All of Government

Secure Government Email SPF Deployment Guide

Issued by

Digital Services branch

Internal Affairs
Te Tari Taiwhenua

New Zealand Government

Contents

1 Document Control

Service Name	Secure Government Email
Author	Matt Oliver, Operations Security Specialist, Department of Internal Affairs
Title	Secure Government Email SPF Deployment Guide
Date and Version	3 November 2025, v1.0
Index Number	AoGSD.SGE.Guidance.2025_249

2 Introduction

The Secure Government Email (SGE) Common Implementation Framework was confirmed late in 2024 with a goal to improve email security standards across the New Zealand Government. This deployment guide complements the Framework through providing examples on how to deploy Sender Policy Framework (SPF) in line with both the framework and to meet the requirements of the New Zealand Information Security Manual (NZISM).

It provides configuration examples covering commonly used platforms and configurations but is not an exhaustive guide. It is recommended Agencies without experience in the deployment of email security tools engage with a provider with expertise in this area.

Services are available for Agencies via the Secure Email Management and Administration service in Marketplace Marketplace | Pae Hokohoko — Infrastructure Managed Services catalogue.

3 NZISM and SGE Framework requirements for SPF

Chapter 15.2 (Email Infrastructure) of the NZISM requires SPF be configured across all domains irrespective of whether those domains are used in association with email. It requires Agencies to use a fail (-all) SPF record, and requires the use of SPF to verify the authenticity of incoming emails.

The SGE Framework maps back to the NZISM and requires:

- All mail sending domains must have an SPF record finishing with -all.
- Blank SPF records with a -all suffix must be configured on non-email enabled domains.
- Inbound emails must be scanned and acted on with SPF*.

*Scanning of inbound emails for SPF compliance is a part of Domain-based Message Authentication, Reporting, and Conformance (DMARC) and is covered in the Secure Government Email DMARC Deployment guide.

4 SPF Configuration

Enabling SPF requires configuration changes in in your domain's DNS environment. Configuring SPF is similar across most platforms, though the exact configuration steps may differ. You need to:

1. Identify all mail sending servers or services sending from your domain.
2. Construct your SPF record.
3. Publish the record in DNS.
4. Test the record.
5. Monitor Email deliverability.
6. Maintain the record.

It is assumed you have the required access and knowledge to configure the required services.

Step 1: Identify all mail sending services on your domain

Deploying SPF with a hardfail (-all) suffix will impact mail deliverability if it is not configured correctly.

You must identify **all** servers or services which send email on behalf of your domain. All major mail sending platforms will have publicly accessible documentation advising of SPF values to use with their services.

The following table assumes the fictitious domain minties.govt.nz uses M365 for sending most of their day-to-day email. They also use an on-site mail server which is listed in their DNS MX record. A monitoring service is used on both IPv4 and IPv6, and they are using an external marketing company to send emails from a marketing subdomain.

Domains	IP Address or SPF value	Service / description
minties.govt.nz	include:spf.protection.outlook.com	M365 sending SPF range as defined by Microsoft.
minties.govt.nz	192.0.2.1	Old mail server specified in DNS MX record.
minties.govt.nz	192.0.2.2	IPv4 monitoring service
minties.govt.nz	2001:db8::1	IPv6 monitoring service
marketing.minties.govt.nz	include:<external-service-SPF-data>	Marketing emails sent from an external platform

Step 2: Construct your SPF record

While it is possible to nest SPF records under most situations you will only have one SPF record per domain and there is a maximum of 10 lookups. Lookups are any type of service which requires a DNS lookup to resolve to an IP address. IPv4 and Ipv6 addresses are not counted in the lookup.

Using the information from step 1 build the required SPF records.

For the main domain minties.govt.nz the record will be:

```
v=spf1 mx ip4:192.0.2.2 ip6:2001:db8::1 include:spf.protection.outlook.com -all
```

mx is used as a lookup to resolve to 192.0.2.1. The ip4 and ip6 addresses are entered for the monitoring service and the address provided by Microsoft is used for M365.

For the subdomain marketing.minties.govt.nz, following best practice, only the marketing service is permitted.

```
v=spf1 include:<include:spf.examplesecuremailprovider.com> -all
```

Step 3: Add TXT Records to your DNS

The following assumes use of the Govt DNS platform, exact steps may vary for other platforms.

Note: Setting an SPF record in DNS is effectively enabling SPF on the domain. Although the framework, and NZISM, require use of the -all suffix, it is recommended you start with ~all at the suffix.

1. Log in to the DNS portal and browse to your domain.
2. Click on the Current tab under DNS Zones.
3. Click on Edit.
4. Click on the + symbol to add a new row.
5. Set the TTL to 3600.*
6. Change the type to TXT.
7. Copy and Paste the record created in step 2.
8. Add a comment or change number if needed for your environment.
9. Click on Publish.
10. Repeat this for other domain records if required.

*3600 seconds for a TTL on an SPF record provides a good balance between DNS caching and flexibility. If you are in the process of making changes perhaps reduce it to 300-900 seconds (5-15 minutes). If you’re in a highly stable environment, like perhaps the external marketing service you may wish to set it out as high as 86,400 seconds (24 hours).

When changing DNS records always allow time for internet propagation. If you have specialist configurations or email security platforms, those services should be specifically checked to ensure propagation.

Step 4: Test your SPF Record

Once DNS records are published, use an external service to check your SPF record is valid. The SPF checker on the MXToolbox supertool provides a useful test. (https://mxtoolbox.com/SuperTool.aspx#)

Enter your domain name and select the SPF Record Lookup. This will return your record and will show it in a green box if validated, or a red box if there are errors. If there are any errors it will list them below.

The most common errors made in SPF records are:

- Too many lookups (max = 10).
- Incorrect ‘include’ statements, for instance including a domain which doesn’t have its own valid SPF record.
- Missing the -all or ~ all at the end of the SPF record.
- Syntax errors in the record like missing spaces, inserted commas or typos.

- Multiple SPF records – you can have only one SPF record per domain.

Step 5: Monitor email deliverability

After enabling SPF with a -all directive, monitor email deliverability by regularly reviewing DMARC reports for your domain.

These reports will show:

- Which IPs are sending mail on your behalf.
- Whether SPF (and DKIM) passed or failed.
- Whether the message aligned with your DMARK policy.

See the Secure Government Email DMARC Deployment Guide for more information.

Step 6: SPF record maintenance

Once SPF is enabled with a -all directive the record will need to be maintained / updated whenever there are email infrastructure changes. This could be for new services coming on board or old services being disestablished. Below are some best practice tasks for SPF record maintenance:

- Establish a Review Schedule

  Review SPF records quarterly or whenever email infrastructure changes.

  Include SPF checks in change management processes for email services.

- Inventory All Sending Services

  Maintain a list of all services that send email on behalf of your domain (e.g., Microsoft 365, marketing platforms, CRM tools).

  Ensure each service is properly included in the SPF record using include: or ip4: mechanisms.

- Check for DNS Lookup Limits

  Use tools like MXToolbox SPF Checker to verify that your SPF record stays within the 10 DNS lookup limit.

  Consolidate or flatten includes if necessary.

- Avoid Deprecated or Risky Mechanisms

  Do not use ptr or overly broad IP ranges.

  Prefer -all (fail) over ~all (soft fail) for stricter enforcement, once confident in coverage.

- Monitor Authentication Results

  Use DMARC reports to monitor SPF pass/fail outcomes for outbound email.

  Review Microsoft 365 Defender message traces for inbound SPF failures.

- Document Changes

  Keep a changelog of SPF updates, including who made the change and why.

  Use version control if managing DNS via infrastructure-as-code.

- Test Before Deploying

Use staging domains or test environments to validate SPF changes before applying them to production.

4.1 Deploying SPF when you have an external mail security service

If you are using an external mail security service which is processing your outbound email, it is that service which will be seen as the sending server. Their IP address or include domain therefore must be contained in your SPF record. This will vary depending on the supplier, with an include statement such as: `include:<spf.examplesecuremailprovider.com>`.

In most cases external mail security services will not alter the mail From addresses in an outbound email. This needs to be confirmed with the supplier. If the service is configured to rewrite addresses it could break alignment (refer to Section 5.3 SPF Alignment).

4.2 Deploying SPF on non-mail-enabled domains

The NZISM requires blank SPF records, with a suffix of -all, be configured on all non-email-enabled domains. This is to force all SPF lookups on the domain to 'fail' rather than to just receive no response.

As these domains are not enabled for email the following SPF record will only have an impact on any spoofed email from the domain. It is designed to be used in conjunction with a blank DKIM record and relevant DMARC policy.

Example DKIM Record:

Name	TTL	Type	Data	Comment
<yourdomainname>	3600	txt	"v=spf1 -all"	Blank SPF record

SPF records do not inherit across subdomains so each subdomain must have its own blank SPF record.

4.3 Moving from SPF ~all to SPF -all

Migrating from SPF ~all to -all is required to comply with the both the NZISM and SGE Framework. This needs to be done with care to avoid disrupting legitimate mail flow. Here is a step by step process:

Step-by-Step SPF Migration: ~all to -all

Step 1: Establish a Baseline

- Review your current SPF record and ensure all legitimate sending services (e.g., Microsoft 365, mail security, MX platforms) are included.
- Example starting record:
- `v=spf1 mx ip4:192.0.2.2 ip6:2001:db8::1 include:spf.protection.outlook.com ~all`

Step 2: Enable DMARC with Reporting

- Publish a DMARC record to collect authentication reports:

```
_dmarc.minties.govt.nz TXT "v=DMARC1; p=none; rua=mailto:dmarc@minties.govt.nz"
```

- This allows you to monitor SPF alignment and failures across all senders. Note the p=none is only given as an example. The framework requires moving to p=reject. Refer to the Secure Government Email DMARC Configuration Guide for more information.

Step 3: Monitor DMARC Reports

- Use a DMARC reporting tool to:
  - Identify senders failing SPF.
  - Confirm that all legitimate sources are passing SPF and aligning with your domain.

Step 4: Audit and Update SPF Record

- Based on DMARC data:
  - Add missing senders.
    Note: Ensure you check each sender is valid before adding them to your record. These reports will also show domains and Ips of attackers spoofing your domain.
  - Remove unused or unauthorised ones.
  - Flatten or optimize includes if you're nearing the 10 DNS lookup limit.

Step 5: Test with ~all

- Keep ~all in place while monitoring for at least 4 weeks.
- Ensure no legitimate mail is failing SPF unexpectedly.

Step 6: Migrate to -all

- Once confident, update your SPF record suffix from ~all to -all:
- This enforces a hard fail for any sender not explicitly authorised.

Step 7: Continue Monitoring

- Keep DMARC reporting active.
- Periodically review SPF and DMARC reports to catch new services or misconfigurations.

Appendix 1 – SPF Description

What is SPF?

SPF is an email authentication protocol defined in RFC7208 designed to detect and prevent email spoofing through allowing administrators to specify which mail servers were authorised to send email on behalf of their domains.

When SPF is used in conjunction with DMARC it also verifies alignment between the “Return Path” (or envelope-from) address with the “From” header in the email.

Here's how SPF works:

1. Domain publishes SPF record: The domain owner adds a DNS TXT record that lists the IP addresses or hostnames allowed to send email on behalf of the domain.
2. Receiving server checks SPF: When an email is received, the recipient's mail server looks up the SPF record of the sender's domain.
3. Validation: The server compares the sending IP address with the list in the SPF record. If it matches, the email passes SPF; if not, it fails.
4. Action on result: Based on the result (pass, fail, softfail, neutral, etc.), the receiving server may accept, reject, or flag the message as suspicious.

Why SPF matters:

- Reduces spam and phishing by making it harder for attackers to forge sender addresses.
- Improves email deliverability for legitimate senders.
- Works with other protocols like DKIM and DMARC for stronger email security.

SPF quick deny or quick drop

While not formal SPF terminology, "quick deny" or "quick drop" typically refers to how receiving mail servers handle SPF failures immediately and decisively, often rejecting or dropping the message without further processing. This is especially relevant in high-security environments or when SPF is used in conjunction with DMARC policies.

This quick deny functionality occurs when the sending server opens a connection to the destination server. The destination server performs the SPF check and if it fails, the connection is dropped before the email is transmitted. This means no other policy checking mechanisms can come in to play. For instance when quick deny closes the connection it is not possible for an email to prove its validity through DKIM alone, even though DMARC normally allows this.

For that reason it is critical to understand all your mail sending services and to ensure they are correctly accounted for within your SPF record.

Here's how it works:

1. **SPF Evaluation**:
   - The receiving server checks the sender's IP against the domain's SPF record.
   - If the IP is not authorized, the SPF check fails.
2. **Quick Deny / Drop Behaviour**:
   - If the SPF record ends with -all, this is a hard fail.
   - Many mail servers are configured to reject the message outright (quick deny) or drop it silently (quick drop), especially if DMARC policy is set to reject.

3. **Why Use Quick Deny?**
    - Efficiency: Reduces processing overhead by terminating unauthenticated messages early.
    - Security: Prevents spoofed or malicious messages from reaching inboxes or triggering downstream filters.
    - Compliance: Aligns with strict DMARC enforcement policies.
4. **Configuration Examples**:
    - SPF record: v=spf1 ip4:203.0.113.5 -all
        - This means: only allow mail from 203.0.113.5; deny all others.
    - Mail server behaviour:
        - If a message comes from 203.0.113.6, it fails SPF and is rejected immediately.

The most common scenario where quick deny impacts legitimate email is when emails are forwarded (SMTP forwarding) through an external mail service prior to delivery.

Scenario: SPF Failure Due to Forwarding via External Mail Security

1. **Original Email Sent**
    - Sender: alice@example.com
    - Sender IP: 203.0.113.5 — listed in example.com's SPF record.
    - DKIM: Signed by example.com
2. **Delivered to External Mail Security Gateway**
    - Service: securemail.filter.com
    - Action: Scans and relays the message to the recipient.
    - SPF: ✅ Passes
    - DKIM: ✅ Passes
    - DMARC: ✅ Passes (SPF and DKIM align)
    - Envelope sender remains: alice@example.com
    - New sending IP: 198.51.100.10 (IP of securemail.filter.com)
3. **Message Forwarded to Final Destination**
    - Recipient: bob@destination.org
    - Destination Mail Server: mx.destination.org (typically via a secure connector)
    - SPF Check:
        - Looks up SPF for example.com
        - Sees 203.0.113.5 is authorised, but not 198.51.100.10
        - SPF fails

4. **SPF Quick Deny Triggered**

- mx.destination.org is configured to **reject** mail on SPF hard fail (-all)
- Result: ❌ Message is denied or dropped
- Even though:
  - Original sender was legitimate
  - DKIM may still be valid
  - Message passed through a trusted filtering service

Mitigation Options

- Use Enhanced Filtering (Skiplisting) for the service via a Trusted Connector (see below)
- SPF rewrite on forwarding (Contact your security provider for advice on this option)

Steps to Configure a Skiplisting via a Trusted Connector in M365

1. Prerequisites

- You must have an inbound connector already configured for your third-party mail relay or filtering service.
- You must know the public IP addresses of the service.

2. Enable Enhanced Filtering (Skiplisting)

This tells M365 to ignore the connector's IP and look deeper into the message headers to find the true source IP, avoiding SPF failures caused by relaying.

Steps:

1. Go to the Microsoft 365 Defender portal:
   https://security.microsoft.com/skiplisting (shortcut direct to the Enhanced Filtering for Connectors)
2. Navigate to:
   Email & Collaboration > Policies & Rules > Threat Policies > Enhanced Filtering for Connectors
3. Select the inbound connector you want to configure.
4. In the flyout pane, choose one of the following:
   - Automatically detect and skip the last IP address (Recommended), or use the Skip these IP addresses associated with the connector setting if you require more precise control.
   - Apply to entire organization (or to a group of users if required)
5. Save the configuration.

What This Does

- Preserves the original sender IP for SPF evaluation.
- Prevents SPF failures due to the connector's IP being seen as the sender.
- Improves DMARC accuracy, anti-phishing, and spoof detection.

- Helps avoid quick drop behaviour on SPF hard fails.

In most other situations, where SPF quick drop impacts mail flows, it is caused by incomplete or inaccurate SPF records.

There may be some deliberate scenarios where you may need to permit SPF to fail, and rely on DKIM to pass the email during DMARC checks. If this scenario impacts you it is recommended the sending service be configured on a separate sub domain, and the applicable ~all SPF setting is applied only on that sub domain.

This is outside the bounds of the Framework which is bound to the NZISM, control 15.2.48.C.02. You will need to undertake your own risk assessment and place appropriate mitigations in place.

SPF Alignment

What is SPF Alignment?

When used in conjunction with DMARC (Domain-based Message Authentication, Reporting & Conformance) SPF Authentication checks the SMTP envelope sender address (RFC 5321) and the visible from address of the sender (RFC5322) within an email. The domains must match for SPF alignment to pass.

This alignment helps prevent spoofing by verifying that the domain claiming to send the email is actually authorized to do so, and that it matches the domain the user sees. Without alignment, a malicious sender could pass SPF using a different domain than the one shown to the recipient, undermining trust.

Why It Matters:

DMARC requires that either SPF or DKIM (preferably both) pass and align. Without alignment, even a valid SPF source won't satisfy DMARC tests.

How SPF Alignment Works

When DMARC checks an inbound email for SPF alignment, it verifies whether the domain in the Envelope Sender (used for SPF authentication) matches the domain in the Header From address. This ensures that the domain shown to the recipient is also the one authorised to send the message, helping prevent spoofing and impersonation.

Within DMARC there are two settings for SPF, they are aspf=s or aspf=r. The S and R are for strict or relaxed alignment. When using strict alignment, the domain portion must match exactly, subdomains will not pass strict alignment. When using relaxed alignment, the domain portion must be included in the match, so subdomains will align.

The following table shows how SPF authentication and DMARC alignment interact, with examples showing the DMARC check result:

SMTP Envelope Sender (RFC 5321 address)	Header From address – user visible (RFC 5322)	SPF Result	Alignment	DMARC Result	Notes
bounce@example.com	ceo@example.com	Pass	Aligned	✅ Pass	Same domain, SPF passes and aligns

bounce@thirdparty.com	ceo@example.com	Pass	Not aligned	❌ Fail	SPF passes but domain mismatch
bounce@example.com	ceo@example.com	Fail (bad server)	N/A	❌ Fail	SPF fails because the sending server is not in the SPF record. Alignment is irrelevant.
bounce@mail.example.com	ceo@example.com	Pass	Aligned (relaxed)	✅ Pass	Subdomain aligns under relaxed mode
bounce@mail.example.com	ceo@example.com	Pass	Not aligned (strict)	❌ Fail	Subdomain fails strict alignment

Appendix 2 – Frequently asked Questions

Does the SGE project recommend SPF2.0/PRA?

No. SPF2.0/pra is problematic. It tried to unify SPF and Microsoft's approach to validating the visible sender, however, it caused issues with forwarding, mailing lists, and standards compliance. The IETF rejected Sender ID as a standard due to these problems. Most modern systems use SPF (v=spf1), DKIM, and DMARC instead.
If you have SPF2.0 type records these should be removed from DNS.

Can I use SPF redirect services?

Yes. Several providers support SPF redirects to hosted SPF services. These fit within the bounds of the Framework, so long as the lookup results in a -all suffix.

What do the ~all, -all, and ?all mean?

Mechanism	Meaning	Recommended use
-all	**Fail** — only listed servers are allowed.	Use when configuration is complete. **Required for SGE Framework and NZISM Compliance**
~all	**Soft fail** — treat non-listed senders as suspicious but not outright fails.	Use during rollout/testing.
?all	**Neutral** — no policy.	Rarely recommended.

What counts against the maximum 10 lookups?

Anything which triggers a DNS action counts as one of the available 10 lookups for an SPF record. Here’s the minties.govt.nz SPF statement from earlier in the document:

```
v=spf1 mx ip4:192.0.2.2 ip6:2001:db8::1 include:spf.protection.outlook.com -all
```

Only the mx and include statements trigger further DNS lookups, so this record has a count of 2. The ip4 and ip6 records do not trigger a DNS lookup or impact the count.

Can a message pass SPF but fail DMARC?

Yes. SPF can pass, but if the SPF-authenticated domain doesn’t align with the domain in the visible “From:” header, DMARC fails.

Can a message fail SPF but still pass DMARC?

Yes — if the message passes DKIM and the DKIM domain aligns with the From domain, DMARC passes even if SPF fails.

What happens if I have multiple SPF records?

It is invalid to have multiple SPF records on a single domain.
If more than one exists, receivers may treat it as a permanent error (permerror), and SPF validation may fail. Combine all mechanisms into a single record if needed.

What’s the difference between SPF and DKIM?

Feature	SPF	DKIM
Authenticates	Sending mail server	Message content and sender’s domain
Uses	SMTP envelope (MAIL FROM)	Digital signature in message headers
Breaks if message is forwarded?	Often yes	Usually no

Appendix 3 – List of Acronyms

Acronym	Definition
CNAME	Canonical Name (used as an alias in DNS)
CRM	Customer Relationship Management
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
ESP	Email Service Providers (Typically referring to bulk senders)
MX	Mail Exchange
M365	Microsoft 365
NZISM	New Zealand Information Services Manual
SGE	Secure Government Email (Framework)
SPF	Sender Policy Framework