Creating a Sender Policy Framework record

The number of phishing and spam attacks on email systems continue to rise. While many email security standards have been developed to help prevent such attacks, this article focuses on the SPF security standard: what it is, how to correctly implement it, and why it is so important in email threat protection.

SPF record

A Sender Policy Framework (SPF) record is an email security standard that defines the authorized mail servers for a particular domain. An SPF record is published by the domain administrator as part of the domain's DNS records. A domain can have only one SPF record.

Because an SPF record includes the domain's list of servers that are allowed to send emails, it plays a critical role in preventing spam and phishing attacks. When carrying out these attacks, the sender disguises the email address from which they are actually sending the emails, a technique known as spoofing. So it appears to the recipient that the email came from a known and trusted domain.

SPF record benefits

A properly written SPF record provides key security benefits for an email recipient and the domain.

Inbound email servers can access a domain's SPF record to verify that incoming email was sent from a server authorized by the domain. An inbound email server may have its own policies to protect recipients against attacks based on results found in the SPF record.

For example, if the sending mail server's address doesn't match an address in the domain's SPF record, the inbound email server may identify an email as spam or bounce it back to the sender.

An SPF record that is correctly written for your domain greatly improves the probability your domain's emails will be delivered successfully. Also, it helps protect against malicious emails being sent from your domain.

Importance of SPF records for Datto SaaS Defense

Datto SaaS Defense is very proficient at preventing phishing and spam attacks the first time they are encountered. First, it checks that the incoming email has the full organization domain in its return-path address. Then, SaaS Defense accesses the domain's SPF record to verify the sending server is authorized. SaaS Defense considers any discrepancy as a definitive sign of email spoofing.

The importance of a correctly configured SPF record is evident in a common business practice. Many organization's use a third-party service to send emails on behalf of the organization. The third-party domains from which these emails are sent must be identified in the organization's SPF record, or the emails may be treated as BEC phishing attempts.

SaaS Defense treats emails as BEC phishing attempts when:

- The sender's domain indicated in the From address is identical to the client's domain.
- The client's SPF record returned a non-pass result. See the "Common SPF record errors" on page 10 section at the end of this article.

Therefore, depending on whether Datto SaaS Defense is operating in Prevention or Monitoring mode, it blocks or flags these emails, even though the emails may be legitimate.

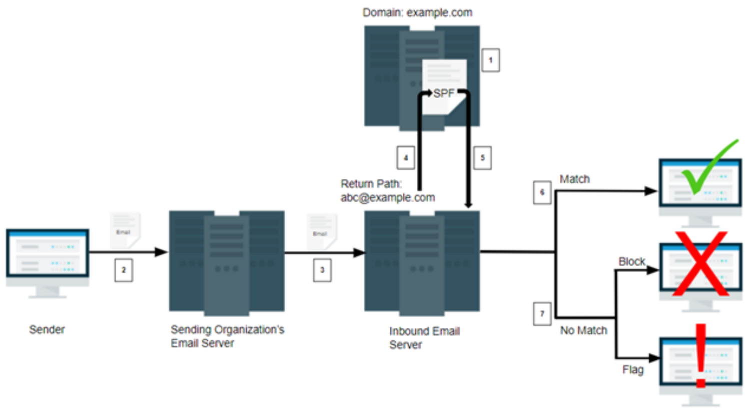
> EXAMPLE
> The Testsite company uses a third-party company, IT Anywhere, to provide customer support for its clients. In emails sent by IT Anywhere, the Testsite company's domain, testsite.com, is used in the From address, as in ITAnywhere@testsite.com. The IT Anywhere servers from which the emails are sent must be configured in testsite.com's SPF record. Otherwise, SaaS Defense will determine that the emails are BEC phishing attempts.

> IMPORTANT To prevent legitimate emails from being blocked, it is essential that each client creates an SPF record correctly for its domain.

SPF record process

The following steps describe the SPF process (and illustrated below):

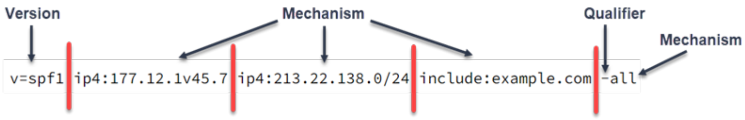
1. The domain administrator creates the SPF record and publishes it as part of the domain's DNS records.
2. The sender authors and sends the email.
3. The sending organization's email server transfers the email to the inbound email server.
4. The inbound mail server uses the return-path domain indicated in the email header to look up the domain's DNS records.
5. The inbound mail server compares the IP address of the mail sender with the IP addresses authorized in the SPF record. Evaluation of the IP addresses within the SPF record is done left to right.
6. If the IP address of the mail sender is the same as (matches) one of the IP addresses in the SPF record, the inbound mail server delivers the email to the intended recipient.
7. If the IP address of the mail sender does not match one of the IP addresses in the SPF record, the inbound mail server uses the rules specified in the domain's SPF record and either blocks or flags the message.



SPF record syntax

An SPF record includes the following elements (identified in image below):

- Version: An SPF record must start with `v=spf1`. Current version is version 1.
- Mechanism: A mechanism is a rule identifying a specific email server or servers to include in the SPF record. The inbound mail server looks for the mechanism that matches the IP address of the mail sender. An SPF record can include many mechanisms, each separated by a space.
- Qualifier: A qualifier identifies how the inbound mail server should process emails sent by a server not defined in the domain's SPF. In other words, an email from a server that fails the SPF verification.



```
v=spf1 ip4:177.12.1v45.7 ip4:213.22.138.0/24 include:example.com -all
```

The following sections describe mechanisms and qualifiers in depth.

> NOTE For more information about creating an SPF record, see the Microsoft article Set up SPF to prevent spoofing.

Common mechanisms

There are various mechanisms that you can use to define the servers in your SPF record. The table describes common mechanisms and provides examples.

Mechanism	Examples
ip4: Specifies an Internet Protocol version 4 server address as a valid email sending source. Multiple ip4 addresses can be included. A prefix-length can be specified to define an IPv4 network range of servers to include in the SPF record.	Syntax options: • `ip4:`*`<ip4-address`* Example: `v=spf1 ip4:123.456.0.12 -all` • `ip4:`*`<ip4-address>/<-prefix-length>`* Example: `v=spf1 ip4:123.456.0.1/16 -all` Means any IP address between 123.456.0.1 and 123.456.255.255 is authorized. If a prefix-length is not given, /32 is assumed (identifying a single host address) Recommended not to include prefix length greater than /16.
mx: Indicates that the domain's inbound receiving servers are authorized to send emails as well. All the A records in all of the domain's MX records are tested in order of MX priority. The A records must match the mail sender's IP address exactly. If a prefix-length is indicated, each IP address returned by the A lookup will be expanded to its corresponding CIDR prefix.	Syntax options: • `mx:` domain not specified, current domain is used • `mx/`*`<prefix-length>`* Example: `v=spf1 mx/24 -all` • `mx:`*`<domain>`* Example: `v=spf1 mx:example.com -all` • `mx:`*`<domain>/<prefix-length>`* Example: `v=spf1 mx:example.com/24 -`

Mechanism	Examples
The sender's IP is sought within that subnet.	`all`
all: Defines the policy for all other email sources that are not defined in the SPF. A qualifier (-, ˜, +, ?) indicates the strictness in which the inbound server should process an email from a non-authorized server: • -all: The (-) qualifier means fail. Emails from non-authorized servers should be blocked, not delivered. • ˜all: The (˜) qualifier means softfail. Emails from non-Inzed servers should be delivered, but flagged as suspicious (e.g., junk). • +all: The (+) qualifier means pass. Emails from any servers should be delivered. *Not recommended to use this qualifier.* • ?all: The (?) qualifier means neutral, there is no policy. *Not recommended to use this qualifier.* The all mechanism is required at the end of your SPF record.	Examples: • `v=spf1 mx -all` Indicates inbound mail servers should allow emails from the domain’s MX servers, block all others. • `v=spf1 mx ~all` Indicates inbound mail servers should allow emails from the domain’s MX servers, allow but flag all others.

Additional mechanisms

Additional, less common mechanisms you can use to define a server in an SPF record are described in the following table.

Mechanism	Examples
ip6: Specifies an Internet Protocol version 6 server address as a valid email sending source. Multiple ip6 addresses can be included. A prefix-length can be specified to define an IPv6 network range of servers to include in the SPF record.	Syntax options: • `ip6:<ip6-address>` Example: `v=spf1 ip6:2001:0db8:0123:4567:89ab:cdef:1234:5678 -all` • `ip6:<ip6-address>/<prefix-length>` Example: `v=spf1 ip6:1080::8:800:200C:417A/96 ~all` Allows any IPv6 address between 1080::8:800:0000:0000 and 1080::8:800:FFFF:FFFF. If a prefix-length is not given, /128 is assumed (identifying a single host address).
a: Indicates that all the A records for the domain are tested. For connections made via IPv6, AAAA records are searched.	Syntax options: • `a` domain not specified, current domain is used Example: `v=spf1 a ~all` • `a/<prefix-length>` Example: `v=spf1 a/24 ~all` • `a:<domain>` Example: `v=spf1 a:example.com ~all` • `a:<domain>/<prefix-length>` Example: `v=spf1 a:example.com/24 ~all`
ptr: The hostname or hostnames for the mail sender's IP address are looked up using PTR queries.	Syntax options: • `ptr` Example: `v=spf1 ptr ~all` Indicates that the current domain allows all its servers to send mail. • `ptr:<domain>` Example: `v=spf1 ptr:example.com`

Mechanism	Examples
Validates that at least one A record for a PTR address matches the sender's IP address. *Not recommended to use this mechanism as it results in expensive DNS lookups*.	`~all` Indicates that any server whose hostname ends in example.com is authorized.
exists: Performs an A record lookup on the given domain name. A match exists as long as the domain name resolves to any address.	Syntax options: `exists:<domain>` Example: `v=spf1 exists:example.com ~all` Indicates if a server source is found, regardless of the address, a match results.
include: Specifies that the SPF record from another domain or sub domain is included in your SPF record. Use this mechanism if a third-party service or multiple domains/sub-domains send email on behalf of your domain.	Syntax options: `include:<domain>` Example: `v=spf1 ip4:123.456.0.12 include:example.com ~all` Indicates that in addition to the ip4 address, the SPF record also includes the example.com domain's SPF record.

Mechanism	Examples
If the included domain does not have a valid SPF record, the result is a permanent error. Some mail receivers will reject based on a PermError.	

Creating an SPF record

1. Identify the process for publishing the SPF record to your DNS server. You may need to work with your domain's DNS server administrator.
2. Compile a list of all of your domains. Be sure to include inactive domains that don’t send emails in order to protect them from abuse as well.
3. Compile the list of your organization's own mail servers, ISPs, and third-party mail servers.
4. Create your domain SPF record:
   a. Define the SPF version: v=spf1
   b. Identify all of the IP addresses authorized to send emails for your domain.
   c. Use the include mechanism to identify third-party organizations authorized to send emails for your domain.
   d. If necessary, use other applicable mechanisms.
   e. End the record with the all mechanism. Be sure to include the correct qualifier.
5. Publish the SPF record to your DNS server.

SPF record examples

Here are a few SPF record examples using common mechanisms:

- In this example, two of the domain's Internet Protocol version 4 server addresses are authorized. Emails sent by any other servers or IP addresses should be rejected by the inbound server.

```
v=spf1 ip4:111.456.0.10 ip4:102.555.123.10 -all
```

- In the following example, one of the domain's Internet Protocol version 4 server addresses is authorized as well as the domain's mx servers. Emails sent by any other servers or IP addresses should be allowed but flagged as suspicious by the inbound server.

  ```
  v=spf1 ip4:111.456.0.10 mx ~all
  ```

- In this example, the first mx means its mx servers are authorized. The mx:deferrals.example.com syntax indicates a set of servers that resend emails to recipient mail servers who refused a previous delivery attempt.

  ```
  v=spf1 mx mx:deferrals.example.com ~all
  ```

Common SPF record errors

Datto SaaS Defense performs a daily SPF record test for each client's domain. The purpose of the test is to verify that a valid SPF record exists for the domain. Common errors that cause an SPF record to fail the daily test are described below. Verify that your SPF record does not include any of these errors.

Errors	Description
Default SPF Record	This error means that the organization is using a third-party service to send emails on behalf of the organization, but the IP address of the third-party server is not configured in the organization's default SPF record. This may cause SaaS Defense to treat an email sent by the third-party server as a BEC phishing attempt when the email may be legitimate. **To fix this error:** Edit the default SPF record to include the third-party server IP address. IMPORTANT Every organization that uses Microsoft Exchange has a default SPF record. The Default SPF Record error *only* occurs when using a third-party service whose IP address is not configured in the organization's default SPF record.
SPFRecordNotFound	This error applies when one of the following occurs: - The sender's IP address is not found in the SPF record. For example, an email is sent from the testsite.com domain. The sending server's IP address is `4:111.456.0.10`. However, the IP address in not listed in the testsite.com's SPF record.

Errors	Description
	To fix this error: If email should be allowed from the sender's IP address, configure the IP address in your SPF record. - The domain has more than one SPF record or no SPF record at all. One SPF record must exist for each domain. **To fix this error:** Verify that one SPF record exists for the domain.
SPFSyntaxError	This error means the SPF record contains syntax errors. **To fix this error:** Review and correct the syntax errors.
SPFTooManyDNSLookups	This error means the SPF record includes more than 10 SPF records from other domains or sub domains. The `include` mechanism specifies that the SPF record from another domain or sub domain is included in your SPF record. This mechanism is commonly used when a third-party service sends emails on behalf of the organization. **To fix this error:** Reduce the number of `include` mechanisms in your SPF record to 10 or less. One option is to obtain the actual IP addresses of the domain indicated in the `include` mech-

Errors	Description
	anism and replace the mechanism with the addresses.
SPFIncludeLoop	This error means the SPF record includes an SPF record from another domain (or sub domain) but that domain includes the SPF record of the original domain, causing an endless loop. **To fix this error:** Contact the organizations configured in the `include` mechanisms in your SPF record until you determine the organization that has included your SPF record in their SPF record. Work with them to resolve the issue.