Understanding the CES SPF Record

Contents

Introduction

This document describes how the SPF record recommended by Cisco for CES hosted customers functions.

Requirements

1. Basic understanding of how DNS works.

Importance of SPF macros

The record that is recommended by Cisco uses a SPF macro defined in RFC7208 Section 7. The macro is used in this case to reduce the amount of DNS lookups that would be required to allow the CES appliances to pass SPF verification. This is important because SPF limits the amount of DNS lookups per SPF verification to 10 according to RFC7208 Section 4.6.4. If more than 10 DNS lookups are required, the SPF verification result will be permerror. This may not be a problem but if more hosted ESA's are provisioned, more DNS lookups will be required.

You could add the IP address of each hosted ESA to the SPF record. This won't require any additional DNS lookups during SPF verification. However, the downside to this is you have to change the SPF record whenever any new ESA's are provisioned or when the IP address of an existing ESA changes. The SPF record Cisco recommends doesn't require any management from you after the record is added.

SPF record explained

The following is an example of the SPF record:

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

> **Note**: *The "acme" portion of this SPF record is considered the allocation name. Your CES hosted cluster has a unique allocation name and should be used in place of "acme" if you add this SPF record to DNS.*

In this SPF record, the macro "%{i}" is used. This macro is used as a variable that is replaced by the IP address of the connecting host when SPF verification takes place. For example, if 192.168.0.1 is the sending host, the hostname "%{i}.spf.acme.iphmx.com" would expand to "192.168.0.1.spf.acme.iphmx.com."

The "exists" mechanism is defined at RFC7208 Section-5.7 and will match if the hostname "%{i}.spf.acme.iphmx.com" has an A record in DNS. For example, let's say 192.168.0.1 is the sending host again. The hostname "%{i}.spf.acme.iphmx.com" would expand to "192.168.0.1.spf.acme.iphmx.com" and the verifying host would do the following DNS lookup:

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

> **Note**: The domain iphmx.com is managed by Cisco. Because of that, only Cisco can add/remove/modify DNS records for that domain like the record above. What this means for you is you don't need to add these records anytime new ESA's are provisioned to your CES cluster. It's the responsibility of Cisco to ensure these records are added and correct.

Because the IP address 127.0.0.2 was returned, the exists mechanism would match and the SPF verification result would be pass.

Let's say the sending host is 10.0.0.1. The hostname "%{i}.spf.acme.iphmx.com" would expand to "10.0.0.1.spf.acme.iphmx.com" and the verifying host would do the following DNS lookup:

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

Because no result was returned, the exists mechanism wouldn't match and the SPF verification result would be softfail.

Additional information

SPF technology can be complex depending on the amount of hosts that you would like to authorize to relay mail for your domain. If the CES hosted appliances are the only hosts authorized to relay mail for your domain, then the above record works great for you. Otherwise, you will have to modify the SPF record we provide so that it will authorize all hosts that you need it to.

If you have an existing SPF record, "exists:%{i}.spf.acme.iphmx.com" can be added to that SPF record.