPF, aby e-mailové zprávy odeslané ze SendGrid prošly ověřením SPF.

Speciální záznam SPF, který zabraňuje odesílání jakéhokoli e-mailu jménem domény, vypadá takto:

```
v=spf1 -all
```

Tento záznam určuje, že žádná IP adresa není oprávněna odesílat e-maily pro doménu.

Záznam SPF byste měli publikovat na doménách, které nemají odesílat žádné e-maily, včetně parkovaných domén. V opačném případě jsou široce otevřeny útokům spoofingu a v konečném

důsledku utrpí zhoršenou pověst domény a doručitelnost e-mailů, pokud se rozhodnete je použít k odesílání e-mailů později.

Pamatujte: musíte uvést všechny IP adresy, které budou posílat e-maily pro vaši firmu; jinak e-maily odeslané z některých IP selžou při ověřování SPF.

Jak vygenerovat/vytvořit SPF záznam

Záznam SPF můžete generovat dvěma způsoby: ručně nebo pomocí nástroje, jako je generátor záznamů SPF od DMARCLY.

Pokud vytvoříte záznam SPF ručně, můžete začít od `v=spf1` části, poté do záznamu přidat všechny legitimní odesílatele ve vašich e-mailových proudech a nakonec `-all` záznam dokončit připojením.

Alternativně můžete k jeho vytvoření použít generátor SPF záznamů DMARCLY. Viz další část.

Generátor/tvůrce SPF záznamů

Pomocí generátoru záznamů SPF jednoduše vyplníte nastavení záznamu, jako legitimní odesílatelé, a stisknete tlačítko Generovat záznam SPF, vygeneruje se vám záznam SPF. To je méně náchylné k chybám a je preferováno.

Vše v jednom průvodce DMARC/DKIM/SPF

Pokud implementujete SPF v širším kontextu včetně DKIM a DMARC, můžete také zvážit použití DMARCLY all-in-one průvodce DMARC/DKIM/SPF. Tento průvodce poskytuje úplné pokyny k tomu, jak implementovat SPF, DKIM a DMARC v řadě, aby byla zajištěna úplná ochrana proti e-mailovému spoofingu.

Podívejte se na to na: Průvodce DMARC/DKIM/SPF .

Jak přidat/publikovat SPF záznam v DNS

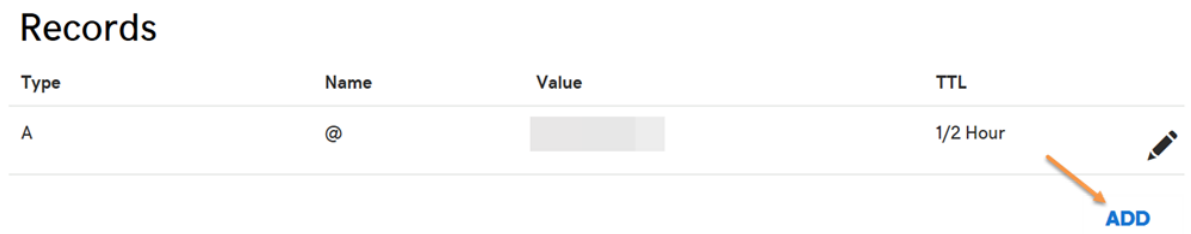
Jakmile vytvoříte záznam SPF, musíte jej publikovat v DNS, než si jej přijímající e-mailový server může vyzvednout. Publikování SPF záznamu je záležitostí vytvoření TXT záznamu na vaší doméně.

Předpokládejme, že používáte GoDaddy jako službu hostování domény. Pokud používáte jinou službu hostování domény, uživatelské rozhraní by mělo být podobné.

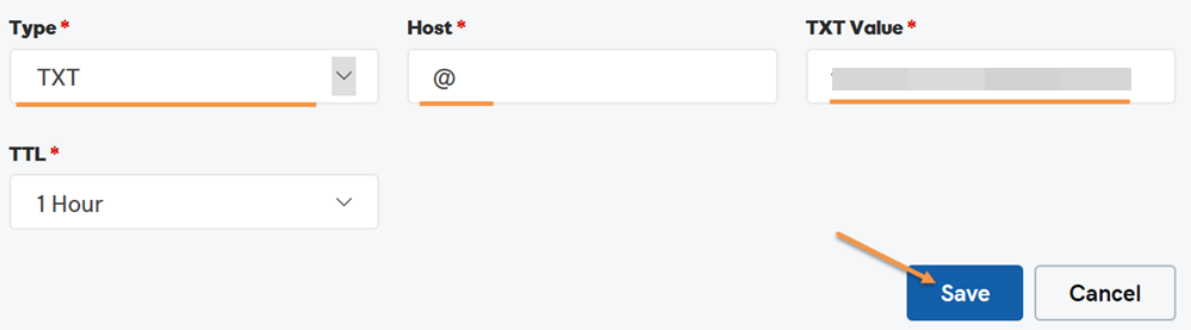
Zde jsou kroky:

- Přihlaste se do GoDaddy. Klikněte na příslušnou doménu a poté klikněte na tlačítko DNS.

- Pokud jste v doméně nikdy nevytvářeli záznam SPF, klikněte v části Záznamy na tlačítko Přidat.



- V opačném případě již máte existující záznam SPF, místo toho jej upravte. Chcete-li zkontrolovat, zda existuje nějaký záznam SPF, zkuste najít záznam TXT s hodnotou začínající na `v=spf1`.
- V rozevírací nabídce Typ vyberte TXT. Do pole Host zadejte @. Zadejte záznam SPF jako hodnotu TXT. Poté klikněte na tlačítko Uložit.



Nyní jste zveřejnili SPF záznam. Všimněte si, že pokud zkontrolujete nově publikovaný záznam SPF, může trvat až 1 hodinu, než se objeví v jakémkoli nástroji, který používáte ke kontrole, kvůli šíření DNS.

Limit vyhledávání DNS SPF

Pokaždé, když e-mailová zpráva zasáhne hostitele e-mailové služby, hostitel vyhledá v DNS a provede kontrolu SPF. Byla věnována pozornost tomu, aby se to nezměnilo v útok DoS (Denial of Service).

Specifikace SPF ukládá, že počet mechanismů a modifikátorů, které provádějí vyhledávání DNS, nesmí překročit deset na kontrolu SPF, včetně všech vyhledávání způsobených použitím mechanismu „include“ nebo modifikátoru „redirect“. Pokud je toto číslo během kontroly překročeno, vrátí se PermError.

Mechanismy `include` , `a` , , a a také modifikátor se do tohoto `mx` limitu započítávají. Mechanismy , , a nevyžadují vyhledávání DNS, a proto se do tohoto limitu nezapočítávají. Modifikátor se do tohoto limitu nezapočítává, protože vyhledávání DNS za účelem načtení řetězce vysvětlení probíhá po vyhodnocení záznamu SPF. `ptr` `exists` `redirect` `all` `ip4` `ip6` `exp`

Podívejme se například na `google.com` záznam SPF:

```
v=spf1 include:_spf.google.com ~all
```

mechanismus `include` v tomto záznamu počítá 1 proti limitu. Další je `_spf.google.com` SPF záznam uživatele:

```
v=spf1 include:_netblocks.google.com
include:_netblocks2.google.com include:_netblocks3.google.com
~all
```

3 `include` mechanismy v tomto záznamu počítají 3 do limitu. Všechny níže uvedené záznamy `_netblocks.google.com` `_netblocks2.google.com` `_netblocks3.google.com` se převádějí na plochý seznam IP adres. Žádný z nich se tedy do limitu nepočítá.

Celkový počet mechanismů a modifikátorů, které provádějí vyhledávání DNS v `google.com` záznamu SPF, je tedy 4 (1+3).

Výše uvedený výsledek kontroly záznamu SPF můžete ověřit pomocí kontroly záznamu SPF na `google.com`.

Jak zkontrolovat/ověřit/otestovat SPF záznam

Občas je potřeba zkontrolovat, zda je váš SPF záznam správně zveřejněn. Stejně jako při vytváření SPF záznamu jej můžete zkontrolovat buď ručně, nebo pomocí DMARCLY's SPF record checker.

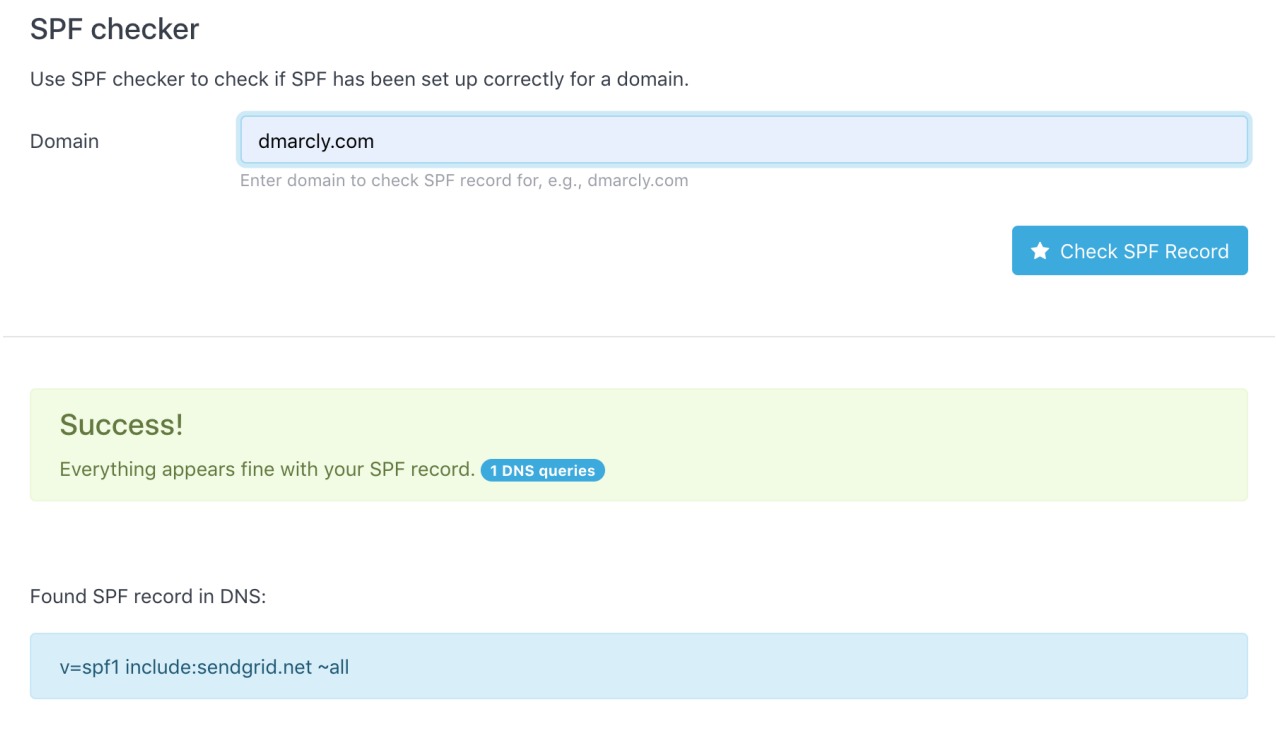
Následující část popisuje, jak používat DMARCLY's SPF record checker ke kontrole vašeho SPF záznamu.

Kontroloři/validátoři/testeři záznamů SPF

Chcete-li zkontrolovat záznam SPF na vaší doméně, přejděte na kontrolu záznamu SPF . Jednoduše zadejte příslušnou doménu a ta načte SPF záznam (pokud existuje) z DNS. Po vrácení záznamu:

- zkontroluje, zda je syntaxe záznamu SPF správná;
- zajišťuje, že počet mechanismů a modifikátorů, které provádějí vyhledávání DNS, nepřesáhne deset;
- "sloučí" vrácený SPF záznam do seznamu obyčejných IP adres, takže je můžete v případě potřeby zkontrolovat jednu po druhé. To je užitečné, když potřebujete vysledovat nějaké drsné problémy SPF.

Zde je příklad kontroly záznamu SPF:



Jak je vidět výše, test záznamu SPF ukazuje, že nastavení SPF na doméně `dmarcly.com` je správné.

Nejčastější dotazy

> Jaký typ záznamu SPF používají někteří poskytovatelé služeb DNS?

Používání typu záznamu prostředku SPF, který byl dříve podporován, bylo ukončeno v roce 2014. Záznamy SPF MUSÍ být nyní publikovány pouze jako **DNS TXT záznam** .

> Mohu mít na své doméně více záznamů SPF?

Neměli byste to dělat. Pokud má doména více záznamů SPF TXT, SPF vrátí PermError.

Více se dozvíte zde: Mohu mít na své doméně více záznamů SPF?