RFC 4408
Epostada Alanların Kullanım Yetkilendirilmesi için Gönderici Politik Çerçevesi (SPF), 1. Sürüm

Yazan: **M. Wong**
Yazan: **W. Schlitt**
Çeviren: **Nilgün Belma Bugüner**

Ekim 2006

Özet

Genel Ağ'da epostaların bazı yollarla sahteleri yapılabilir. Özellikle, SMTP HELO/EHLO komutlarında belirtilen alan veya bir iletinin dönüş yolu olarak kullanılabilen bir gönderici konak ile ilgili olarak mevcut protokollerde bir kısıtlama yer almaz. Bu belge, bir alanın, kendi alan adını kullanmaya izin verdiği konakları açıkça yetkilendirebildiği ve böyle bir yetkilendirmeyi bir alıcı konakla sınayabildiği Gönderici Politik Çerçevesi (Sender Policy Framework – SPF) protokolünün 1. sürümünü açıklar.

Konu Başlıkları

Geçmiş

1.0 İlk çeviri	Ekim 2006	NBB
Deneysel Özgün sürüm	Nisan 2006	MW ve WS

Sürüm Bilgileri

Ağ Çalışma Grubu
Açıklama İsteği: 4408
Durumu: Deneysel

Yasal Uyarı

Bu Belgenin Durumu

Bu belge Genel Ağ topluluğu için bir Deneysel Protokol tanımlar. Bir çeşit Genel Ağ stardardı değildir. Gelişmesi için üzerinde tartışılmasını ve önerilerde bulunulmasını talep edilmektedir. Bu belgenin dağıtımına sınırlama getirilmemiştir.

IESG Notu

Genel bir fikir birliği olmadığından ve iki başarısız yaklaşımı bağdaştırma çabaları nedeniyle RFC 4405, RFC 4406, RFC 4407 ve RFC 4408 aynı anda Deneysel Açıklama İstekleri olarak yayınlanmıştır. Bu sıfatla, bu belgeler tam IETF gözden geçirmesine alınmamış ve MARID çalışma grubunda ele alındıkları halleriyle farklı yaklaşımları belgeleyecek şekilde "OLDUKLARI GİBİ" yayınlanmışlardır.

Hangi yaklaşımın tercih edileceği ve bunların iki kişilik bir araçta kullanımından duyulan endişelerin ve yaklaşımların her biri için tartışmaya açık konulara okuyucunun dikkatinin çekilmesi hususunda IESG taraflardan biri değildir. IESG farklı yaklaşımların belgelenmesinde belgelenmemesinden daha az kötülük olduğuna inanmaktadır.

Gönderici kimliği deneyinin o an ki SPF deneyi için veya bu deneylerin eski sürümleri için oluşturulabilen DNS kayıtlarını kullanabileceğine dikkat ediniz. Kaydın içeriğine bağlı olarak, bu, gönderici kimliği ampiriklerinin iletiye doğru biçimde uygulanamadığı anlamına gelir. Bu ampiriklerle alıcı tarafından bağdaştırılan eylemlere bağlı olarak ileti teslim edilemeyebilir veya alıcıda yok edilebilir.

Gönderici kimliği deneyinin DNS kayıtlarına güvenen tarafları, bu gibi durumlarda geçerli iletilerini kaybedebilecekleri hususunda uyarılır. SPF deneyinin DNS kayıtlarını yayınlayan tarafları ise, RFC 4406'nın 3.4. bölümünde verilen tavsiyeyi değerlendirerek v=spf1 ve spf2.0 kayıtlarının her ikisini de yayınlamayı isteyebilirler.

Gönderici kimliği deneyindeki tarafların, Resent–* başlık alanlarının, standartlara uygun sistemlerle etkileşirken meşru epostayı almada başarısızlıkla sonuçlanacak kullanımı hakkında bilgi sahibi olmaları gerekir (özellikle, Resent–* başlıklarını eklemeyen standartlara uyan özdevinimli sevkediciler ve RFC 2822 Resent–* başlıklarının anlamsallığını henüz gerçeklememiş olup RFC 822'ye razı olan sistemler). Bu birlikte çalışabilirlik sorunlarını çözümlemeksizin Gönderici Kimliğini standartlaşma aşamalarına sokmak uygun olmazdı.

Gelecekte toplulukta bir fikir birliği oluşabileceğinden hareketle, topluluk, yayımı izleyen iki yıl boyunca iki yaklaşımın başarılarını ve başarısızlıklarını gözlemlemeye davet edilmiştir.

1. Giriş

Şu an ki eposta alt yapısı, kendisini istediği bir alan ismiyle tanıtabilen bir posta sistemine herhangi bir konağın posta bırakabilmesi özelliğine sahiptir. Konaklar bunu çeşitli seviyelerde yapabilir: özellikle, oturum, zarf ve posta başlıkları seviyelerinde. Bu özellik bazı durumlarda istenen birşey olduğundan, spamı azaltmada başlıca engeldir. Üstelik, bir çok alan adı sahibi, alan isimlerinin başkaları tarafından rahatça, çoğunlukla kötü niyetle kullanılabilmesinden anlaşılabilir olarak endişelenmektedir.

Bu belge, alan adı sahiplerinin alan adlarının "MAIL FROM" veya "HELO" kimliği olarak kullanımına yetkili konakları belirtebildikleri bir protokol tanımlar. Uyumlu alan sahipleri, alan isimlerini kullanmalarına izin verdikleri konakları belirttikleri SPF kayıtlarını yayınlarlar. Uyumlu posta alıcıları da, bir posta aktarımı sırasında posta aktarım aracısının "HELO" veya "MAIL FROM" komutlarında belirttiği kimlikleri kullanmaya yetkili olup olmadığını bu yayınlanan SPF kayıtlarına bakarak sınar.

Bunun posta alıcılarına ek bir yararı da, kimlik kullanımının doğrulanmasından sonra, yerel önlem kararlarının konağın IP adresinden ziyade göndericinin alan adına dayandırılabilmesidir. Alan isimlerinin reddinin konak IP adreslerinin reddinden daha doğru görünmesinden dolayı bu yararlıdır. Üstelik, eğer talep edilen kimliğin doğrulaması başarısız olursa, böyle bir epostaya karşı alınacak yerel önlem postanın reddedilmesi gibi daha sert bir eylem olabilir.

1.1. Protokolün Durumu

SPF, 2003 yazından beri geliştirilmekte olup, geliştiricilerin 2003 Aralığından beri konuşlandırdıkları görülmektedir. SPF tasarımı 2004 güzüne kadar yavaş yavaş gelişerek kararlı hale geldi. Epeyce SPF biçimi vardır, bir kısmı belgelendirilmiş, bir kısmı Genel Ağ Taslağı olarak yayınlanmış ve geliştirme forumlarında üzerlerinde birçok inceleme ve tartışma yapılmıştır.

Bu belgenin amacı, mevcut gerçeklenimlerde kullanılmış haliyle SPF'nin evvelki taslak belirtimlerine göre tanımlanmış protokolünü temiz ve belirgin olarak belgelemektir. SPF protokolünün bu hali bazan "Klasik SPF" olarak anılır. Belli gerçeklenimlerin ve konuşlandırmaların bu çalışmaya dayanması veya bundan farklı olması anlaşılır bir şeydir. Ancak, SPF sürüm 1'in anlatıldığı gibi algılanacağını umuyoruz.

1.2. Terminoloji

Bu belgenin İngilizce aslında kullanılan "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" ve "OPTIONAL" anahtar sözcükleri yerine çeviride *ZORUNLU*, *ÖNERİ* ve *SEÇİMLİK* imleri kullanılmış olup bunların (hem İngilizce'lerinin hem de Türkçe'lerinin) nasıl yorumlanmaları gerektiği [*RFC2119*]'da açıklanmıştır.

Bu belge bir posta iletisinin "zarf göndericisi", "dönüş yolu", "boş gönderici adresi", "2821 FROM" ve "MAIL FROM" olarak bilinen bölümü ile ilgilidir. Bu terimlerin bazıları iyi tanımlanmadıklarından veya çoğunlukla kazayla kullanıldıklarından, "MAIL FROM" kimliği bu belgenin *MAIL FROM Kimliği* (sayfa: 5) bölümünde açıklanmıştır. "dönüş yolu" gibi üstünkörü olarak bile anlaşılabilen diğer terimler uyulması zorunlu belgelerde tanımlanan anlamlarıyla kullanılmışlardır.

2. İşlem

2.1. HELO Kimliği

"HELO" kimliği ya SMTP HELO ya da EHLO komutundan türetilir (bkz, [*RFC2821*]). Bu komutlar SMTP oturumundaki SMTP istemcisinden (gönderici konak) kaynaklanır. HELO ya da EHLO komutunda sağlanan alan adı ile ilgili gereksinimlerin gönderici taraf açısından her zaman belirgin olmadığına ve SPF istemcilerinin "HELO" kimliğinin bozuk olmasına veya bir IP adres sabiti olmasına hazırlıklı olmaları gerekir. Bu belgenin yazımı sırasında, meşru postaların çoğu hala geçersiz HELO alanları ile teslim ediliyordu.

SPF istemcilerinin sadece "MAIL FROM" kimliğini sınamakla yetinmeyip, ayrıca, `<gönderici>` olarak `check_host()` işlevini (*check_host() İşlevi* (sayfa: 10)) uygulayarak "HELO" kimliğini de sınamaları tavsiye olunur *ÖNERİ*.

2.2. MAIL FROM Kimliği

"MAIL FROM" kimliği ya SMTP MAIL komutundan türetilir (bkz, [*RFC2821*]). Bu komut, bir iletinin, genellikle göndericinin posta kutusundan oluşan ve teslimatla ilgili bir sorun olduğunda teslimat durum bildirimi iletisinin gönderileceği "dönüş yolu"nu sağlar.

[*RFC2821*] dönüş yolunun boş olmasına izin verir (RFC 2821'in Dönüş yolu boş olan iletiler[B12] bölümüne bakınız). Bu durumda belirgin bir posta kutusu yoktur ve böyle bir iletinin posta sisteminin kendisinden kaynaklanan bir bildirim iletisi olduğu varsayılır. Dönüş yolu boş olduğunda, bu belge, "MAIL FROM" kimliğinin "postmaster" yerel kısmından ve "HELO" kimliğinden (evvelce sınanmış olsun olmasın) oluşan bir posta kutusu olacağı varsayılır.

SPF istemcilerinin "MAIL FROM" kimliğini sınamaları gerekir *ZORUNLU*. SPF istemcileri "MAIL FROM" kimliğini `check_host()` işlevini `<gönderici>`yi "MAIL FROM" kimliğine uygulayarak sınarlar.

2.3. Yetkilendirmenin Yayınlanması

Bir SPF uyumlu alanın *SPF Kayıtları* (sayfa: 8) bölümünde açıklandığı gibi geçerli bir SPF kaydı yayınlaması gerekir. Bu kayıt, posta aktarım aracıları tarafından "HELO" ve "MAIL FROM" kimliklerinde alan adını kullanmaya yetkili konakları belirtir.

Eğer alan sahipleri SPF kayıtlarını yayınlamayı tercih ederlerse, bu kayıtların "–all" ile bitmesi veya bunu yapan başka kayıtlara yönlendirilmesi önerilir *ÖNERİ*, böylece yetkilendirmenin tanımsal belirlemesi yapılmış olur.

Alan sahipleri SPF kayıtlarını bu alanı kullanarak asla posta gönderemeyecek konakları belirtmek için de kullanabilirler.

SPF kayıtlarını değiştirirken, tüm meşru postalar sınanıncaya kadar eski kuralın geçerli kalacağı bir geçiş sürecinin olacağı hesaba katılmalıdır.

2.4. Yetkilendirmenin Sınanması

Bir posta alıcısı aldığı her posta iletisi için bir SPF kaydı sınaması yapabilir. Bir SPF sınamasında, konağın belirtilen kimlikle posta bırakmaya yetkili bir istemci olup olmadığına bakılır. Genellikle böyle sınamalar alıcı posta aktarımcısı tarafından yapılır, fakat posta işleme zincirinin, gerekli bilginin elverişli ve güvenilir olduğu başka bir yerinde de yapılabilir. En azından "MAIL FROM" kimliği sınanmalı *ZORUNLU* ve "HELO" kimliği de bunun öncesinde ayrıca sınanmış olmalıdır *ÖNERİ*.

Alan sahibinin açık onayı olmaksızın, SPF'nin 1. sürümü kayıtlara karşın diğer kimliklerin sınanması, yanlış sonuçlar verdiği bilinen durumların varlığı nedeniyle tavsiye edilmez *ÖNERİ*. Örneğin, hemen hemen tüm posta listeleri "MAIL FROM" kimliğini yeniden yazar (bkz, *Postalama Listeleri* (sayfa: 24)), fakat bazıları iletideki diğer kimlikleri değiştirmez. *Yönlendirme Hizmetleri ve Takma Adlar* (sayfa: 24) bölümünde 1.2 şıkkındaki açıklama diğer bir örnektir. Diğer kimlikleri tanımlayan belgeler belirgin bir onay için gereken yöntemi tanımlamalıdır.

SPF sınamalarını gelen posta üzerinde yapılan daha geniş çaplı sınamaların bir parçası olarak kullanmak da mümkündür. Diğer sınamaların sonuçları hangi SPF sınamalarının yapılacağının belirleyicisi olabilir. Örneğin, gönderen konağın IP adresinin yerel aklistede bulunuyor olması tüm diğer sınamaların atlanmasına ve bu konaktan gelen postanın tümünün kabul edilmesine sebep olabilir.

Bir posta alıcısı bir SPF sınaması yapmaya karar verdiğinde, doğru gerçeklenmiş bir `check_host()` işlevini (*check_host() İşlevi* (sayfa: 10)) doğru parametrelerle kullanmalıdır *ZORUNLU*. Sınama bir bütün olarak isteğe bağlı olsa da, bir sınama bir kere uygulanmaya karar verildi mi, belirtildiği gibi uygulanmalı, yani yayıncı ile alıcı arasında doğru anlamsallık korunmalıdır.

Sınamayı yaparken, posta alıcı `check_host()` işlevini işlevin argümanlarına aşağıdaki atamaları yaparak değerlendirmelidir *ZORUNLU*:

`<ip>`
: postayı teslim etmeye çalışan SMTP istemcisinin IP adresi, IPv4 veya IPv6.

`<alan>`

"MAIL FROM" veya "HELO" kimliğinin `alan` kısmı.

`<gönderici>`
"MAIL FROM" veya "HELO" kimliği.

`<alan>` argümanının iyi biçimlenmiş bir alan ismi olmayabileceğine dikkat ediniz. Örneğin, eğer dönüş yolu boşsa, EHLO/HELO alanı kendiyle ilgili sorunlarla birlikte kullanılır (bkz, *HELO Kimliği* (sayfa: 5)). Bu durumlarda, `check_host()` işlevi, *İlk İşlem* (sayfa: 11) bölümünde bir "`None`" sonucu döndürmek üzere tanımlanmıştır.

Bir SPF kaydı olmaması sebebiyle, geçersiz, bozuk ve mevcut olmayan alanlar SPF sınamalarının "`None`" döndürmelerine sebep olsalar bile, hala çoğu MTA'nın önlemi böyle alanlardan gelen epostayı reddetmektir; özellikle, geçersiz "MAIL FROM" durumunda. SPF kayıtlarında bozmadan kaçınma sırasında, eposta reddinin geçersiz alanlardan kaynaklandığı varsayılmalıdır.

Gerçeklenimler, SMTP MAIL FROM komutu ile verilen veriden `<alan>`ı doğru düzgün elde etmek konusunu dikkatle almalıdırlar, çünkü çoğu MTA, güvenlik sistemlerini aşmak için kötü niyetlerle kullanılmakta olan kaynak rotaları ([*RFC2821*]'in Kaynak Rotalar[B20] bölümüne bakınız), yüzde kotarımları [*RFC1123*] ve ünlemli yollar [*RFC1983*] gibi şeyleri hala kabul etmektedir.

2.5. Sonucun Yorumlanması

Bu bölümde yetkilendirme uygulayan yazılımların, `check_host()` işlevinin sonuçlarını nasıl yorumlamaları gerektiği açıklanacaktır. Yetkilendirme sınaması SMTP aktarım işlemi sınasında yapılmalıdır *ÖNERİ*. Bu, hataların gönderen MTA'ya doğrudan doğruya SMTP yanıtları yoluyla dönmesini mümkün kılar.

Yetkilendirmenin SMTP aktarımı bittikten sonra sınanması şu gibi sonuçlara yol açar: (1) aldatıcı olması muhtemel başlıklardan gerekli bilginin kusursuz olarak elde edilmesi zor olabilir; (2) göndericinin yetkilendirme kuralı bu arada değişebileceğinden dolayı meşru eposta reddedilebilir.

Yetkilendirme sınaması başarısız olmuş taklit kimliklerle ilgili teslimatın kabul edilmediğine dair bildirimlerin üretilmesi genellikle istismarcılık olarak görülür ve kimlik sahibinin isteklerine açıkça aykırıdır.

2.5.1. `None`

"`None`" sonucu, alanda yayınlanmış bir kaydın bulunmadığını veya verilen kimlikten sınanabilir bir gönderici alanı saptanamadığını belirtir. Sınama yazılımı, istemci konağın yetkili olup olmadığını araştıramamıştır.

2.5.2. `Neutral`

Alan sahibi, IP adresinin yetkili olup olmadığı konusunda belirleyici olmak istememekte veya belirleyici olamamakta olduğunu belirtmiştir. "`Neutral`" (tarafsız) sonucu, bir "`None`" sonucu gibi ele alınmamalıdır *ZORUNLU*; sadece bilgilendirici amaçlarla bir ayrım mevcuttur. "`Neutral`" sonucunun, bir "`None`" sonucundan daha sertçe ele alınması, alan adı sahiplerini SPF kayıtları kullanımını denemekten vazgeçirirdi (*Gönderici Alanlar* (sayfa: 24) bölümüne bakınız).

2.5.3. `Pass`

"`Pass`" sonucu, istemcinin belirttiği kimlikle posta teslimine yetkili olduğu anlamına gelir. `Alan`, inkar bağlamında, artık, ileti göndermekte yetkili olarak ele alınabilir ve ilgili politik sınamalar kimliğin meşruluğundan emin olarak yapılabilir.

2.5.4. `Fail`

"Fail" sonucu, istemcinin belirttiği kimlikle posta teslimine yetkili olmadığı anlamına gelir. Sınama yazılımı postayı imleyerek kabul edebilir veya derhal reddedebilir.

Eğer sınama yazılımı SMTP aktarımı sırasında postayı reddetmeyi seçerse, bir 550 SMTP yanıt koduyla (bkz, [*RFC2821*]), ek olarak, eğer destekleniyorsa, 5.7.1 Teslimat Durum Bildirimi (DSN) kodlu (bkz, [*RFC3464*]) bir red yanıtı vermelidir *ÖNERİ*. `check_host()` işlevi ya öntanımlı ya da SPF kaydı yayınlamış alanlardan birinin açıklama dizgesini döndürmelidir (bkz, *İzahat (exp)* (sayfa: 18)). Eğer bilgi, sınama yazılımından kaynaklanmıyorsa, göndericinin alanı tarafından sağlanan metin açıkça belirtilmelidir. Örnek:
(Dikkat: Örnek dilimize çevrilmiş olduğundan us–ascii olmayan karakterler içermektedir, dolayısıyla bir SMTP yanıtı olarak uygulanabilir değildir)

```
550-5.7.1 SPF MAIL FROM sınaması başarısız oldu:
550-5.7.1 example.com'un açıklaması için, lütfen:
550-5.7.1 http://www.example.com/posta-politikasi.html
550 5.7.1 adresine bakınız.
```

2.5.5. SoftFail

"SoftFail" sonucu, "Fail" ile "Neutral" arasında kalan bir sonuç gibi ele alınmalıdır. Alan sahibi konağın yetkili olmadığına inanmakta, ama kesin bir beyanattan kaçınmaktadır. Alıcı yazılım sırf bu sonuca bakarak iletiyi reddetmemelidir *ÖNERİ*, fakat normalden daha dikkatli bir incelemeye konu edebilir *SEÇİMLİK*.

"SoftFail" sonucu alındığında, alan sahibinin bu konağı kullanmaktan vazgeçmek istediği ve bu nedenle sınırlı bir geribesleme istediği anlamı çıkarılabilir. Örneğin, alıcının MTA'sı "SoftFail" durumuna dikkat çekebilir veya alıcı MTA göndericiye "grilisteleme" denilen tekniği kullanarak yanıt verebilir; bu teknikte, alıcı MTA bir 451 SMTP yanıt kodu (4.3.0 DSN kodu) ile isteğin alınmış olduğunu ama ikinci bir teslimat denemesinde iletinin kabul edileceğini belirterek postanın ilk teslimatını reddeder.

2.5.6. TempError

"TempError" (geçici hata) sonucu, SPF istemcisinin sınamayı yaparken geçici bir hata saptadığı anlamına gelir. Sınayan yazılım iletiyi ya kabul eder ya da geçici olarak reddeder. Eğer ileti SMTP aktarımı sırasında bu sebeple reddedilmişse, yazılım 451 yanıt kodunu ve destekleniyorsa 4.4.3 DSN kodunu kullanmalıdır *ÖNERİ*.

2.5.7. PermError

"PermError" sonucu, alanın yayınladığı kaydın gerektiği gibi yorumlanamadığı anlamına gelir. Bu sonuç, "TempError" sonucunun aksine, çözümlenmesi için elle müdahalenin gerekli olduğu bir hata durumunu belirtir. Haberiniz olsun, eğer alan sahibi makro kullanıyorsa (bkz, *Makrolar* (sayfa: 20)), bu sonuç sınanan kimliklerin beklenmedik bir biçime sahip olmasından kaynaklanabilir.

3. SPF Kayıtları

Bir SPF kaydı, alan ismini "HELO" ve "MAIL FROM" kimliklerinde kullanmaya yetkili olan ve olmayan konakların bildirildiği bir DNS özkaynak kaydıdır. Tam bu şekilde olmasa da, bu kayıtta yer alan konaklar izin verilenler ve izin verilmeyenler (hiçbir kategoriye girmeyenler) olarak gruplanır, denebilir.

SPF kaydı tek bir dizgeden oluşur. Bir kayıt örneği:

```
v=spf1 +mx a:colo.example.com/28 -all
```

Bu kayıt "spf1" sürümüdür ve 3 yönerge içerir:"+mx", "a:colo.example.com/28" (+ imi örtüktür) ve "–all".

3.1. Yayınlama

SPF uyumlu olmak isteyen alan sahipleri "HELO" ve "MAIL FROM" kimliklerinde kullanılan konaklar için SPF kayıtları yayınlamalıdır. SPF kayıtları DNS ağacında bir alt alan adı altında değil, ilgili oldukları konak ismine, örneğin SRV kayıtlarına yerleştirilir. Bu TXT veya SPF özkaynak kaydı kullanımı ile aynıdır (bkz, *DNS Özkaynak Kaydı Türleri* (sayfa: 9)).

SPF Kayıtları (sayfa: 8) bölümündeki örnek, bir alan bölge dosyası üzerinden şu satırlarla yayınlanabilir:

```
example.com.          TXT "v=spf1 +mx a:colo.example.com/28 -all"
smtp-out.example.com. TXT "v=spf1 a -all"
```

TXT kayıtları üzerinden yayınlarken, başka amaçlarla yayınlanmış başka TXT kayıtlarının varolabileceğine dikkat ediniz. Bunlar boyut sınırlarıyla ilgili sorunlara yol açabilirler (bkz, *Kayıt Uzunluğu* (sayfa: 9)).

3.1.1. DNS Özkaynak Kaydı Türleri

Bu belge 99 koduyla yeni bir DNS RR türü olarak SPF özkaynak kaydını tanımlar. Bu türün biçimi TXT özkaynak kaydı [*RFC1035*] ile aynıdır. Her iki tür için de kaydın karakter içeriği [*US–ASCII*] olarak kodlanır.

Mevcut uygulama (bir TXT kaydı kullanımı) en iyisi olmamakla beraber, henüz yeni özkaynak kaydı türüyle çalışamayan ama hala kullanımda olan pek çok DNS sunucusu ve çözümleyici gerçeklenimi olduğundan bu gereklidir. Bu iki kayıt türlü şema, aynı amaç için ayrılmış bir özkaynak kaydı türünü kullanarak daha iyi bir çözüme geçişin yolunu açar.

Bir SPF uyumlu alan adı her iki özkaynak kaydı türünde de SPF kaydı içermelidir *ÖNERİ*. Bir uyumlu alan adı en az bir türde kayda sahip olmalıdır *ZORUNLU*. Örneğin, *Yayınlama* (sayfa: 8) bölümündeki kayıtlardan biri yerine şu kayıtlar daha iyidir:

```
example.com. IN TXT "v=spf1 +mx a:colo.example.com/28 -all"
example.com. IN SPF "v=spf1 +mx a:colo.example.com/28 -all"
```

Örnek özkaynak kayıtları bu belgede TXT kaydı türünde gösterilmiştir; yine de, bunlar SPF türünde veya her iki türde de yayınlanabilirdi.

3.1.2. Çoklu DNS Kayıtları

Bir alan adı bir yetkilendirme sınamasında bir kayıttan fazlasının seçilmesine sebep olacak şekilde çok sayıda kayda sahip olmamalıdır *ZORUNLU*. Seçim kuralları için *Kayıtların Seçilmesi* (sayfa: 11) bölümüne bakınız.

3.1.3. Tek DNS Kaydında Çok Sayıda Dizge

[*RFC1035*]'in 3.3 ve 3.3.14. bölümlerinde tanımlandığı gibi, tek bir metin DNS kaydı (TXT ve SPF'nin ikisi de) birden fazla dizgeden oluşabilir. Eğer yayınlanan bir kayıt çok sayıda dizge içeriyorsa, bu dizgeler aralarına boşluk konmaksızın birleştirilmiş tek bir kayıt gibi ele alınmalıdır *ZORUNLU*. Örnek:

```
IN TXT "v=spf1 .... ilk" "ikinci dizge..."
```

kaydı ile aşağıdaki kayıt bir diğerinin eşdeğeri olarak ele alınmalıdır *ZORUNLU*:

```
IN TXT "v=spf1 .... ilkikinci dizge..."
```

Çok sayıda dizge içeren TXT ve SPF kayıtları, tek bir kayıtta 255 baytlık azami uzunluğu aşabilecek kayıtları oluşturmak için yararlıdır.

3.1.4. Kayıt Uzunluğu

Belli bir alan isminde yayınlanacak bir SPF kaydı bir sorgunun sonucunda 512 sekizliye sığacak kadar küçük olmalıdır *ÖNERİ*. Bu, eski DNS gerçeklenimlerini TCP'ye toslayıp devrilmekten koruyacaktır. Yanıt uzunluğu bu belgenin kepsamı dışında kalan pek çok şeye bağlı olduğundan, sadece şu söylenebilir: Belirtilen türde (TXT veya SPF) kayıtların tümünün ve DNS isminin toplam uzunluğu 450 karakterin altında kalırsa, DNS yanıtları

UDP paketlerine sığacaktır. TXT biçimi sorgular için boyut hesaplanırken, alan adı altında yayınlanmış diğer TXT kayıtları da hesaba katılmalıdır. Tek bir UDP paketine sığamayacak kadar uzun kayıtlar SPF istemcileri tarafından sessizce yoksayılabilirler *SEÇİMLİK*.

3.1.5. İsim Kalıplı Kayıtlar

Yayınlamak için isim kalıplarının kullanılması önerilmez. Eğer bu tür kayıtlar kullanılmışsa dikkatli olunmalıdır. Eğer bir alan bu tür MX kayıtları yayınlıyorsa, aynı sorunlara ve gereksinimlere konu isim kalıbı bildirimlerini de yayınlarsa iyi olur. Özellikle de öznitelik kayıtlarının bulunduğu her konak ve alt alan adı için bu bildirim yinelenmelidir. Örneğin, [*RFC1034*]'ün 4.3.3. bölümünde verilen örnek şu kayıtlarla genişletilebilirdi:

```
X.COM.          MX      10      A.X.COM
X.COM.          TXT     "v=spf1 a:A.X.COM -all"

*.X.COM.        MX      10      A.X.COM
*.X.COM.        TXT     "v=spf1 a:A.X.COM -all"

A.X.COM.        A       1.2.3.4
A.X.COM.        MX      10      A.X.COM
A.X.COM.        TXT     "v=spf1 a:A.X.COM -all"

*.A.X.COM.      MX      10      A.X.COM
*.A.X.COM.      TXT     "v=spf1 a:A.X.COM -all"
```

Uyarı

SPF kayıtları alan içindeki her isim için iki tane olmalıdır: biri isim için, diğeri isim altındaki ağacı kapsayan bir isim kalıbı için.

İsim kalıplarının kullanımından genellikle vazgeçilir, çünkü bunlar alan altında her ismin bulunmasına ve herhangi bir isme yapılan bir sorgunun asla RCODE 3 (İsim Hatası) döndürmemesine sebep olur.

4. check_host() İşlevi

check_host() işlevi SPF kayıtlarını alır, onları çözümler ve belli bir konağın belirtilen kimlikle posta gönderme izninin olup olmadığını saptamak için onları yorumlar. Bu sınamayı uygulayan posta alıcılarının check_host() işlevini burada açıklandığı gibi doğru olarak değerlendirmeleri gerekir *ZORUNLU*.

Gerçeklenimler, bütün durumlarda sonuçlar aynı kalmak üzere, burada tanımlanmış kurallı algoritmadan farklı bir algoritma kullanabilirler *SEÇİMLİK*.

4.1. Argümanlar

check_host() işlevi şu argümanları alır:

<ip>
: Postayı teslim etmeye çalışan SMTP istemcisinin IP adresi, IPv4 veya IPv6.

<alan>
: Peşinde koşulan yetkilendirme bilgisini sağlayan alan; başlangıç olarak, "MAIL FROM" veya "HELO" kimliğinin alan kısmı.

<gönderici>

"MAIL FROM" veya "HELO" kimliği.

<gönderici>'nin alan kısmı, check_host() ilk olarak değerlendirirken, normal olarak <alan> argümanı ile aynıdır. Bununla birlikte, ardışık değerlendirmeler için bu genellikle doğru olmayacaktır (bkz, *"include"* (sayfa: 14)).

check_host() işlevinin asıl gerçeklenimleri ek argümanlara ihtiyaç duyabilir.

4.2. Sonuçlar

check_host() işlevi *Sonucun Yorumlanması* (sayfa: 7) bölümünde açıklanan çeşitli sonuçlardan birini döndürebilir. Sonuca bağlı olarak, eylem alıcının yerel politikasına göre saptanır.

4.3. İlk İşlem

Eğer <alan> bozuksa (63 karakterden uzun, sonda olmayan sıfır uzunluk, vs.) veya tamamen nitelenmiş alan adı değilse ya da DNS sorgusu "alan mevcut değil" (RCODE 3) diye bir sonuç döndürüyorsa, check_host() işlevi anında "None" sonucunu döndürür.

Eğer <gönderici> bir yerel kısım içermiyorsa, yerel kısmın "postmaster" olduğu varsayılır.

4.4. Kayıt Arama

Kayıtların nasıl yayınlandıklarına bağlı olarak (bkz, *Yayınlama* (sayfa: 8)), TXT, SPF veya her ikisinin de sorgulanması, <alan> için bir DNS sorgusu yapılmasını gerektirir. Eğer sorgu, TXT ve SPF özkaynak kayıtlarının her ikisi için de yapılıyorsa, sorgular aynı anda yapılabilir *SEÇİMLİK*.

Eğer yapılan tüm DNS sorguları bir sunucu başarısızlığı (RCODE 2) veya başka bir hata (RCODE 0 veya 3 dışında) ya da bir zamanaşımı döndürüyorsa, check_host() işlevi anında "TempError" sonucu ile çıkar.

4.5. Kayıtların Seçilmesi

Bir sürüm bölümü ile başlayan kayıtlar:

```
kayıt          = sürüm terimler *BOŞLUK
sürüm          = "v=spf1"
```

Sorgu tarafından döndürülen kayıtlarla başlayarak, kayıt seçimi iki adımda gerçekleşir:

1. Açıkça "v=spf1" şeklinde bir sürüm bölümü ile başlamayan kayıtlar iptal edilir. sürüm bölümünün bir BOŞLUK veya kayıt sonu ile sonlandığına dikkat ediniz. "v=spf10" içeren sürüm bölümlü bir kayıt uygun değildir ve iptal edilmelidir.
2. Küme içinde SPF türünde bir kayıt varsa, TXT türündeki tüm kayıtlar iptal edilir.

Bu adımlardan sonra, kalan tam olarak tek bir kayıt olmalı ve değerlendirme yapılmalıdır. Eğer iki veya daha fazla kayıt kalıyorsa, check_host() işlevi anında "PermError" sonucu ile çıkar.

Hiçbir eşleşen kayıt dönmezse, bir SPF istemcisinin alanın bir SPF bildirimi yapmadığını varsayması gerekir *ZORUNLU*. SPF işlemi durmalı ve "None" dönmelidir *ZORUNLU*.

4.6. Kayıt Değerlendirme

SPF kaydı seçildikten sonra, check_host() işlevi kaydı çözümler ve o an ki sınama için bir sonuç bulmak için yorum yapar. Eğer bir sözdizimi hatası varsa, check_host() işlevi anında "PermError" sonucu ile çıkar.

Gerçeklenimler çözümlemek için önce kaydın tümünü seçebilir ve eğer kayıt sözdizimsel olarak iyi biçimlenmemişse "PermError" döndürebilirler *SEÇİMLİK*. Yine de, tüm durumlarda, kaydın herhangi bir yerinde bir sözdizimi hatası saptanmış olmalıdır *ZORUNLU*.

4.6.1. Terim Değerlendirme

İki tür terim vardır: mekanizmalar ve değiştiriciler. Bir kayıt, (aşağıda ABNF gösterimiyle belirtilmiş olarak) bunların bir listesini içerir.

```
terimler       = *( 1*BOŞLUK ( yönerge / değiştirici ) )

yönerge        = [ niteleyici ] mekanizma
niteleyici     = "+" / "-" / "?" / "~"
mekanizma      = ( tümü / dahili
                   / A / MX / PTR / IP4 / IP6 / mevcut )
değiştirici    = sevket / izahat / bilinmeyen-değiştirici
bilinmeyen-değiştirici = isim "=" makro-dizgesi

isim           = HARF *( HARF / RAKAM / "-" / "_" / "." )
```

Çoğu mekanizma isimden sonra bir ":" veya "/" karakterine izin verir.

Bir değiştirici daima hemen isimden sonra ve bir makro-dizgesinin parçası olabilen bir ":" veya "/" karakterinden önce bir eşit işareti ('**=**') içerir.

Bir "=", ":" veya "/" içermeyen terimler *Mekanizma Tanımları* (sayfa: 13) bölümünde tanımlandığı gibi mekanizmalardır.

[*RFC4234*]'teki ABNF gösterimi tanımına göre mekanizma ve değiştirici isimleri harf büyüklüğüne duyarsızdırlar.

4.6.2. Mekanizmalar

Her mekanizma soldan sağa doğru ele alınır. Bir mekanizma yoksa, sonuç *Öntanımlı Sonuç* (sayfa: 13) bölümünde belirtilmiştir.

Bir mekanizma değerlendirilirken şu üçünden biri oluşur: eşleşebilir, eşleşmeyebilir ya da bir hata oluşur.

Eşleşme olursa, işlem sona erer ve niteleyici değeri bu kaydın sonucu olarak döndürülür. Eşleşme olmazsa, işlem sonraki mekanizma ile devam eder. Bir hata oluşursa, mekanizma işlemi sonlanır ve hata değeri döndürülür.

Olası niteleyiciler ve döndürdükleri sonuçlar:

```
"+" Pass
"-" Fail
"~" SoftFail
"?" Neutral
```

Niteleyici isteğe bağlıdır ve öntanımlı değer "+"dır.

Bir mekanizma eşleşir ve niteleyici "–" (eksi) olursa, "Fail" sonucu döndürülür ve izahat-dizgesi *İzahat (exp)* (sayfa: 18) bölümünde açıklandığı gibi hesaplanır.

Bellibaşlı mekanizmalar *Mekanizma Tanımları* (sayfa: 13) bölümünde açıklanmıştır.

4.6.3. Değiştiriciler

Değiştiricileler birer mekanizma değildirler: bir eşleşme ya da eşleşmeme sonucunu döndürmezler. Ek bilgi sağlarlar. Değiştiricileler kaydın değerlendirmesini doğrudan etkilemeseler de, "redirect" değiştiricisi, tüm mekanizmalar değerlendirildikten sonra etkili olur.

4.7. Öntanımlı Sonuç

Eğer eşleşen bir mekanizma yoksa ve bir "redirect" değiştiricisi de belirtilmemişse, check_host() işlevi son yönerge olarak "?all" belirtilmiş gibi "Neutral" sonucu ile döner. Eğer bir "redirect" değiştiricisi belirtilmişse, check_host() işlevi *Yönlendirilmiş Sorgu (redirect)* (sayfa: 17) bölümünde tanımlandığı gibi işlem yapar.

İşlemin açıkça sonlandırılabilmesi için kayıtların daima ya bir "redirect" değiştiricisi ya da bir "all" mekanizması içermesi gerektiğine *ÖNERİ* dikkat ediniz. Örnek:

```
v=spf1 +mx -all
```

veya

```
v=spf1 +mx redirect=_spf.example.com
```

4.8. Alan Belirtimi

Bu mekanizma ve değiştiricilerin bazılarının bir <alan-belirtimi> bölümü vardır. <alan-belirtimi> dizgesi bir makro oluşumudur (bkz, *Makrolar* (sayfa: 20)). Sonuç dizgesi, tamamen nitelenmiş bir alan adının bilinen gösterim biçimindedir: noktalarla ayrılmış yaftalar dizisi. Bu alana belgenin devamında <hedef-ismi> denilecektir.

Bilgi

Makro yorumlamasının sonucu bir öncelemeye konu değildir. Bu bakımdan, bu oluşum bir DNS yaftasında meşru olan tüm karakterleri üretemez (örn, denetim karakterlerini). Yine de, bu oluşum, DNS'de kullanılan işe yarar yaftaları ("_spf" gibi) ve meşru konak isimlerini ifade etmek için yeterince güçlüdür.

Birçok mekanizma için <alan-belirtimi> isteğe bağlıdır. Sağlanmazsa, <hedef-ismi> olarak <alan> kullanılır.

5. Mekanizma Tanımları

Bu bölümde iki tür mekanizma tanımlanmaktadır.

Temel mekanizmalar dil çerçevesi dahilinde destek verir. Belli bir yetkilendirme şeması türü belirtmezler.

```
tümü
dahili
```

Tasarlanmış gönderici mekanizmaları, posta gönderimi için <alan>'ı kullanmaya izin verilmiş veya verilmemiş bir <ip> adresi kümesini tasarlamakta kullanılır.

```
a
mx
ptr
ip4
ip6
mevcut
```

Aşağıdaki uzlaşımlar <ip> ile herhangi bir noktadaki IP adresi arasında bir karşılaştırma yapacak tüm mekanizmalara uygulanır:

yönergede bir CIDR uzunluğu belirtilmemişse, <ip> ve IP adresi eşitlik için karşılaştırılır. (Burada CIDR, "sınıfsız alanlar arası yönlendirme" anlamına gelen "Classless Inter–Domain Routing" kısaltmasıdır.)

Bir CIDR uzunluğu belirtilmişse, <ip> ve IP adresinin sadece belirtilen sayıda yüksek biti eşitlik için karşılaştırılır.

Bir mekanizma <ip> ile karşılaştırmak için konak adreslerini alırken, <ip> bir IPv4 adresi ise A kayıtlarını alır, bir IPv6 adresi ise AAAA kayıtlarını alır. SMTP bağlantısı IPv6 üzerinden bile olsa, bir IPv4 eşlemli IPv6 adresi ([*RFC3513*]'ün 2.5.5. bölümüne bakınız) yine de bir IPv4 adresi sayılmalıdır *ZORUNLU*.

Birçok mekanizma DNS'den alınan bilgiye bel bağlar. Bu DNS sorguları için, aksi belirtilmedikçe, eğer DNS sunucusu bir hata döndürüyorsa (0 ve 3 dışında bir RCODE) veya sorgu zamanaşımına uğruyorsa, mekanizma "TempError" verir. Eğer sunucu "alan mevcut değil" (RCODE 3) diyorsa, sanki hata alınmamış (RCODE 0) gibi mekanizmanın değerlendirilmesi sürer ve sıfır yanıt kaydedilir.

5.1. "all"

```
tümü            = "all"
```

"all" mekanizması daima eşleşen bir sınamadır. Bir kayıttakı en sağdaki mekanizma açık bir öntanım sağlayacakmış gibi kullanılır.

Örnek:

```
v=spf1 a mx -all
```

"all"dan sonra gelen mekanizmalar asla sınanmaz. Bir "all" mekanizmasi varsa, hiçbir "redirect" değiştiricisinin (*Yönlendirilmiş Sorgu (redirect)* (sayfa: 17)) etkisi yoktur.

5.2. "include"

```
dahili          = "include"  ":" alan-belirtimi
```

"include" mekanizması check_host() işlevinin ardışık değerlendirilmesini tetikler. alan-belirtimi *Makrolar* (sayfa: 20) bölümündeki gibi yorumlanır ve check_host() işlevi, sonuçlanan dizgeyi <alan> olarak değerlendirir. <ip> ve <gönderici> argümanları o an ki check_host() değerlendirmesindekiyle aynı kalır.

Önemine ve niteliğine bakarak, bu mekanizma için "include" ismi yetersiz kalmıştır. Atıf yapılan SPF kaydı ilk kayıtta harfiyen içerilmiş gibi davranılacağı yerde, sadece atıf yapılan SPF kaydının değerlendirilen sonucu kullanılır. Örneğin, atıf yapılan alandaki bir "all" yönergesinin değerlendirilmesi işlemin tamamını sonlandırmaz ve sonucun bir bütün olarak "Fail" olmasını gerekli kılmaz. (Bu mekanizma için "if–pass", "on–pass", vb. bir isim daha uygun olurdu.)

"include" mekanizması, çok sayıda yönetimsel olarak bağımsız alanı tek bir alanda tasarlamayı mümkün kılar. Örneğin, sözde alan "example.net" yönetimsel olarak bağımsız alanlar olan example.com ve example.org sunucularını kullanarak posta gönderebilir.

Example.net şöyle bir kayıt içerirse,

```
IN TXT "v=spf1 include:example.com include:example.org -all"
```

bu kayıt, check_host() işlevini bir "Pass" sonucu için example.com ve example.org'un kayıtlarını sınamaya yöneltir. Sadece, konak bu alanların ikisinde de izinli değilse sonuç "Fail" olurdu.

check_host() işlevinin ardışık değerlendirmesinin sonucunda bu mekanizmanın davranış tarzı:

```
+--------------------------------+--------------------------------+
| Ardışık check_host() sonucunun | "include" mekanizması bunlara  |
| bunlar olması için:            | sebep olmalıdır:               |
+--------------------------------+--------------------------------+
```

```
| Pass                            | eşleşir                         |
|                                 |                                 |
| Fail                            | eşleşmez                        |
|                                 |                                 |
| SoftFail                        | eşleşmez                        |
|                                 |                                 |
| Neutral                         | eşleşmez                        |
|                                 |                                 |
| TempError                       | TempError verir                 |
|                                 |                                 |
| PermError                       | PermError verir                 |
|                                 |                                 |
| None                            | PermError verir                 |
+---------------------------------+---------------------------------+
```

"include" mekanizması yönetimsel sınırları çaprazlamak için düşünülmüştür. "include" mekanizması çok sayıda alanın aynı konak kümesini paylaşmak üzere birleştirilmesi için kullanılması olasılığına rağmen, alanlar mümkün olduğunca "redirect"'leri kullanmaya, tek bir yönetimsel alan içinde "include"'ların sayısını azaltmaya teşvik edildiler. Örneğin, example.com ve example.org aynı öğe tarafından yönetiliyor ve eğer her iki alan "mx:example.com" konaklarına izin veriyorsa, example.org için "include:example.com" belirtmek mümkün olurdu, ama "redirect=example.com" hatta "mx:example.com" belirtmek tercih edilmektedir.

5.3. "a"

Eğer <ip>, <hedef-ismi>nin IP adreslerinden biriyse bu mekanizma eşleşir.

```
A                = "a"      [ ":" alan-belirtimi ] [ çifte-cidr-uzun ]
```

<hedef-ismi> üzerinde bir adres sorgusu yapılır ve dönen adresler <ip> ile karşılaştırılır. Eğer adreslerden biri eşleşirse, mekanizma eşlemiş olur.

5.4. "mx"

Eğer <ip>, alan adının MX konaklarından birine aitse bu mekanizma eşleşir.

```
MX               = "mx"     [ ":" alan-belirtimi ] [ çifte-cidr-uzun ]
```

check_host() işlevi önce <hedef-ismi> üzerinde bir MX sorgusu ve dönen her MX ismi üzerinde bir adres sorgusu yapar. Dönen adresler <ip> ile karşılaştırılır. Eğer adreslerden biri eşleşirse, mekanizma eşlemiş olur. Hizmet reddi (DoS) saldırısına dönüşmemesi için "mx" mekanizmasının değerlendirilmesi sırasında 10 taneden fazla MX ismi sorgusu yapılmamalıdır *ZORUNLU* (bkz, *Güvenlik Değerlendirmeleri* (sayfa: 26)).

Örtük MX'ler hakkında

Eğer <hedef-ismi> hiç MX kaydı içermiyorsa, check_host() işlevi hedefin tek bir MX'i varmış gibi yapmamalı *ZORUNLU* ve <hedef-ismi>'ne doğrudan bir A sorgusu yöneltmemelidir *ZORUNLU*. Bu davranış standart "örtük MX" kuralını bozar ([*RFC2821*]'in Adres Çözümleme ve Posta Yönetimi[B52] bölümüne bakınız). Böyle bir davranış isteniyorsa, kaydı tasarlayanın bir "a" yönergesi belirtmesi gerekir.

5.5. "ptr"

Bu mekanizma, DNS'nin <ip> için tersine eşleşmesi olup olmadığını yani alan içindeki belli bir alan adını gösterip göstermediğini sınar.

```
PTR             = "ptr"     [ ":" alan-belirtimi ]
```

Önce, <ip>'nin ismi şu yordamla aranır: <ip> için, eğer adres bir IPv4 adresi ise "in–addr.arpa." içinde, IPv6 adresi ise "ip6.arpa." içinde ilgili PTR kaydını aramak suretiyle bir DNS tersine eşleşme sorgusu uygulanır. Dönen her kayıt için, alan adının IP adresi <ip> ile karşılaştırılır. Hizmet reddi (DoS) saldırısına dönüşmemesi için "ptr" mekanizmasının değerlendirilmesi sırasında 10 taneden fazla PTR sorgusu yapılmamalıdır *ZORUNLU* (bkz, *Güvenlik Değerlendirmeleri* (sayfa: 26)). Eğer adreslerden biri eşleşirse, mekanizma eşlemiş olur. Şu sözde kod içinde:

```
gönderen_alan_adları := ptr_sorgusu (gönderen_konak_ip_adresi);
Eğer gönderen_alan_adı_sayısı > 10 ise
   gönderen_alan_adı_sayısı := 10;
gönderen_alan_adı_sayısı isim için {
   ip_adresleri := a_sorgusu (isim);
   Eğer gönderen_alan_ip_adresi == ip_adresleri'nden biri ise {
       doğrulanmış_gönderen_alan_adları += isim;
   }
}
```

Tüm doğrulanmış alan adlarına, <hedef-ismi> alanı ile eşleşiyor mu diye bakılır. Eğer bir eşleşme bulunursa, bu mekanizma eşleşmiş olur. Eğer doğrulanmış hiç alan adı yoksa ya da doğrulanmış olup da <hedef-ismi> ile eşleşen biri yoksa, bu mekanizma eşleşmemiş olur. Eğer PTR sorgusu sırasında bir DNS hatası oluşursa, bu mekanizma eşleşmemiş olur. Bir A sorgusu yaparken bir DNS hatası oluşursa, alan ismi atlanır ve arama devam eder.

Sözde kod:

```
doğrulanmış_gönderen_alan_adları içindeki her ad için {
  Eğer ad <alan-belirtimi> ile bitiyorsa, eşleşme döndür;
  Eğer ad <alan-belirtimi> ile aynıysa, eşleşme döndür;
}
eşleşmeme döndür;
```

Eğer <hedef-ismi>, doğrulanmış alan adlarından birinin atasıysa ya da onlardan biri ile aynıysa bu mekanizma eşleşir. Örneğin, "posta.iyi–misal.çom" adı "iyi–misal.çom" alanı altındadır ama "posta.berbat–misal.çom" değildir.

Bilgi

Yavaş olduğundan bu mekanizmanın kullanımı teşvik edilmemektedir. DNS hataları bakımından diğer mekanizmalar kadar güvenilir değildir ve arpa isim sunucularına ağır bir yük getirir. Eğer kullanılırsa, alanın konakları için doğru PTR kayıtları bulunmalı ve "ptr" mekanizması sınanması gereken son mekanizmalardan biri olmalıdır.

5.6. "ip4" ve "ip6"

Bu mekanizma, <ip>, belirtilen IP ağında mıymış acaba diye bakar.

```
IP4             = "ip4"      ":" ip4-ağı    [ ip4-cidr-uzun ]
IP6             = "ip6"      ":" ip6-ağı    [ ip6-cidr-uzun ]

ip4-cidr-uzun   = "/" 1*RAKAM
ip6-cidr-uzun   = "/" 1*RAKAM
çifte-cidr-uzun = [ ip4-cidr-uzun ] [ "/" ip6-cidr-uzun ]
```

```
ip4-network      = dörtlü "." dörtlü "." dörtlü "." dörtlü
dörtlü             = RAKAM                 ; 0-9
                   / %x31-39 RAKAM       ; 10-99
                   / "1" 2RAKAM          ; 100-199
                   / "2" %x30-34 RAKAM   ; 200-249
                   / "25" %x30-35        ; 250-255
                   ; bilinen noktalı dörtlü gösterim.  192.0.2.0 gibi
ip6-ağı      = <[RFC3513], 2.2. bölüme göre>
                   ; örn, 2001:DB8::CD30
```

<ip> belirtilen ağ (IP bloğu) ile karşılaştırılır. Eğer CIDR uzunluğunun yüksek seviyeli bitleri eşleşiyorsa (Türkçesi, <ip> belirtilen IP bloğunun üyesi ise) mekanizma eşleşir.

Eğer ip4-cidr-uzun verilmemişse "/32" olduğu, ip6-cidr-uzun verilmemişse "/128" olduğu varsayılır. CIDR gösterimi yerine IP parçalarının kullanımına, örneğin 192.0.2.0/24 yerine 192.0.2 belirtilmesine izin verilmez.

5.7. "exists"

Bu mekanizma, bir DNS A kaydı sorgusu için kullanılmak üzere keyfi bir alan adı oluşturmakta kullanılır. Neye izin verildiğini saptamak için posta zarfının keyfi parçalarının oluşturduğu karmaşık şemaları mümkün kılar.

```
exists           = "exists"   ":" alan-belirtimi
```

alan-belirtimi *Makrolar* (sayfa: 20) bölümüne göre yorumlanır. Sonuçlanan alan adı DNS A kaydı sorgusu için kullanılır. Eğer bir A kaydı dönerse bu mekanizma eşleşmiş olur. Bağlantı türü IPv6 bile olsa, DNS sorgu türü A'dır.

Alanlar bu mekanizmayı keyfi karmaşık sorguları belirtmek için kullanırlar. Örneğin, example.com'un şöyle bir kaydı olsun:

```
v=spf1 exists:%{ir}.%{l1r+-}._spf.%{d} -all
```

<hedef-ismi> "1.2.0.192.someuser._spf.example.com" olarak yorumlanabilirdi. Bu, kullanıcı ve istemci IP adresi seviyesinde ayrıntılı kararlar verilmesini mümkün kılar.

Bu mekanizma mevcut antispam DNS karalistelerinin (DNSBL) kullandığı sınama tarzını taklit eden sorguları etkinleştirir.

6. Değiştirici Tanımları

Değiştiriciler ek bilgi sağlayan isim/değer çiftleridir. Değiştiriciler daima isim ve değeri ayıran bir "=" imi içerirler.

Bu belgede tanımlanmış değiştiriciler ("redirect" ve "exp") kaydın her yerinde görünebilir *SEÇİMLİK* fakat sonda, tüm mekanizmalardan sonra görünürse iyi olur *ÖNERİ*. Bu iki değiştirici arasında bir öncelik sözkonusu değildir. Bu iki değiştiricinin her biri bir kayıtta birden fazla görünemez *ZORUNLU*. Eğer bu yapılırsa, check_host() işlevi "PermError" sonucu ile çıkar.

Tanınmayan değiştiriciler nerede nasıl göründüklerine bakılmaksızın yok sayılmalıdırlar *ZORUNLU*. Bu, bu belgenin gerçeklenimcilerine diğer belirtimlerde tanımlanmış değiştiricileri içeren kayıtlarla rahatça çalışma imkanı verir.

6.1. Yönlendirilmiş Sorgu (redirect)

Eğer tüm mekanizmalar eşleşmez ve bir "redirect" değiştiricisi de mevcutsa süreç şöyle gelişir:

```
sevket           = "redirect" "=" alan-belirtimi
```

Sevket belirtiminin alan-belirtimi bölümü *Makrolar* (sayfa: 20) bölümündeki makro kurallarına göre yorumlanır. Sonuçlanan dizge check_host() işlevinde <alan> olarak değerlendirilir, <ip> ve <gönderici> ise o anki değerlendirme değerleri olarak değişmeden kalır.

Bu yeni check_host() değerlendirmesinin sonucu, bir SPF kaydının yokluğu dışında mevcut değerlendirmenin sonucu sayılır ya da <hedef-ismi> bozuksa, sonuç "None"'dan ziyade bir "PermError" olur.

Yönlendirme sonucu sorgulanan alanın kendisinin de bir yönlendirme belirtebileceğine dikkat ediniz.

Bu oluşum, aynı kaydı çok sayıda alana uygulamak isteyen bir örgüt tarafından kullanılmak üzere tasarlanmıştır. Örnek:

```
    la.example.com. TXT "v=spf1 redirect=_spf.example.com"
    ny.example.com. TXT "v=spf1 redirect=_spf.example.com"
    sf.example.com. TXT "v=spf1 redirect=_spf.example.com"
_spf.example.com. TXT "v=spf1 mx:example.com -all"
```

Bu örnekte, bu üç alanın her birine ait posta için aynı kayıt kullanılmaktadır. Bu yönetimsel bir yarar sağlayabilir.

Bilgi

Genelde, aynı yönetimsel denetim altında olmayan "B" alanına "A" alanı tarafından yapılan bir yönlendirme güvenilir olmayacaktır. <gönderici> aynı kaldığından, özellikle "B" alanının yerel kısımlarla ilgili mekanizmaları kullanması durumunda, "B" alanındaki kaydın "A" alanındaki posta kutuları için doğru çalışacağının hiçbir garantisi yoktur. Bir "include" yönergesi daha uygun olabilirdi.

Bir "redirect" değiştiricisinin bir kaydın en sonunda yer alması tavsiye edilir *ÖNERİ*.

6.2. İzahat (exp)

```
izahat          = "exp" "=" alan-belirtimi
```

Eğer tüm mekanizmaların eşleşmemesinin sonucu olarak check_host() işlevi "Fail" sonucunu verirse ve bir "exp" değiştiricisi de mevcutsa izahat-dizgesi aşağıda açıklandığı gibi hesaplanır. Eğer bir "exp" değiştiricisi de mevcut değilse ya öntanımlı bir izahat-dizgesi ya da boş bir izahat-dizgesi dönebilir.

<alan-belirtimi> *Makrolar* (sayfa: 20) bölümündeki makro kurallarına göre yorumlanır ve <hedef-ismi> haline gelir. <hedef-ismi> için DNS TXT kaydı sorgulanır.

<alan-belirtimi> boşsa veya bir DNS hatası dönmüşse (0'dan farklı bir RCODE) ya da hiç kayıt dönmemişse, ya da birden fazla kayıt dönmüşse veya izahat-dizgesi nde bir sözdizimi hatası varsa, hiç "exp" değiştiricisi verilmemiş gibi işlem yapılır.

Alınan TXT kayıtlarındaki dizgeler aralarına boşluk konmaksızın ardarda eklenir ve makro yorumlamalı bir <izahat-dizgesi> olarak ele alınır. Gerçeklenimler <izahat-dizgesi>nin sonuç uzunluğunu makul işlem sınırları veya diğer protokol kısıtlamalarına izin vermek için sınırlayabilirler. <izahat-dizgesi> bir SMTP yanıtı olarak tasarlandığından ve [*RFC2821*]'in Sözdizimsel Genel Prensipler ve Harekât Modeli[B59] bölümü yanıtların [*US–ASCII*] olmasını gerektirdiğinden, <izahat-dizgesi> de US–ASCII kodlanmış olmalıdır.

check_host() işlevini değerlendiren yazılım, bu dizgeyi, yayınlayan alandaki bilgiyi bir kısa ileti veya bir URL biçiminde iletmek için kullanabilir. Yazılım bu dizgenin üçüncü şahıslardan kaynaklandığını açıklığa kavuşturmalıdır *ÖNERİ*. Örneğin, dizgenin başına *Fail* (sayfa: 7) bölümünde gösterildiği gibi "%{o} explains: " makro dizgesini ekleyebilir.

example.com'un şöyle bir kaydı olsun:

```
v=spf1 mx -all exp=explain._spf.%{d}
```

Aşağıda explain._spf.example.com'da <izahat-dizgesi> olarak kullanılabilecek olası TXT kayıtları örneklerine yer verilmiştir:

```
"Mail from example.com should only be sent by its own servers."
    -- basit ve sabit bir ileti

"%{i} is not one of %{d}'s designated mail servers."
    -- sınaması başarısız olan IP adresini içererek biraz daha bilgi
       veren bir ileti

"See http://%{d}/why.html?s=%{S}&i=%{I}"
    -- check_host() işlevine argümanlar içeren bir URL'den oluşan
       biraz daha karmaşık bir ileti; böylece daha ayrıntılı ve
       özel talimatlar içeren bir sayfa hazırlanabilir
```

Bilgi

Bir "include" mekanizmasına yineleme sırasında, <hedef-ismi>'ndeki bir "exp" değiştiricisi kullanılmamalıdır *ZORUNLU*. Aksine, bir "redirect" değiştiricisi değerlendirilirken özgün alandaki bir "exp" değiştiricisi kullanılmamalıdır *ZORUNLU*.

7. "Received-SPF" Başlık Alanı

SMTP alıcılarının SPF işleminin sonucunu ileti başlığına kaydetmeleri önerilir *ÖNERİ*. Eğer bir SMTP alıcısı bunu yapmak isterse, sınadığı her kimlik için burada tanımlanan "Received-SPF" başlık alanını kullanmalıdır *ÖNERİ*. Bu bilgi alıcı için tasarlanmıştır. (Gönderici için tasarlanmış bilgi *İzahat (exp)* (sayfa: 18) bölümünde açıklanmıştı.)

"Received-SPF" başlık alanı bir izleme alanıdır ([*RFC2822*]'nin İzleme alanları[B64] bölümüne bakınız) ve mevcut başlıkların önüne, SMTP alıcı tarafından üretilen "Received:" alanının üstüne eklenmelidir *ÖNERİ*. İletideki diğer tüm "Received-SPF" başlık alanlarının üstünde görünmelidir *ZORUNLU*. Başlık alanının biçimi:

```
başlık-alanı      = "Received-SPF:" [AKBOŞ] sonuç KBOŞ [açıklama KBOŞ]
                    [ anah-değer-list ] CRLF

sonuç             = "Pass" / "Fail" / "SoftFail" / "Neutral" /
                    "None" / "TempError" / "PermError"

anah-değer-list   = anah-değer-çifti *( ";" [AKBOŞ] anah-değer-çifti )
                    [";"]

anah-değer-çifti = anahtar [AKBOŞ] "=" ( nokta-atom / tırnaklı-dizge )

anahtar           = "client-ip" / "envelope-from" / "helo" /
                    "problem" / "receiver" / "identity" /
                    "mechanism" / "x-" isim / isim

kimlik            = "mailfrom"    ; "MAIL FROM" kimliği için
                    / "helo"      ; "HELO"kimliği için
```

```
                    / isim       ; diğer kimlikler

   nokta-atom       = <[RFC2822]'ye göre tırnaksız sözcük>
   tırnaklı-dizge   = <[RFC2822]'ye göre tırnaklı dizge>
   açıklama         = <[RFC2822]'ye göre açıklama dizgesi>
   AKBOŞ            = <[RFC2822]'ye göre açıklamalı katlama boşlukları>
   KBOŞ             = <[RFC2822]'ye göre katlama boşlukları>
   CRLF             = <[RFC2822]'ye göre standart satır sonu dizgeciği>
```

Başlık alanı <sonuç>tan sonra <ip>, <gönderici>, ve <alan> gibi sonucu destekleyen bilgileri içeren "(...)" tarzı bir <açıklama> içermelidir *ÖNERİ*.

Aşağıdaki anahtar–değer çiftleri sonraki bir makine çözümlemesi için tasarlanmışlardır. SPF istemcileri SPF sonuçlarını doğrulayabilecek yeterli bilgiyi vermelidirler *ÖNERİ*. Yani, en azından "client-ip" ve "helo" anahtarlarıyla, "MAIL FROM" kimliği sınanmışsa "envelope-from" bulunmalıdır.

client-ip
: SMTP istemcinin IP adresi

envelope-from
: Zarf gönderici posta kutusu

helo
: **HELO** veya **EHLO** komutunda verilmiş konak adı

mechanism
: eşleşen mekanizma (eşleşen mekanizma yoksa "default" kullanılır)

problem
: bir hata dönmüşse, sorun ile ilgili ayrıntılar

receiver
: SPF istemcisinin konak adı

identity
: sınanan kimlik; <kimlik> ABNF kuralına bakınız

SPF istemcileri tarafından başka anahtarlar tanımlanabilir. Yeni bir anahtar geniş kabul görene kadar isimleri "x-" ile başlatılmalıdır.

SPF istemcileri "Received-SPF" başlık alanlarının geçersiz karakterler içermediğinden, aşırı uzun olmadığından ve göndericiden kaynaklanan bozucu veri içermediğinden emin olmalıdırlar *ZORUNLU*.

Üretilebilecek çeşitli başlık alanlarından örnekler:

```
   Received-SPF: Pass (mybox.example.org: domain of
    myname@example.com designates 192.0.2.1 as permitted sender)
       receiver=mybox.example.org; client-ip=192.0.2.1;
       envelope-from=<myname@example.com>; helo=foo.example.com;

   Received-SPF: Fail (mybox.example.org: domain of
                     myname@example.com does not designate
                     192.0.2.1 as permitted sender)
                     identity=mailfrom; client-ip=192.0.2.1;
                     envelope-from=<myname@example.com>;
```

8. Makrolar

8.1. Makro Tanımları

Bazı mekanizmalar ve değiştiriciler terim parçaları üzerinde makro yorumlaması yaparlar.

```
alan-belirtimi   = makro-dizgesi alan-sonu
alan-sonu        = ( "." tepeyafta [ "." ] ) / makro-genleş

tepeyafta        = ( *harfrakam HARF *harfrakam ) /
                   ( 1*harfrakam "-" *( harfrakam / "-" ) harfrakam )
                   ; HRT kuralı artı ek TLD kısıtlamaları
                   ; (bkz [RFC3696], 2. bölüm)
harfrakam        = HARF / RAKAM

izahat-dizgesi    = *( makro-dizgesi / SP )

makro-dizgesi    = *( makro-genleş / makro-sabiti )
makro-genleş     = ( "%{" makro-harfi dönüştürücüler *ayraç "}" )
                   / "%%" / "%_" / "%-"
makro-sabiti     = %x21-24 / %x26-7E
                   ; "%" hariç görünür karakterler
makro-harfi      = "s" / "l" / "o" / "d" / "i" / "p" / "h" /
                   "c" / "r" / "t"
dönüştürücüler   = *RAKAM [ "r" ]
ayraç            = "." / "-" / "+" / "," / "/" / "_" / "="
```

Yüzde imi "%%" ile ifade edilir.
"%_" makrosu tek bir " " (boşluk) olarak yorumlanır.
"%-" makrosu "%20" şeklinde bir URL kodlu boşluk olarak yorumlanır.

Terim argümanlarında kullanılan makro harflerinin anlamları:

```
s = <gönderici>
l = <gönderici>'nin yerel kısmı
o = <gönderici>'nin alanı
d = <alan>
i = <ip>
p = <ip>'nin doğrulanmış alan adı
v = <ip> bir ipv4 ise "in-addr" dizgesi, bir ipv6 ise "ip6" dizgesi
h = HELO/EHLO alanı
```

Sadece "exp" metni içinde kullanılabilen makro harfleri:

```
c = SMTP istemci IP'si (kolayca okunabilir biçim)
r = sınamayı yapan konağın alan adı
t = o an ki zaman damgası
```

Bir yüzde imi '{', '%', '-', '_' karakterlerini öncelemekte kullanılmamışsa sözdizimi hatası olarak yorumlanır. Yani,

```
-exists:%(ir).sbl.spamhaus.example.org
```

yanlıştır ve check_host() işlevinin "PermError" döndürmesine sebep olur. Doğrusu şöyle olmalıdır:

```
-exists:%{ir}.sbl.spamhaus.example.org
```

İsteği bağlı dönüştürücüler:

```
*RAKAM = sıfır veya başka rakamlar
'r'    = yedek değer, öntanımlı olarak noktalarla ayrılarak
```

Dönüştürücüler veya ayraçlar kullanılmışsa, bir makro harfinin değeri parçalara ayrılır. Tersine bir işlem yürütüldükten sonra ve/veya sol taraf parçaları kaldırıldıktan sonra parçalar özgün ayraç karakterleri değil "." kullanılarak biraraya getirilirler.

Öntanımlı olarak dizgeler "." (nokta) kullanılarak birbirlerinden ayrılırlar. Baştaki, sondaki ve ardarda gelen ayraçların özel olarak ele alınmadığına ve dolayısıyla parça listelerinin boş dizgeler içermeyebileceğine dikkat ediniz. SPF'nin eski gerçeklenimleri alan isimlerinden sonra nokta konmasına izin vermezdi; dolayısıyla, alan sahiplerinin bu belgeyle uyumlu gerçeklenimlerce kabul edilebilmesi için böyle isimler yayınlamaması gerekir. Makrolarda "." yerine kullanılan ayraç karakterleri belirtilebilir.

'r' dönüştürücüsü tersinir bir işlem belirtir: istemci IP'si 192.0.2.1 ise, %{i} makrosu "192.0.2.1" üretirken, %{ir} makrosu "1.2.0.192" üretir.

RAKAM dönüştürücüsü kullanılacak sağ taraf parçalarının sayısını belirtir. Eğer bir RAKAM belirtilmişse, değeri sıfır olmamalıdır *ZORUNLU*. Eğer hiç RAKAM belirtilmemişse veya değer kullanılan parça sayısından fazlasını belirtiyorsa, kullanılabilecek bütün parçalar kullanılır. Eğer RAKAM 5 ise ve 3 parça varsa, makro RAKAM'ın değeri 3'müş gibi yorumlanır. Gerçeklenimler bir alan ismindeki azami yafta sayısı olarak en azından 128 değerine destek vermelidiriler *ZORUNLU*.

"s" makrosu <gönderici> olarak yorumlanır. bir yerel kısım, de–imi ve bir alandan oluşan bir eposta adresidir. "l" makrosu yerel-kısım olarak yorumlanır. "o" makrosu ise alan olarak yorumlanır. bu değerlerin "include" ve/veya "redirect" nedeniyle ardışık yorumlama sırasında aynı kaldıklarına dikkat ediniz. Ayrıca, özgün <gönderici>'de yerel-kısım yoksa, yerine, ilk işlem sırasında "postmaster" getirileceğini unutmayınız (bkz, *İlk İşlem* (sayfa: 11)).

IPv4 adresler için, "i" ve "c" makrolarının ikisi de standart noktalı dörtlü biçiminde yorumlanır.

IPv6 adresler için, "i" makrosu noktalı biçimde bir adrestir ve %{ir} kullanımı için tasarlanmıştır. "c" makrosu ise [*RFC3513*]'ün 2.2. bölümünde belirtilen ikinoktalı onaltılık biçimli bir adres olarak yorumlanır ve insanların okuması için düşünülmüştür.

"p" makrosu <ip>'nin doğrulanmış alan adı olarak yorumlanır. Doğrulanmış alan adının bulunması *"ptr"* (sayfa: 15) bölümünde tanımlanmıştır. Eğer <alan> doğrulanmış alan adları içindeyse, onun kullanılması gerekir *ÖNERİ*, yoksa, eğer <alan>'ın bir alt alan adı varsa o kullanılmalıdır *ÖNERİ*. Aksi takdirde listedeki herhangi bir isim kullanılabilir. Eğer doğrulanmış bir alan adı yoksa veya bir DNS hatası oluşmuşsa, "unknown" dizgesi kullanılır.

"r" makrosu alıcı MTA'nın ismi olarak yorumlanır. Bunun tamamen nitelenmiş bir alan adı olması gerekir *ÖNERİ*, fakat böyle bir isim yoksa (sınama bir MUA tarafından yapılıyorsa) veya sınama önlemleri belirtilmemesini gerektiriyorsa, "unknown" dizgesi kullanılmalıdır *ÖNERİ*. Alan adı, istemci MTA'nın alıcı MTA'yı bulmak için kullandığı MX kaydında bulunan isimden farklı olabilir.

"t" makrosu, onluk tabanda, mutlak zaman başlangıcından beri (UTC olarak, 1 Ocak 1970 geceyarısından itibaren) geçen saniye sayısı olarak yorumlanır. Bu, standartlarla uyumlu çoğu kütüphanede bulunan POSIX time() işlevinden dönen değerdir.

Makro yorumunun sonucu bir alan adı sorgusunda kullanılırken, eğer yorumlanmış alan adı 253 karakteri (azami alan adı uzunluğu) aşıyorsa, baştan itibaren 253 karakter alınır.

Büyük harfli makrolar küçük harfli eşdeğerleri olarak yorumlanır ve bundan sonra URL öncelenir. [*RFC3986*]'da tanımlanmış "urice" karakter kümesinde bulunmayan karakterlere URL öncelemesi uygulanmalıdır.

Bilgi

Meşru eposta için makro yorumlaması sırasında DNS yaftalarında 63 karakterlik sınırın aşılamayacağına dikkat ediniz. Eposta adreslerinin yerel kısımlarında ise noktalar arasındaki dizgecikler 63 karakterden uzun olabilir.

Bilgi

Alanlar, herhangi bir mekanizma yönergesi ile birlikte "s", "l", "o" veya "h" makrosunu kullanmaktan kaçınmalıdırlar. Bu makrolar çok güçlü olduklarından ve kullanıcı temelinde kayıt yayınlamayı mümkün kıldıklarından check_host() sonucunu arabellekleyen gerçeklenimlerin yeteneklerini epeyce sınırlarlar ve DNS arabelleklerinin etkinliğini azaltırlar.

"s", "l", "o" veya "h" makrorusun içeren bir check_host() değerlendirmesi sırasında işlenen bir yönerge yoksa, değerlendirme sonucu, tüm DNS kayıtlarının uyması gereken en kısa yaşam süresince (TTL) sadece <alan> ve <ip> temelinde arabelleklenebilir.

8.2. Makro Yorumlama Örnekleri

<gönderici> strong–bad@email.example.com, IPV6 SMTP istemcisi 2001:DB8::CB01 ve istemci IP'nin PTR alan adı mx.example.org olmak üzere:

```
makro                          yorumu
-------  ----------------------------
%{s}     strong-bad@email.example.com
%{o}                email.example.com
%{d}                email.example.com
%{d4}               email.example.com
%{d3}               email.example.com
%{d2}                     example.com
%{d1}                             com
%{dr}               com.example.email
%{d2r}                  example.email
%{l}                       strong-bad
%{l-}                      strong.bad
%{lr}                      strong-bad
%{lr-}                     bad.strong
%{l1r-}                        strong

makro-dizgesi                                                  yorumu
-------------------------------------------------------------------------
%{ir}.%{v}._spf.%{d2}             3.2.0.192.in-addr._spf.example.com
%{lr-}.lp._spf.%{d2}                  bad.strong.lp._spf.example.com

%{lr-}.lp.%{ir}.%{v}._spf.%{d2}
                     bad.strong.lp.3.2.0.192.in-addr._spf.example.com

%{ir}.%{v}.%{l1r-}.lp._spf.%{d2}
                          3.2.0.192.in-addr.strong.lp._spf.example.com

%{d2}.trusted-domains.example.net
                               example.com.trusted-domains.example.net
```

```
IPv6:
%{ir}.%{v}._spf.%{d2}                                  1.0.B.C.0.0.0.0.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.B.D.0.1.0.0.2.ip6._spf.example.com
```

9. Etkilenimler

Bu bölümde Genel Ağ Epostasıyla ilgili çeşitli öğelere bu belgenin uygulanmasının belli başlı sonuçlarına anahatlarıyla değinilecektir. Bu belgenin bu tür öğelerin işlemleri üzerindeki bilinen etkileri konusunda okuyucunun aydınlanması amaçlanmıştır. Bu bölüm bir "nasıl" kılavuzu ya da bir "en iyi uygulamalar" belgesi değildir ve bu belgenin ışığında böyle öğelere neler yapılması gerektiğinin kapsamlı bir listesi değildir.

Bu bölüm, uyulması zorunlu bölümlerden biri değildir.

9.1. Gönderici Alanlar

Bu belirtimle uyumlu olmak isteyen alanların, alan isimlerini "HELO" ve "MAIL FROM" kimliklerinde kullanarak posta gönderebilecek konakları belirlemeleri gerekecektir. Böyle bir listenin hazırlanması, basitçe bir teknik alıştırmanın değil hem teknik hem de yönetimsel değerlendirmeler altında verilen kararların sonucu olarak ortaya çıkar.

"Mevcutların izlenmesi" mekanizmasını içeren kayıtlar yayınlamak yararlı olabilir. İsim sunucusunun günlüklerine bakarak kabaca bir liste üretilebilir. Örnek:

```
v=spf1 exists:_h.%{h}._l.%{l}._o.%{o}._i.%{i}._spf.%{d} ?all
```

9.2. Postalama Listeleri

Postalama listelerinin listeye gönderecekleri postayı nasıl teslim edeceklerini bilmeleri gerekir. Postalama listelerinin [*RFC2821*]'in Postalama Listeleri ve Rumuzlar[B77] bölümünde ve [*RFC1123*]'ün 5.3.6. bölümündeki, dönüş yolunun listeyi yöneten şey veya şahsın posta kutusu olarak değiştirilmesi gereğini *ZORUNLU* belirten gereksinimlere uyması gerekir *ZORUNLU*. Dönüş yolunun değiştirilmesi gereğinin çok çeşitli ve uzun uzadıya giden sebepleri vardır, SPF bu gereksinime güç katar.

Uygulamada, halihazırda kullanımda olan hemen tüm postalama listesi yazılımları bu gereksinimi karşılamaktadır. Listeye erişimle ilgili sorunları saptayamayan veya belki de uyum sağlamayan postalama listelerinin kullanım alanı sınırlıdır. Tamamen tek bir alana dahili olarak hizmet sunan böyle listeler bu gereksinimden etkilenmezler.

9.3. Yönlendirme Hizmetleri ve Takma Adlar

Yönlendirme hizmetleri postayı harici bir posta kutusuna teslim edilmek üzere alırlar. Bu belgenin yazımı sırasında, böyle hizmetlerin genel uygulaması, postayı harici bir posta kutusuna teslim ederken iletinin özgün "MAIL FROM" kimliğini kullanmak şeklindedir. [*RFC1123*] ve [*RFC2821*] belirtimleri bu eylemi bir "posta listesi" değil, bir "takma ad" uygulaması olarak açıklarlar. Bu, harici posta kutusu MTA'sının böyle postaları yönlendirme hizmetinin bir konağı ile yaptığı bağlantıda göreceği ve dolayısıyla "MAIL FROM" kimliğinin genelde sınamayı aşamayacağı anlamına gelir.

Bu sorunu gidermekte kullanılabilen teknikler üç yerde olabilir.

1. Başta, eposta ilk gönderilirken.
    1. Yönlendiricilerin IP adresi olabilecekler için "`Fail`" yerine "`Neutral`" sonuçlar verilebilir. Örnek:

```
"v=spf1 mx -exists:%{ir}.sbl.spamhaus.example.org ?all"
```

Bu, bir anti–spam DNS karalistesinde bir sorguya sebep olur. Sadece, burada kayıtlı kaynaklardan gelen epostalara "Fail" sonucu verilebilir. Diğer epostalar, yönlendiricilerden gelenler de dahil olmak üzere "Neutral" sonucu alabilirler. Bilinen iyi kaynaklardan gelenler ayrıldıktan sonra DNS kara listelerine bakmak, bu listelerin hatalı kayıtlarından büyük oranda korunmayı sağlar.

2. "MAIL FROM" kimliğindeki yerel kısım, postanın yetkili bir kaynaktan geldiğini şifreli biçimde belli eden ek bir bilgi içerebilir. Bu durumda şöyle bir SPF kaydı kullanılabilirdi:

   ```
   "v=spf1 mx exists:%{l}._spf_verify.%{d} -all"
   ```

   Sonra da,özelleştirilmiş bir DNS sunucusu yerel kısmı doğrulayan _spf_verify alt alanını sunmaya ayarlanabilir. Bu ek bir DNS sorgusu gerektireceğinden, epostanın bilinen bir iyi kaynaktan gelmemesi sebebiyle reddedilmesi sözkonusu olduğunda bu ek sorgu yapılabilir.

   Alan yaftalarındaki 63 karakterlik sınırdan dolayı, bu yaklaşım sadece, yerel kısım oluşturma şeması sadece azami 63 karakterlik yerel kısımların oluşturulacağını veya kırpılmış yerel kısımların gerektiği gibi işleneceğini garanti ediyorsa güvenilir olarak çalışır.

3. Benzer şekilde, umulmadık IP adreslerinden gelen epostaya hız sınırlaması koyan özelleştirilmiş bir DNS sunucusu ayarlanabilir.

   ```
   "v=spf1 mx exists:%{ir}._spf_rate.%{d} -all"
   ```

4. SPF, özel durumlarda kullanıcıya özgü kural oluşturmaya izin verir. Örneğin, bu SPF kaydı ve ona uygun isim kalıplı DNS kayıtları kullanılabilir:

   ```
   "v=spf1 mx redirect=%{l1r+}._at_.%{o}._spf.%{d}"
   ```

2. Ortada, eposta yönlendirilirken.

   1. Yönlendirme hizmetleri "MAIL FROM" kimliğini kendilerine göre yeniden yazarak sorunu çözümleyebilir. Bu, harici posta kutusundaki boş dönüş yollu postanın yönlendirme hizmeti tarafından yeniden boş dönüş yollu yapıldığı anlamına gelir. Yönlendirme hizmetinin parçası olarak özkaynak gereksinimleri ve karmaşıklığındaki çeşitliliğe bağlı olarak bunu yapan çeşitli şemalar vardır.

   2. Çok kullanılan MTA'ların birçoğu "takma ad" anlamsallığına, özgün takma ada "owner–" öneki getirerek ek bir takma isim oluşturan "postalama listesi" anlamsallığını verebilirler (örn, "friends: george@example.com, fred@example.org" takma adı, "owner–friends: localowner" şeklinde başka bir takma ad gerektirirdi).

3. Sonda, eposta alınırken.

   1. Harici posta kutusunun sahibi yönlendirme hizmetine güvence vermek isterse, istemci konak, yönlendirme hizmetine ait olduğunda, harici posta kutusunun MTA'sının SPF sınamalarını atlamasını sağlayabilir.

   2. "HELO" kimliği gibi, diğer kimliklerle yapılan sınamalar başarısız olmuş bir "MAIL FROM" kimliği sınamasından sonra red öncesi ek bir sınama olarak kullanılabilir.

   3. Büyük alanlar için, alanın posta kutularının sahipleri tarafından kullanılan yönlendirme hizmetlerinin tam ve doğru bir listesini yapmak mümkün olmayabilir. Böyle durumlarda, genel olarak tanınan yönlendirme hizmetleri aklistelere kaydedilebilir.

9.4. Posta Hizmetleri

Üçüncü şahıs alanlara toptan posta göndermek gibi posta hizmetleri sunan hizmet sağlayıcılar, bu belgede açıklanan yetkilendirme sınaması ışığında kendi ayarlarını yapabilirler. "MAIL FROM" kimliği hizmet sağlayıcının alanını kullanan böyle bir eposta için kullanılmışsa, hizmet sağlayıcı sadece, gönderici konağının (varsa) kendi SPF kaydı tarafından yetkilendirilmesine ihtiyaç duyar.

"MAIL FROM" kimliği hizmet sağlayıcının alanını kullanmıyorsa, biraz daha dikkatli olmak gerekir. SPF kaydının biçimi dahilinde, üçüncü şahıs alanların kendi yararına posta göndermesi için hizmet sağlayıcınan MTA'sını yetkili kılacak birçok seçenek bulunmaktadır. Aynı MTA'yı kullanan çok çeşitli müşterileri olan ISP'ler gibi posta hizmeti sağlayıcıları çapraz–müşteri sahtekarlıklarından kaçınmayı sağlayacak adımları atmalıdırlar (bkz, *Çapraz–Kullanıcı Sahtekarlığı* (sayfa: 28)).

9.5. MTA Röleleri

Yetkilendirme sınaması, bir epostanın alıcısı ve göndericisi arasında keyfi MTA röleleri kullanımına genel olarak imkan vermez.

Bir örgüt içinde, MTA röleleri etkin olarak konuşlandırılmış olabilir. Bununla birlikte, bu belgenin amaçları gereği, böyle röleler aslında şeffaf olmalı, SPF yetkilendirme sınaması da farklı alanların sınır MTA'ları arasındaki bir sınama olmalıdır.

Posta göndericiler için bu, SPF kayıtlarının, postayı Genel Ağ'a gönderen MTA'ları yetkilendirdiği anlamına gelir. Kendi aralarında posta alışverişi yapan dahili MTA'lar gibi, bunlar da kendi aralarında posta alışverişi yapan sınır MTA'lardır, şeklinde düşünülebilir.

Posta alıcıları, özellikle tüm ikincil MX'leri de içererek, sınır MTA'larda yetkilendirme sınaması yapmak isteyeceklerdir. Bu, SMTP oturumu sırasında DSN üretilmeksizin reddilerek başarısız olan postaya izin verir. Dahili MTA'lar bundan sonra yetkilendirme sınaması yapmazlar. Sınırdan başka bir yerde yetkilendirme sınaması yapmak için, iletiyi örgüte aktaran ilk konak saptanmalıdır. Böyle bir saptama için bilginin ileti başlığından çıkarılması zor olduğundan sınırdan başka bir yerde sınama yapılması önerilmez.

10. Güvenlik Değerlendirmeleri

10.1. İşlem Sınırları

Eposta ile ilgili pekçok şey gibi, kötü niyetlilerin protokolü hizmet reddi (DoS) saldırıları için bir bulvar olarak kullanabileceği bazı yöntemler vardır. Burada anahatlarıyla ele alınacak olan işlem sınırları şu tür saldırılardan korunmak için tasarlanmıştır:

- Kötü niyetli biri, mağdurun alanına atıflarda bulunan bir SPF kaydı oluşturabilir ve farklı SPF istemcilerine çok sayıda posta gönderebilir; bu SPF istemcileri bir hizmet reddi saldırısı oluştururlar. Aslında, SMTP oturumunda DNS sorgularında kullanılandan daha az bayt kullanılmasını sağlayarak, SPF istemcileri saldırganın band genişliğini arttırmakta kullanılmış olurlar.

- DNS sorgularının sayısını sınırladığı varsayılan `check_host()` gerçeklenimlerinin olduğu yerlerde, kötü niyetli alanlar posta gönderdikleri zaman, hedeflerinde boş hesaplama çabasına yol açarak bu sınırların aşılmasına sebep olan kayıtlar yayınlayabilirler. Kötü niyetli alanlar ayrıca, bazı gerçeklenimlerin üşırı bellek ve işlemci kullanmasına veya hataların tetiklenmesine yol açan SPF kayıtları tasarlayabilirler.

- Kötü niyetli alanlar, geniş çaplıa meşru posta konaklarından geliyormuş gibi görünen büyük hacimde posta gönderebilirler. Bu meşru makineler ilgili kayıtları almak isterken aşırı bir DNS yükü oluşmasına sebebiyet verirler.

Bunlardan dolayı, SPF kaydında bir üçüncü tarafa atıfta bulunulması durumu bir hizmet reddi saldırısı için en kolay istismar edilen durumdur. Sonuç olarak, tek başına bir posta sunucusu için makul görünebilen sınırlar, çok sayıda konak bir araya geldiğinde kabul edilemez miktarda band genişliği harcanmasını sebep olabilir. Bu bakımdan, işlem sınırlarının oldukça düşük tutulmasına ihtiyaç duyulur.

SPF gerçeklenimleri, DNS sorgusuna yol açan mekanizmaların ve değiştiricilerin sayısını SPF sınaması başına en fazla 10 sorgu olabilecek şekildi sınırlamalıdır. Bunlara, kullanımları ek sorgulara yol açan "include" mekanizması ve "`redirect`" değiştiricisi dahildir. Bir sınama sırasında bu miktar aşılırsa, bir "`PermError`" dönmelidir *ZORUNLU*. "`redirect`" değiştiricisinden başka "`include`", "`a`", "`mx`", "`ptr`" ve "`exists`" mekanizmaları da bu sınırla ilgilidir. "`all`", "`ip4`" ve "`ip6`" mekanizmaları DNS sorgusu gerektirmezler ve dolayısıyla bu sınırla ilgili sayıya dahil edilmezler. "`exp`" değiştiricisi de bu sayıya dahil edilmez, çünkü bunun DNS sorgusu SPF kaydı değerlendirildikten sonra yapılır.

"`mx`" ve "`ptr`" mekanizmaları veya `%{p}` makrosu değerlendirilirken 10'dan fazla MX ve PTR kaydı sorgusu ve sınaması yapılamaması için bir sınırlama olmalıdır *ZORUNLU*.

SPF gerçeklenimleri, DNS sorgularından sağlanacak toplam veri miktarını sınırlamalıdırlar *ÖNERİ*. Örneğin, TCP üzerinden DNS veya EDNS0 mümkün olduğunda, aşırı band genişliği veya bellek kullanımından veya hizmet reddi saldırılarından kaçınmak için ne kadar veri kabul edilebileceği ile ilgili açıkça bir sınırlama koymak ihtiyacı ortaya çıkabilir.

MTA'lar veya işlemciler ayrıca, `check_host()` işlevinin işlem yapma süresine bir sınırlama getirebilirler. Böyle bir sınırlamanın en azından 20 saniyelik bir süre sağlaması gerekir *ÖNERİ*. Bu sınır aşıldığında, sınama sonucu "`TempError`" olmalıdır *ÖNERİ*.

Kayıt yayınlayan alanlar "`include`" mekanizması sayısını ve "`redirect`" değiştiricisi zincirini olası en düşük miktarda tutmaya çalışmalıdırlar *ÖNERİ*. Alanlar ayrıca, bir kaydın değerlendirilme ihtiyacını ortaya çıkaran DNS bilgisi mitarını da azaltmaya çalışmalıdırlar *ÖNERİ*. Bu, daha az DNS bilgisi gerektiren yönergeler seçilerek ve SPF kayıtlarına ucuz maliyetli mekanizmalar yerleştirilerek yapılabilir.

Örneğin, şöyle bir alan ayarlaması yapılmış olsun:

```
example.com.      IN MX   10 mx.example.com.
mx.example.com.   IN A    192.0.2.1
a.example.com.    IN TXT  "v=spf1 mx:example.com -all"
b.example.com.    IN TXT  "v=spf1 a:mx.example.com -all"
c.example.com.    IN TXT  "v=spf1 ip4:192.0.2.1 -all"
```

"a.example.com" alanı için `check_host()` işlevinin değerlendirmesi, "example.com" için `MX` kayıtlarını ve ardından listelenen konaklar için `A` kayıtlarını gerektirir. "b.example.com" için yapılan değerlendirme ise, sadece `A` kayıtları gerektirir. "c.example.com" için ise hiçbir şey gerekmez.

Bununla birlikte, yönetimsel değerlendirmeler sözkonusu olabilir: "ip4" yerine "a" kullanımı konakların yeniden numaralanmasını kolaylaştırır. "a" yerine "mx" kullanmak da posta konaklarında kolayca değişiklik yapılabilmesini sağlar.

10.2. SPF Yetkilendirmeli Eposta Yanlış Kimlikler İçerebilir

"MAIL FROM" ve "HELO" kimlikleri ile ilgili yetkilendirmeye olabildiğinden daha fazla anlam yüklemeye çalışılmamalıdır. Alanın SPF kaydı gönderen konağı yetkilendirdiğinden ve ileti diğer kimlikleri başlığında listeleyebildiğinden, kötü niyetli bir göndericinin SPF tarafından kullanılan kimliklerde kendi alanını kullanarak bir ileti teslim etmeye çalışması mümkündür. Kullanıcı veya MUA, yetkili kimliğin diğer varlığı bilinen kimliklerle (örn, From: başlık alanında) eşleşip eşleşmediğine dikkat etmedikçe, kullanıcı güvenlik konusunda bir yanlışa düşebilir.

10.3. Taklit Edilmiş DNS ve IP Verisi

Kötü niyetli kişiler bu protokolü, `check_host()` işlevinin altını oyacak şekilde iki bakımdan istismar edebilirler:

- `check_host()` değerlendirmesi önemli derecede DNS'ye bağlıdır. Bir saldırgan, DNS alt yapısına saldırıp `check_host()` işlevinin taklit DNS verisi görmesine ve yanlış sonuçlar döndürmesine sebep olabilir. Asıl alan kaydı "`Fail`" ile sonuçlanacak bir `<ip>` değeri için "Pass" döndürülmesini sağlayabilir. DNS zayıflıkları ile ilgili bilgi edinmek için [*RFC3833*]'e bakınız.
- İstenci IP adresi olarak `<ip>`'nin doğru olduğu varsayılır. Saldırgan TCP sıra numaralarını taklit ederek postanın bir alan için yetkilendirilmiş bir konaktan geliyormuş gibi görünmesini sağlayabilir.

10.4. Çapraz–Kullanıcı Sahtekarlığı

Tanımı gereği, SPF kuralları alan isimleri ile yetkili konakları eşler, eposta adresleri ile yetkili kullanıcıları eşlemez. "l" makrosu, belli eposta adresleri için yetkili konakları tek tek tanımlayacak bir yol sağlasa da (bkz, *Makrolar* (sayfa: 20)), belli eposta adreslerinin aynı konağın bireysel kullanıcıları tarafından kullanıldığını SPF üzerinden doğrulamak genelde imkansızdır.

Posta hizmetleri ve onların MTA'ları doğrudan doğruya çapraz–kullanıcı sahtekarlığından korunabilir: SMTP AUTH'a ([*RFC2554*]) dayanarak, kullanıcılar sadece kendi denetimleri altındaki eposta adreslerini kullanmaya zorlanmalıdırlar ([*RFC4409*]'un 6.1. bölümüne bakınız). Başka bir anlamda kullanıcıların tek tek kimlik doğrulaması PGP ([*RFC2440*]) veya S/MIME ([*RFC3851*]) gibi bir ileti şifrelemesi ile yapılabilir.

10.5. Güvenilmez Bilgi Kaynakları

SPF, üçüncü şahıslar tarafından sağlanan bilgi kaynaklarını kullanır: "HELO" alan adı, "MAIL FROM" adresi ve SPF kayıtları gibi. Bu bilgi daha sonra "Received–SPF:" izleme alanında alıcıya aktarılır ve bir ihtimal, bir SMTP red iletisi biçiminde istemcinin MTA'sına döndürülür. Bu bilginin geçersiz karakterler ve aşırı uzunluktaki satırlar bakımından sınanması gerekir.

Yetkilendirme sınaması başarısız olduğunda, red yanıtında bir izahat dizgesi bulunabilir. Hem alıcının hem de reddedilen göndericinin bu izahatın alıcı tarafından değil, SPF kaydının yayıncısı tarafından sağlandığından haberdar edilmeleri gerekir. Bu izahat kötü niyetli URL'ler içerebileceği gibi taciz edici veya yanıltıcı olabilir.

Böyle iletiler göndericisine döndüğünden ve izahat dizgeleri göndericinin ta kendisi tarafından iddia olunan kimlikteki alan tarafından yayınlanan gönderici kurallarına göre geldiğinden bu belki de göründüğünden daha az kaygı verici olabilir. DSN asıl göndericiden başkasına yönlenmediği sürece kötü niyetli izahat dizgelerini gören kişiler, iletilerinin, böyle dizgeleri kendi SPF kayıtlarında yayınlayan alanlardan gelmesi gerektiğini iddia eden kişiler olacaktır. Uygulamada ise, DSN'ler yanlış yönlenebilir; bir MTA bir postayı kabul ettikten sonra sahte bir adrese bir DSN üretebilir veya bir eposta yönlendiricisi DSN'yi geriye özgün göndericisine yönlendirmeyebilir.

10.6. Mahremiyetin İfşası

SPF kayıtlarının sınanması DNS sorgularının alan sahibine gönderilmesine sebep olur. Bu DNS sorguları, özellikle "`exists`" mekanizmasından kaynaklanmışlarsa, epostayı gönderen ve epostanın gönderildiği MTA hakkında bilgi içerebilirler. Bu noktada gizlilikle ilgili bazı endişeler devreye girebilir; bunlar, yerel kanunlara ve alan sahibi ile epostayı gönderen kişi arasında ilişkiye az veya çok bağlı konular olabilir.

11. Teşekkür

Bu belge geniş ölçüde Meng Weng Wong ve Mark Lentczner'in çalışmasına dayanır. Bu bölümün devamında bahsedildiği gibi bu belgeye çok kişi destek olduğu halde yazım ve düzenleme büyük ölçüde Meng ve Mark'tan kaynaklanır.

Bu tasarımın Hadmut Danisch'in [*RMX*]'ine ve Gordon Fecyk'in [*DMP*]'sine ebeveynlik borcu bulunmaktadır. Bir DNS kaydının bir eposta adresinin meşruluğunu sınamakta kullanılması fikri, David Green [*Green*] ve Paul Vixie'nin [*Vixie*] (Jim Miller'ın tavsiyelerine dayanarak) namedroppers postalama listesindeki iletilerine dayanır.

Philip Gladstone, dilin ifade gücünü katlayarak ve kullanıcıya ve IP'ye göre sorguları mümkün kılarak belirtime makro kavramı ile destek oldu.

Yazarlar ayrıca, bu tasarımın geliştirilmesine destek olan yüzlerce kişiye tet tek teşekkür etmek isterdi. Hepsini yazmak çok uzun olurdu, ama onları şöyle toparlamak mümkün:

spf–discuss postalama listesindekiler.
SPAM–L postalama listesindekiler.
RTF ASRG postalama listesindekiler.
IETF MARID postalama listesindekiler.
#perl kanalındakiler.

12. IANA Değerlendirmeleri

12.1. DNS Kayıt türü olarak `SPF`

IANA, DNS Parametreleri Siciline 99 koduyla `SPF` özkaynak kaydı türünü yeni bir Özkaynak Kaydı (RR) Türü ve Qtype olarak atamıştır.

12.2. "`Received-SPF:`" Posta Başlığı Alanı

[*RFC3864*]'e göre, "`Received-SPF:`" başlık alanı IANA Kalıcı İleti Başlık Alanı Siciline eklenmiştir. Aşağıda sicil kaydının bir örneği bulunmaktadır:

Başlık alanı ismi: Received–SPF
Uygulanabileceği protokol: posta ([*RFC2822*])
Durumu: Deneysel
Yazar/Değişiklik Denetleyici: IETF
Belirtim belgesi: RFC 4408
İlgili bilgi:
Önerilen değişiklikler ve bu alana eklemeler için SPF Konseyi gözden geçirmesinin istenmesi tavsiye edilir. SPF Konseyi hakkında bilgi edinmek için `http://www.openspf.org/Council/` adresine bakınız.

13. Kaynakça

13.1. Uyulması zorunlu Olanlar

- [RFC1035]
  Alar adları – gerçeklenim ve belirtim -- ***Domain names – implementation and specification*** -- **Mockapetris, P.** -- STD 13, RFC 1035 -- Kasım 1987
- [RFC1123]
  Genel Ağ Konakları için Gereksinimler – Uygulama ve Destek -- ***Requirements for Internet Hosts – Application and Support*** -- **Braden, R.** -- STD 3, RFC 1123 -- Ekim 1989

- [RFC2119[B95]]
  RFC'lerde Gereksinim Seviyelerini Belirtmek için Kullanılan Anahtar Sözcükler -- ***Key words for use in RFCs to Indicate Requirement Levels*** -- **Bradner, S.** -- BCP 14, RFC 2119 -- Mart 1997
- [RFC2821[B96]]
  Basit Posta Aktarım Protokolü (SMTP) -- ***Simple Mail Transfer Protocol*** -- **Klensin, J.** -- RFC 2821 -- Nisan 2001
- [RFC2822[B97]]
  Genel Ağ İleti Biçimi -- ***Internet Message Format*** -- **Resnick, P.** -- RFC 2822 -- Nisan 2001
- [RFC3464]
  Teslimat Durum Bildirimleri için Genişletilebilir bir İleti Biçimi -- ***An Extensible Message Format for Delivery Status Notifications*** -- **Moore, K. ve G. Vaudreuil** -- RFC 3464 -- Ocak 2003
- [RFC3513]
  Genel Ağ Protokolü 6. Sürüm (IPv6) Adresleme Mimarisi -- ***Internet Protocol Version 6 (IPv6) Addressing Architecture*** -- **Hinden, R. ve S. Deering** -- RFC 3513 -- Nisan 2003
- [RFC3864]
  İleti Başlık Alanlarının Kayıt Yordamları -- ***Registration Procedures for Message Header Fields*** -- **Klyne, G., Nottingham, M., and J. Mogul** -- BCP 90, RFC 3864 -- Eylül 2004
- [RFC3986]
  Tektip Özkaynak Betimleyici (URI): Soysal Sözdizimi -- ***Uniform Resource Identifier (URI): Generic Syntax*** -- **Berners-Lee, T., Fielding, R. ve L. Masinter** -- STD 66, RFC 3986 -- Ocak 2005
- [RFC4234[B98]]
  Sözdizimi Belirtimleri için Arttırımlı BNF: ABNF -- ***Augmented BNF for Syntax Specifications: ABNF*** -- **Crocker, D. ve P. Overell** -- RFC 4234 -- Ekim 2005
- [US–ASCII]
  Bilgi Değişimi için Amerikan Kodu, X3.4 -- ***USA Code for Information Interchange, X3.4*** -- American National Standards Institute (formerly United States of America Standards Institute) -- 1968

13.2. Bilgilendirici Olanlar

- [RFC1034]
  Alan adları – kavramlar ve oluşumlar -- ***Domain names – concepts and facilities*** -- **Mockapetris, P.** -- STD 13, RFC 1034 -- November 1987
- [RFC1983]
  Genel Ağ kullanıcısının Sözcük Dağarcığı -- ***Internet Users' Glossary*** -- **Malkin, G.** -- RFC 1983 -- Ağustos 1996
- [RFC2440]
  OpenPGP İleti Biçimi -- ***OpenPGP Message Format*** -- **Callas, J., Donnerhacke, L., Finney, H. ve R. Thayer** -- RFC 2440 -- Kasım 1998
- [RFC2554]
  Kimlik Kanıtlama için SMTP Hizmet Eklentisi -- ***SMTP Service Extension for Authentication*** -- **Myers, J.** -- RFC 2554 -- Mart 1999
- [RFC3696]
  İsimleri Sınamak ve Dönüştürmek için Uygulama Teknikleri -- ***Application Techniques for Checking and Transformation of Names*** -- **Klensin, J.** -- RFC 3696 -- Şubat 2004

- [RFC3833]
  Alan Adı Sisteminin (DNS) Evre Çözümlemesi -- ***Threat Analysis of the Domain Name System (DNS)*** -- **Atkins, D. ve R. Austein** -- RFC 3833 -- Ağustos 2004

- [RFC3851]
  Güvenli/Çok Amaçlı Genel Ağ Posta Eklentileri (S/MIME) Sürüm 3.1 İleti Belirtimi -- ***Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*** -- **Ramsdell, B.** -- RFC 3851 -- Temmuz 2004

- [RFC4409]
  Posta için İleti Arzı -- ***Message Submission for Mail*** -- **Gellens, R. ve J. Klensin** -- RFC 4409 -- Nisan 2006

- [RMX]
  Hafif gönderici yetkilendirmesi için DNS RMX özkaynak kaydı türü -- ***The RMX DNS RR Type for light weight sender authentication*** -- **Danish, H.** -- Çalışma Sürüyor

- [DMP]
  Tasarlanmış Postacılar Protokolü -- ***Designated Mailers Protocol*** -- **Fecyk, G.** -- Çalışma Sürüyor

- [Vixie]
  MAIL FROM'ın İnkarı -- ***Repudiating MAIL FROM*** -- **Vixie, P.** -- 2002

- [Green]
  Alan Yetkilendirmeli SMTP Postası -- ***Domain–Authorized SMTP Mail*** -- **Green, D.** -- 2002

A. Toplu ABNF

Bu bölüm uyulması zorunlu bölümlendendir ve önceki metindeki ABNF dizilimleri ile ilgili her çelişki bu dilbilgisinin yardımıyla çözümlenir.

ABNF gösterimi için [*RFC4234*]'e bakınız. Bu ABNF tanımına göre, dizgesel sabitlerin (tırnak içine alınmış olanlar) harf büyüklüğüne duyarsız oluşuna lütfen dikkat ediniz. Yani, "mx" ile "mx", "MX", "mX" ve "Mx" eşleşir.

```
kayıt             = sürüm terimler *BOŞLUK
sürüm             = "v=spf1"

terimler          = *( 1*BOŞLUK ( yönerge / değiştirici ) )

yönerge           = [ niteleyici ] mekanizma
niteleyici        = "+" / "-" / "?" / "~"
mekanizma         = ( tümü / dahili
                    / A / MX / PTR / IP4 / IP6 / exists )

tümü              = "all"
dahili            = "include"  ":" alan-belirtimi
A                 = "a"      [ ":" alan-belirtimi ] [ çifte-cidr-uzun ]
MX                = "mx"     [ ":" alan-belirtimi ] [ çifte-cidr-uzun ]
PTR               = "ptr"    [ ":" alan-belirtimi ]
IP4               = "ip4"      ":" ip4-ağı   [ ip4-cidr-uzun ]
IP6               = "ip6"      ":" ip6-ağı   [ ip6-cidr-uzun ]
mevcut            = "exists"   ":" alan-belirtimi

değiştirici       = sevket / izahat / bilinmeyen-değiştirici
sevket            = "redirect" "=" alan-belirtimi
izahat            = "exp" "=" alan-belirtimi
bilinmeyen-değiştirici = isim "=" makro-dizgesi

ip4-cidr-uzun     = "/" 1*RAKAM
ip6-cidr-uzun     = "/" 1*RAKAM
çifte-cidr-uzun   = [ ip4-cidr-uzun ] [ "/" ip6-cidr-uzun ]

ip4-ağı           = dörtlü "." dörtlü "." dörtlü "." dörtlü
dörtlü            = RAKAM                 ; 0-9
                    / %x31-39 RAKAM       ; 10-99
                    / "1" 2RAKAM          ; 100-199
                    / "2" %x30-34 RAKAM   ; 200-249
                    / "25" %x30-35        ; 250-255
                    ; bilinen noktalı dörtlü gösterim, 192.0.2.0 gibi
ip6-ağı           = <[RFC3513], 2.2. bölüme göre>
                    ; örn, 2001:DB8::CD30

alan-belirtimi    = makro-dizgesi alan-sonu
alan-sonu         = ( "." tepeyafta [ "." ] ) / makro-genleş
tepeyafta         = ( *harfrakam HARF *harfrakam ) /
                    ( 1*harfrakam "-" *( harfrakam / "-" ) harfrakam )
                    ; HRT kuralı artı ek TLD kısıtlamaları
```

```
                    ; (bkz, [RFC3696], 2. Bölüm)

harfrakam         = HARF / RAKAM

izahat-dizgesi    = *( makro-dizgesi / SP )

makro-dizgesi     = *( makro-genleş / makro-sabiti )
makro-genleş      = ( "%{" makro-harfi dönüştürücüler *ayraç "}" )
                    / "%%" / "%_" / "%-"
makro-sabiti      = %x21-24 / %x26-7E
                    ; "%" hariç görünür karakterler
makro-harfi       = "s" / "l" / "o" / "d" / "i" / "p" / "h" /
                    "c" / "r" / "t"
dönüştürücüler    = *RAKAM [ "r" ]
ayraç             = "." / "-" / "+" / "," / "/" / "_" / "="

name              = HARF *( HARF / RAKAM / "-" / "_" / "." )

başlık-alanı      = "Received-SPF:" [AKBOŞ] sonuç KBOŞ [açıklama KBOŞ]
                    [ anah-değer-list ] CRLF

sonuç             = "Pass" / "Fail" / "SoftFail" / "Neutral" /
                    "None" / "TempError" / "PermError"

anah-değer-list   = anah-değer-çifti *( ";" [AKBOŞ] anah-değer-çifti )
                    [";"]

anah-değer-çifti = anahtar [AKBOŞ] "=" ( nokta-atom / tırnaklı-dizge )

anahtar           = "client-ip" / "envelope-from" / "helo" /
                    "problem" / "receiver" / "identity" /
                     mekanizma / "x-" isim / isim

kimlik            = "mailfrom"   ; "MAIL FROM" kimliği için
                    / "helo"     ; "HELO"kimliği için
                    / isim       ; diğer kimlikler

nokta-atom        = <[RFC2822]'ye göre tırnaksız sözcük>
tırnaklı-dizge    = <[RFC2822]'ye göre tırnaklı dizge>
açıklama          = <[RFC2822]'ye göre açıklama dizgesi>
AKBOŞ             = <[RFC2822]'ye göre açıklamalı katlama boşlukları>
KBOŞ              = <[RFC2822]'ye göre katlama boşlukları>
CRLF              = <[RFC2822]'ye göre standart satır sonu dizgeciği>
```

B. Çeşitli Örnekler

Buradaki örnekler aşağıdaki DNS ayarlarına dayandırılmıştır:

```
; İki posta sunuculu bir alan,
; alan adında iki konak ve iki sunucu
```

```
$ORIGIN example.com.
@           MX  10 mail-a
            MX  20 mail-b
            A   192.0.2.10
            A   192.0.2.11
amy         A   192.0.2.65
bob         A   192.0.2.66
mail-a      A   192.0.2.129
mail-b      A   192.0.2.130
www         CNAME example.com.

; İlişkili alan
$ORIGIN example.org.
@           MX  10 mail-c
mail-c      A   192.0.2.140

; Bu adresler için tersinir IP
$ORIGIN 2.0.192.in-addr.arpa.
10          PTR example.com.
11          PTR example.com.
65          PTR amy.example.com.
66          PTR bob.example.com.
129         PTR mail-a.example.com.
130         PTR mail-b.example.com.
140         PTR mail-c.example.org.

; birşeylere ait olmayı istemeyen
; muzip bir tersinir IP alanı
$ORIGIN 0.0.10.in-addr.arpa.
4           PTR bob.example.com.
```

Örnek 1. Basit Örnekler

Bu örnekler, `check_host()` işlevinin "Pass" döndürmesine sebep olan `<ip` değerleri ve example.com için yayınlanması olası çeşitli kayıtlardan oluşmaktadır. `<alan>`'ın "example.com" olduğuna dikkat ediniz.

```
v=spf1 +all
   -- her <ip> geçer

v=spf1 a -all
   -- gönderen konak 192.0.2.10 ve 192.0.2.11 ise posta geçer

v=spf1 a:example.org -all
   -- example.org bir A kaydı içermediğinden
      hiçbir gönderen konak için posta geçmez

v=spf1 mx -all
   -- gönderen konak 192.0.2.129 ve 192.0.2.130 ise posta geçer

v=spf1 mx:example.org -all
   -- gönderen konak 192.0.2.140 ise posta geçer
```

```
v=spf1 mx mx:example.org -all
   -- gönderen konak 192.0.2.129, 192.0.2.130 ve 192.0.2.140
      ise posta geçer

v=spf1 mx/30 mx:example.org/30 -all
   -- 192.0.2.128/30 veya 192.0.2.140/30 içindeki
      her gönderen konak için posta geçer

v=spf1 ptr -all
   -- gönderen konak 192.0.2.65 ise posta geçer
      (ters DNS geçerlidir ve konak example.com içindedir)
   -- gönderen konak 192.0.2.140 ise posta geçmez
      (ters DNS geçerlidir, ama konak example.com içinde değildir)
   -- gönderen konak 10.0.0.4 ise posta geçmez
      (tersinir IP geçersizdir)

v=spf1 ip4:192.0.2.128/28 -all
   -- gönderen konak 192.0.2.65 ise posta geçmez
   -- gönderen konak 192.0.2.129 ise posta geçer
```

Örnek 2. Çok Alanlı Örnek

Bu örnekler etkilerini bu kayıtla ilgili olarak gösterirler:

```
example.org: "v=spf1 include:example.com include:example.net -all"
```

Bu kayıt, eğer example.org'dan gelen postayı aslında example.com ve example.net sunucularından geliyorsa kullanılır. Example.org'un tasarlanmış sunucuları example.com and example.net'in tasarlanmış sunucularının birleşimidir.

```
la.example.org: "v=spf1 redirect=example.org"
ny.example.org: "v=spf1 redirect=example.org"
sf.example.org: "v=spf1 redirect=example.org"
```

Bu kayıtlar bir alanlar kümesinin hepsinin aynı posta sistemini, o sistemin kaydından yararlanarak kullanmasını mümkün kılar. Bu yolla, posta ayarlarında değişiklik yapmak gerektiğinde sadece posta sisteminin kaydının güncellenmesi yeterli olur. Bu alanların kayıtları hiçbir zaman değişmez.

Örnek 3. DNSBL Tarzı Örnek

Farzedelim ki, yukarıda listelenmiş alan kayıtlarına ek olarak bunlar da olsun:

```
$ORIGIN _spf.example.com.  mary.mobile-users                    A
127.0.0.2 fred.mobile-users                    A 127.0.0.2
15.15.168.192.joel.remote-users     A 127.0.0.2
16.15.168.192.joel.remote-users     A 127.0.0.2
```

Aağıdaki kayıtlar postalarını keyfi sunuculardan veya kişisel sunucularından gönderen kullanıcıları açıklamaktadır.

example.com:

```
v=spf1 mx
       include:mobile-users._spf.%{d}
       include:remote-users._spf.%{d}
       -all
```

mobile–users._spf.example.com:

```
v=spf1 exists:%{l1r+}.%{d}

remote-users._spf.example.com:

v=spf1 exists:%{ir}.%{l1r+}.%{d}
```

Örnek 4. Çok Gereksinimli Örnek

Diyelim ki, gönderici kurallarınız, hem IP adreslerinin belli bir aralık içinde kalmasını hem de bu IP'ler için ters DNS kayıtlarının eşleşmesini gerektirsin. Bu çeşitli yollardan yapılabilir, örnek:

```
example.com.            SPF   ( "v=spf1 "
                                "-include:ip4._spf.%{d} "
                                "-include:ptr._spf.%{d} "
                                "+all" )
ip4._spf.example.com.   SPF   "v=spf1 -ip4:192.0.2.0/24 +all"
ptr._spf.example.com.   SPF   "v=spf1 -ptr +all"
```

Bu örnekler "`-include`" mekanizmasının ne kadar kullanışlı olabileceğini, "`+all`" ile biten bir SPF kaydının nasıl çok sınırlayıcı olabileceğini ve De Morgan Kuralının kullanımını göstermektedir.

C. Bu Belge Hakkında

Yazarların Adresleri


```
Meng Weng Wong
   Singapore

   EMail: <mengwong+spf (at) pobox.com>


Wayne Schlitt
   4615 Meredeth #9
   Lincoln Nebraska, NE  68506
   United States of America

   EMail: <wayne (at) schlitt.net>
   URI:   http://www.schlitt.net/spf/
```


Tam telif Hakkı Beyanı

NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Fikri Mülkiyet

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on–line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf–ipr@ietf.org.

Bilgi için

RFC Editor(*B109*) işlevinin mali desteği şu an IETF Yönetimsel Destek Etkinliği (IETF Administrative Support Activity – IASA) tarafından sağlanmaktadır.

Notlar

Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

(*B1*) ftp://ftp.rfc-«editor.org/in-«notes/bcp/bcp78.txt

(*B3*) http://www.ietf.org/

(*B12*) ../rfc/rfc2821.pdf#rfc2821-«s455

(*B20*) ../rfc/rfc2821.pdf#rfc2821-«appc

(*B52*) ../rfc/rfc2821.pdf#rfc2821-«s5

(*B59*) ../rfc/rfc2821.pdf#rfc2821-«s24

(*B64*) ../rfc/rfc2822.pdf#rfc2822-«s367

(*B77*) ../rfc/rfc2821.pdf#rfc2821-«s3a

(*B95*) ../rfc/rfc2119.pdf

(*B96*) ../rfc/rfc2821.pdf

(*B97*) ../rfc/rfc2822.pdf

(*B98*) ../rfc/rfc4234.pdf

(B109) http://www.rfc-«editor.org/

Bu dosya (rfc4408.pdf), belgenin XML biçiminin TEXLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

17 Ocak 2007