Informazioni sul record SPF CES

Sommario

Introduzione

Questo documento descrive come funziona il record SPF consigliato da Cisco per i clienti ospitati CES.

Requisiti

1. Comprensione di base del funzionamento del DNS.

Importanza delle macro SPF

Il record consigliato da Cisco utilizza una macro SPF definita nella RFC7208 sezione 7. In questo caso, la macro viene utilizzata per ridurre la quantità di ricerche DNS necessarie per consentire agli accessori CES di superare la verifica SPF. Questa operazione è importante perché SPF limita a 10 la quantità di ricerche DNS per verifica SPF in base alla sezione 4.6.4 della RFC7208. Se sono richieste più di 10 ricerche DNS, il risultato della verifica SPF sarà premerror. Questo potrebbe non essere un problema, ma se vengono forniti più ESA ospitate, saranno necessarie più ricerche DNS.

Èpossibile aggiungere l'indirizzo IP di ciascuna ESA ospitata al record SPF. Non sono necessarie ulteriori ricerche DNS durante la verifica di SPF. Tuttavia, lo svantaggio è che è necessario cambiare il record SPF ogni volta che una nuova ESA viene predisposta o quando cambia l'indirizzo IP di un'ESA esistente. Il record SPF consigliato da Cisco non richiede alcuna gestione da parte dell'utente dopo l'aggiunta del record.

Spiegazione del record SPF

Di seguito è riportato un esempio del record SPF:

```
$ dig acme.com txt +short
"v=spf1 exists:%{i}.spf.acme.iphmx.com ~all"
```

> **Nota:** *La parte "acme" di questo record SPF è considerata il nome di allocazione. Il cluster ospitato dal Servizio di registrazione unificato ha un nome di allocazione univoco e deve essere utilizzato al posto di "acme" se si aggiunge questo record SPF al DNS.*

In questo record SPF viene utilizzata la macro "%{i}". Questa macro viene utilizzata come variabile sostituita dall'indirizzo IP dell'host che si connette quando viene eseguita la verifica SPF. Ad esempio, se l'host di invio è 192.168.0.1, il nome host "%{i}.spf.acme.iphmx.com" si espanderà a "192.168.0.1.spf.acme.iphmx.com".

Il meccanismo "esiste" è definito nella sezione 5.7 della RFC7208 e corrisponderà se il nome host "%{i}.spf.acme.iphmx.com" ha un record A in DNS. Ad esempio, supponiamo che 192.168.0.1 sia di nuovo l'host di invio. Il nome host "%{i}.spf.acme.iphmx.com" verrà espanso a "192.168.0.1.spf.acme.iphmx.com" e l'host verificante eseguirà la seguente ricerca DNS:

```
$ dig 192.168.0.1.spf.acme.iphmx.com a +short
127.0.0.2
```

> **Nota:** Il dominio iphmx.com è gestito da Cisco. Per questo motivo, solo Cisco può aggiungere, rimuovere o modificare i record DNS per il dominio come il record precedente. Ciò significa che non è necessario aggiungere questi record ogni volta che vengono forniti nuovi ESA al cluster CES. È responsabilità di Cisco verificare che questi documenti siano aggiunti e corretti.

Poiché è stato restituito l'indirizzo IP 127.0.0.2, il meccanismo esistente corrisponderebbe e il risultato della verifica SPF verrà passato.

Si supponga che l'host di invio sia 10.0.0.1. Il nome host "%{i}.spf.acme.iphmx.com" verrà espanso a "10.0.0.1.spf.acme.iphmx.com" e l'host di verifica eseguirà la ricerca DNS seguente:

```
$ dig 10.0.0.1.spf.acme.iphmx.com a +short
$
```

Poiché non è stato restituito alcun risultato, il meccanismo esistente non corrisponderebbe e il risultato della verifica SPF sarebbe soft fail.

Ulteriori informazioni

La tecnologia SPF può essere complessa a seconda della quantità di host che si desidera autorizzare per l'inoltro della posta per il dominio. Se gli accessori ospitati dal CES sono gli unici host autorizzati a inoltrare la posta per il dominio, il record precedente funziona correttamente. In caso contrario, sarà necessario modificare il record SPF fornito in modo che autorizzi tutti gli host necessari.

Se si dispone di un record SPF esistente, è possibile aggiungere al record SPF "exist:%{i}.spf.acme.iphmx.com".