Domain Fraud Protection Background

https://campus.barracuda.com/doc/112164966/

This functionality is available only with Domain Fraud Protection or with Barracuda Email Protection Premium and Premium Plus plans. To purchase Domain Fraud Protection or to upgrade to one of these plans, contact your Barracuda Networks Sales Representative.

This page provides background information on SPF, DKIM, and DMARC. For instructions, refer to:

- Configuring Domain Fraud Protection with Barracuda
- Troubleshooting Domain Fraud Protection

SPF (Sender Policy Framework) enables the owner of an Internet domain to identify the systems authorized to send email with envelope-from addresses associated with their domain. Using the SPF TXT records, the list of authorized IP addresses are published in DNS. Receivers verifying the SPF information in TXT records can then reject emails from unauthorized sources. SPF also ensures that legitimate email from the domain is delivered.

DKIM (DomainKeys Identified Mail) is used to verify that the content of an email is trustworthy, meaning the content has not been changed from the time the email was transmitted by the sending mail server. This additional layer of trust is established using a standard public/private encryption key signing process. The domain owners must add a DNS entry for their email server and include their public DKIM key. The DKIM key can be used by receivers to verify that the DKIM message signature is correct. For the sender, the email server signs the emails with the corresponding private key.

DMARC (Domain-based Message Authentication, Reporting and Conformance) empowers SPF and DKIM by presenting a clear policy. You can also use DMARC to specify an address for reports about the mail messages statistics gathered by receivers against the specific domain.

When you properly configure SPF, DKIM, and DMARC, emails from malicious actors attempting to use your domain are not automatically blocked on the Internet. Email system administrators must configure sender authentication checks, at which point their systems can screen clearly fraudulent email based on your SPF, DKIM, and DMARC settings in DNS.

Email and SMTP

Simple Mail Transfer Protocol (SMTP), the original email protocol deployed in the 1970s, permits any computer to send an email claiming to be from any source address. When Internet mail systems were confined to universities and government agencies, this did not pose a problem for system

administrators or end-users. However, in recent decades, this loophole has been exploited by spammers using fake email addresses, making it more difficult to trace a message back to its source. This loophole is also used in phishing, where users are encouraged to disclose private information in response to an email supposedly sent by a legitimate organization, but actually originating from a nefarious organization.

How to Create SPF Records

SPF enables the owner of an Internet domain to identify the computers that are authorized to send email with envelope-from addresses associated with their domain. Using the SPF TXT records, the list of authorized IP addresses are published in DNS. Receivers verifying the SPF information in TXT records can then reject emails from unauthorized sources. SPF also ensures that legitimate email from the domain is delivered. SPF is a public Internet protocol defined by the IETF in RFC 7208.

To create an SPF record, complete the following steps:

1. Create a list of all of the IP addresses the organization uses to send email from their domain. Include IP addresses for any of the following systems associated with the organization:
   - Web servers
   - On-premises mail servers (for example, Microsoft Exchange)
   - Your ISP's mail servers
   - Third-party mail servers
2. Create a list of the domains used for sending email. Barracuda Networks recommends creating SPF records for all of the domains controlled by the organization. Even though a domain might not be used for sending emails, malicious actors can potentially target any domain associated with a legitimate organization.
3. Create the SPF record. SPF authenticates a sender's identity by comparing the sending mail server's IP address to the authorized IP addresses published in the DNS record. SPF records are limited to a maximum of 255 characters and 10 include statements
   To create an SPF record, complete the following steps:
   1. Start with the v=spf1 (version 1) tag and follow it with the valid IP addresses that are authorized to send mail:
      `v=spf1 ip4:192.0.2.0/24`
   2. For Barracuda Networks customers, add an `include` statement (example shown is for a customer located in the United States) in the SPF record to designate Barracuda as the legitimate sender:
      `include:spf.ess.barracudanetworks.com`
   3. Once you have added all authorized IP addresses and include statements, end your record with the `-all` tag. The `-all` tag specifies a hard SPF failure and indicates that all other systems that have not been identified by this SPF record should be rejected.
      The following is an example of an SPF record:
      `v=spf1 ip4:192.0.2.0/24 include:spf.ess.barracudanetworks.com -all`
      The following is an example of an SPF record for a non-sending domain (the only valid modifier for non-sending domains is `-all` which indicates that any email originating from this domain should be rejected):

```
v=spf1 -all
```

4. Publish your SPF to DNS. You need to publish your SPF record to DNS so that it can be referenced by other email service providers and organizations. If needed, your email service providers can publish the SPF records on your behalf.
5. Check your SPF record. You should test your SPF record to ensure that you have indeed authorized your email servers to send email on behalf of your domain. You'll also be able to check that none of your valid email sending IP addresses are missing. The following website provides an SPF record checking tool that you can use to query the DNS: https://vamsoft.com/support/tools/spf-policy-tester.

SPF Configuration Options

The following mechanisms can be configured in an SPF record:

`all`	Matches always. Used for a default result (for example, `-all` to identify all IPs not matched by prior mechanisms).
`a`	Domain name has an address record (A or AAAA) that can be resolved to the sender's address.
`ip4`	Sender is in a given IPv4 address range.
`ip6`	Sender is in a given IPv6 address range.
`mx`	Domain name has an MX record resolving to the sender's address (for example, the mail comes from one of the domain's incoming mail servers).
`ptr`	Do Not Use
`exists`	Do Not Use
`include`	References the policy of another domain. If that domain's policy passes, this mechanism passes. However, if the included policy fails, processing continues. To fully delegate to another domain's policy, the *redirect* extension must be used.

Each mechanism can be combined with one the following qualifiers. Typically, Barracuda only qualifies the `-all` mechanism, but it is possible to employ the others.

Qualifier	Description
+	Pass. This can be omitted (for example, +mx is the same as mx).
?	Neutral. This is interpreted as a null (no policy).
~	Softfail. Used as a debugging aid between a Neutral and Fail. Messages returning a Softfail are accepted but tagged as suspect.
-	Fail. The email should be rejected.

DKIM Overview

DKIM helps to protect both email receivers and email senders from forged and phishing email. It relies on public key cryptography to enhance the security of email, allowing an email sender to create a

signature which allows any email recipient to verify that the signed message wasn't altered in transit. It works by enabling email server administrators to publish a DKIM signature for their domain to DNS as a public encryption key. The DKIM signature can be attached to the headers of emails originating from their email servers. Email recipients can then check that an email claiming to have originated from a specific domain was indeed authorized by the owner of that domain by verifying the DKIM signature using the public key published in DNS. A valid signature ensures that the content of the email has not been modified since the signature was added.

Many of the largest email service providers (Yahoo, Google, etc) employ DKIM authentication in their mail processing workflows to help prevent email fraud within their own services. If you manage an email server, you can enable DKIM to ensure your email recipients receive only legitimate messages from your domain.

Notes

- If you use Microsoft Office365, you must configure DKIM on your domain prior to enabling DMARC in Barracuda. This procedure is described here: https://docs.microsoft.com/en-us/office365/SecurityCompliance/use-dkim-to-validate-outbound-email.
- If you handle your email through an on-premises Microsoft Exchange server, you must deploy a third party tool to properly sign your emails.

How Does DKIM Work

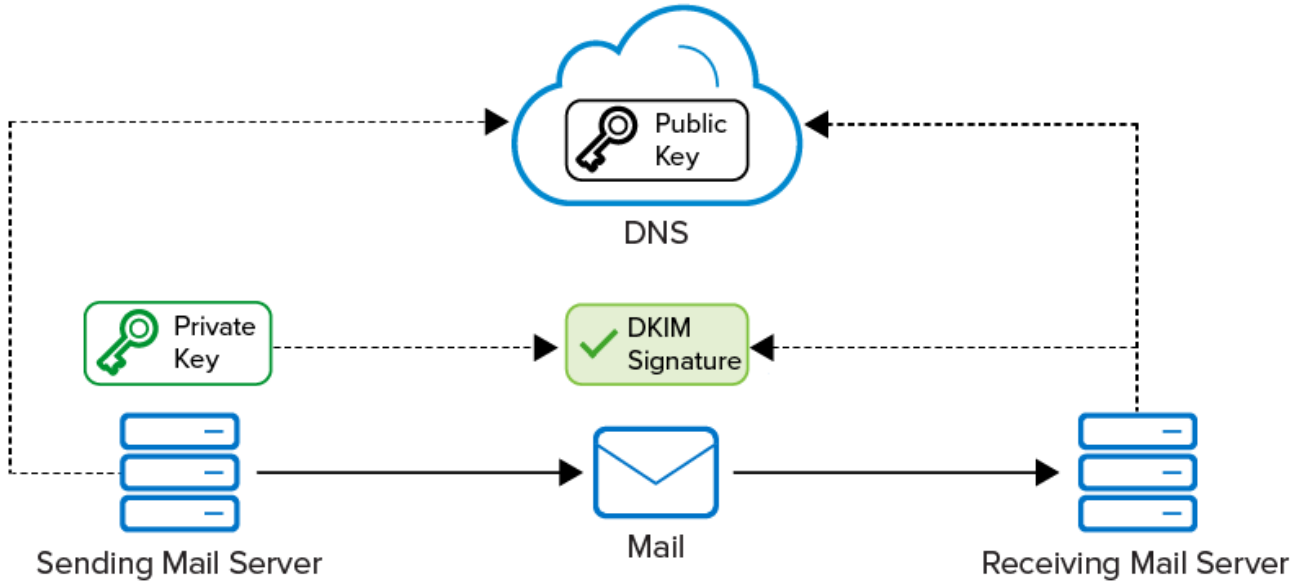
DKIM employs public key cryptography to ensure that emails sent over the Internet are not altered in transit. Public key cryptography employs a pair of cryptographic keys, a private key and a public key. The private key is retained by the email sender in a secure location. The public key enables any email recipient to verify that the DKIM signature was indeed made with the corresponding private key.

When an email is sent to a recipient, the email software generates a signature based on the content of the message and the sender's private key. The signature is added to the email header and the message is sent to the recipient. The recipient's email server can validate the signature using the public key. If the content of the message has been altered, the signature won't validate and the recipient's email server can drop or otherwise dispose of the message.

The sending email server's administrator publishes the public key in DNS, enabling anyone receiving an email from the sender's domain to locate the public key and validate the DKIM signature.

Figure 1.

Receiving email servers can check the integrity of an email by validating the DKIM signature attached to the message against the public key of the sending mail server.



Emails from fraudulent domains won't have a valid signature and are therefore easy to detect. You can use DMARC to specify how to handle email messages that cannot be validated. Typically, such emails should be rejected.

Here is an example of a DKIM signature:

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane;
 c=relaxed/simple; q=dns/txt; l=1234; t=1117574938; x=1118006938;
           h=from:to:subject:date:keywords:keywords;
        bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

Using the DKIM signature above as an example, a verifier queries the TXT resource record type of brisbane._domainkey.example.net. Here, example.net is the *author* domain to be verified against (in the **d** field), brisbane is a selector given in the **s** field while _domainkey is a fixed part of the protocol.

The following table lists descriptions for all of the DKIM signature fields:

Field	Description
v	Version
a	Signing algorithm
d	Domain
s	Selector
c	Canonicalization algorithm for the header and body

q	Default query method
l	Length of the canonicalized part of the signed message body
t	Signature timestamp
x	Expiration time
h	List of signed header fields (repeated for fields that occur multiple times

The data returned from a query is a list of tag-value pairs. It includes the domain's public key along with other key usage tokens and flags. The receiver uses this information to decrypt the hash value in the header field and recalculate the hash value for the mail message (headers and body). If the two values match, this cryptographically proves that the mail was signed by the indicated domain and has not been tampered with in transit.

DMARC Overview

SPF and DKIM provide some assurance as to the identity of the sender of a message and that the message has not been tampered with. The configuration and deployment of these protocols is more and more common across email senders and receivers. However, problems with fraudulent and deceptive emails remain widespread for the following reasons:

- Many senders have complex email systems which often include 3rd party email service providers. It is difficult to ensure that every message can be authenticated using SPF or DKIM.
- If a domain owner sends a mix of messages, some of which can be authenticated and others which cannot, email receivers are forced to discern between the legitimate messages that don’t authenticate and the fraudulent messages that also don’t authenticate. Fraudulent messages tend to make their way to the end user’s inbox.
- It is difficult for senders to validate their email authentication deployments. There are few ways to determine how many legitimate messages are being sent that fail authentication or to determine the scope of the fraudulent emails that are spoofing the sender’s domain.
- Even when SPF and DKIM are configured properly, email receivers are reluctant to reject unauthenticated messages.

To address these problems, senders and receivers need to share information with each other. Receivers need to provide information about their mail authentication infrastructure, while senders need to indicate what should be done when a message does not authenticate. DMARC attempts to provide the criteria email recipients should use to reject unauthenticated messages.

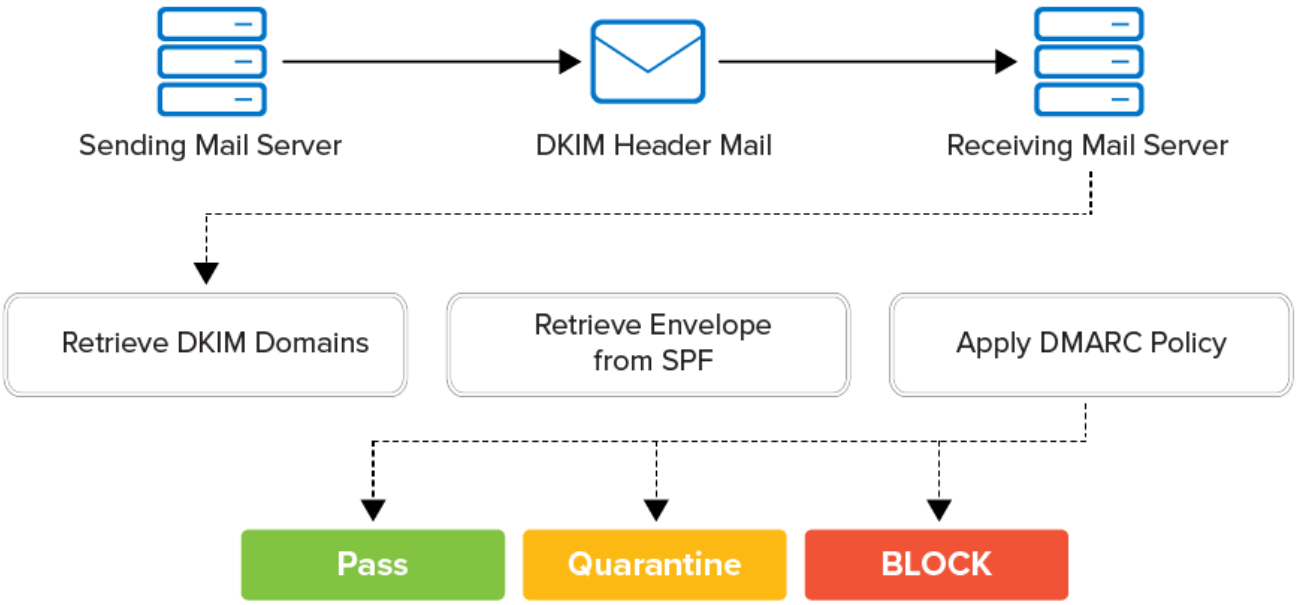
DMARC and the Email Authentication Process

DMARC integrates with existing inbound email authentication processes. It helps email recipients to determine if a message *aligns* with what the receiver knows about the sender. If not, DMARC includes guidance on how to handle the *non-aligned* messages. For example, assuming that a receiver deploys

SPF and DKIM, the email flow and authentication process would be as shown in Figure 2.

Figure 2.

Receiving email servers can apply DMARC against incoming mail messages. Depending on whether the message aligns, the receiving email server can pass, quarantine, or block the message. Whichever domain is aligned must also pass the respective test (SPF or DKIM) for DMARC to pass. Alignment alone won't ensure authentication.



DMARC is designed to satisfy the following requirements:

- Minimize false positives
- Provide robust authentication reporting
- Assert sender policy at receivers
- Reduce successful phishing delivery
- Work at Internet scale
- Minimize complexity

DMARC builds upon both the DKIM and SPF specifications. DMARC is designed to replace Author Domain Signing Practices (ADSP) by adding support for:

- Wildcarding of subdomain policies
- Non-existent subdomains
- Slow rollout (for example, percent experiments)
- SPF
- Quarantining mail

Understanding SPF, DKIM, and DMARC Data Reporting

SPF, DKIM and DMARC report the following types of information:

- SPF uses the domain in the *envelope from* header to complete its checks.
- DKIM uses the domain specified in the signature (d=domain.com), typically located in the *mail from* address.
- When mail is forwarded, the forwarding mail server re-writes the envelope with their domain, while keeping the MAIL FROM domain intact.
- SPF information is dropped from forwarded emails. If an email is sent from your mail server and the receiving server has a mail forward rule in place, that forwarded mail would now fail SPF, because it appears to come from the original receiving mail server.
- DKIM information is retained in forwarded email, because the signature is injected by the sending server and that signature does not get modified as it's forwarded on.
- For DMARC to pass, either SPF or DKIM must align and either the SPF check or DKIM check must pass. This means that the SPF domain *or* the DKIM domain must match the domain in the *mail from* field (the human viewable email address). If neither SPF or DKIM aligns, DMARC will fail even though SPF or DKIM passes.

Using Barracuda to Remediate Issues with SPF, DKIM, and DMARC

Barracuda can help you to analyze and remediate issues tied to your deployments of SPF, DKIM, and DMARC. From the menu in the upper left corner of Impersonation Protection or Domain Fraud, select **Domain Fraud Protection**. For the domain you are having issues with, select **View Report** and then click the **Remediate** tab.

Please be aware of the following:

- Checking the **Legitimate** box for a service does not make any changes to your SPF, DKIM, or DMARC configurations or to Domain Fraud Protection. This is just used as a personal reference to designate which domains are legitimate and which are not.
- The name of each Sender is obtained using a DNS lookup on the sending IP address. If there is no associated hostname, only the IP address is displayed.
- Some senders might include sample emails as part of their DMARC report. If there are no sample emails displayed, Barracuda did not receive any.

You generally want to focus on Senders listed in the **HIGH VOLUME SENDERS** section. These are typically all legitimate. If there are any failures, you will want to resolve them first. The lower volume senders might be legitimate, but are much more likely to be either mail forwards or spam. Focus on the senders with DMARC failures. The primary goal is to have DMARC pass, regardless of whether or not there are SPF and DKIM failures.

Once you have checked all of the legitimate mail senders, you can click the **Investigate** icon to better understand the information provided by the DMARC reports.

Investigate

The Investigate option provides the details needed to understand the DMARC reports.

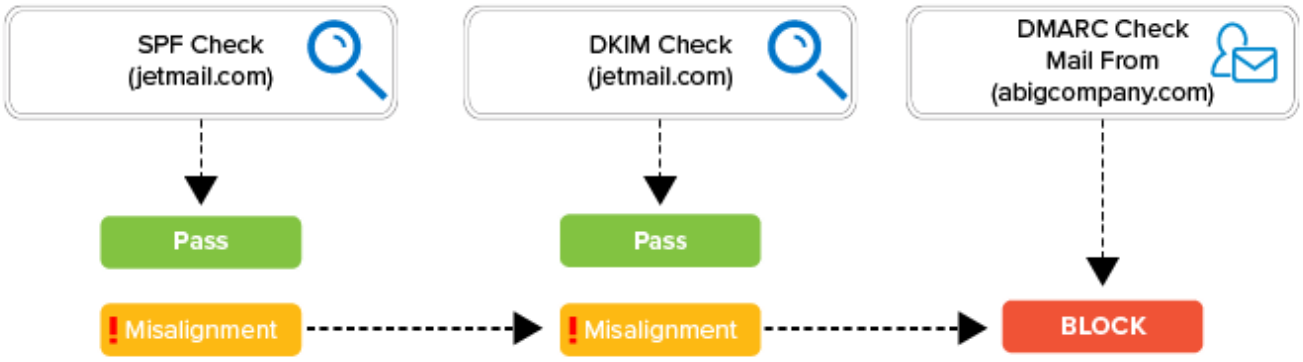
Column Heading	Description
From	Domain displayed in the message header and visible in the mail client.
SPF domain	Domain that the receiving mail server checked against SPF, typically the *envelope from* address.
DKIM domain	Domain stated in the DKIM signature (d=domain.com).
Reports	Number of reports received for the specific SPF and DKIM domain combination.

For example, ABigCompany is using ABigCompany as an email service provider. There is an issue with ABigCompany's SPF record (it includes an extra `-all`). However, even after correcting the SPF record and verifying the fix in DNS, DMARC continues to fail 100% of the time.

After clicking the **Investigate** icon for this domain, green check marks are displayed for both SPF and DKIM, indicating that those checks have passed. For DMARC to pass, either SPF or DKIM must pass and at least one of them also needs to align. Alignment means that the domain listed under either the SPF domain or the DKIM domain must match the domain listed in the **mail from** field in the email header. The numbers reported on the **REMEDIATE** tab list the number of times DMARC has passed or failed and the number of times SPF and DKIM have passed, failed, or misaligned. If Sender only passed the initial check but did not align, it is reported as a failure.

Figure 3.

SPF, DKIM, and DMARC checks are made against ABigCompany's email. Both SPF and DKIM checks pass. However, the DMARC check fails due to misalignment.



In this example, the emails from jetmail.com are not authenticating against ABigCompany's SPF record. Since the envelope from is s1.email.jetmail.com, the SPF checks are completed against jetmail.com. However, jetmail.com domain does not belong to ABigCompany. The DKIM domains are also listed for jetmail.com. This indicates that jetmail.com has configured DKIM for their email systems, but ABigCompany has not configured DKIM.

How to Achieve Alignment

Complete the following steps to align DMARC and SPF:

1. Align the SPF configuration for your email service provider.
2. Review the headers of at least one email coming from your email service provider. If they are available, use the samples in your DMARC report.
3. If SPF fails, verify that your email service provider's domain is included in your SPF record.
4. If SPF passes, verify that the domain in the SPF check matches your domain. For DMARC to pass, this domain must align with your domain. Please inquire with your email service provider whether it can match the *mail from* field in its email headers with your domain.

If you are unable to align SPF, consider the following options:

1. Add DKIM signatures to your email service provider's emails.
2. Change the sending email address for your email service provider’s emails to another domain that will not be protected with DMARC.
3. Change the sending email address for your email service provider’s emails to one of your subdomains and avoid enforcing DMARC on the subdomain. Please contact Barracuda for assistance.

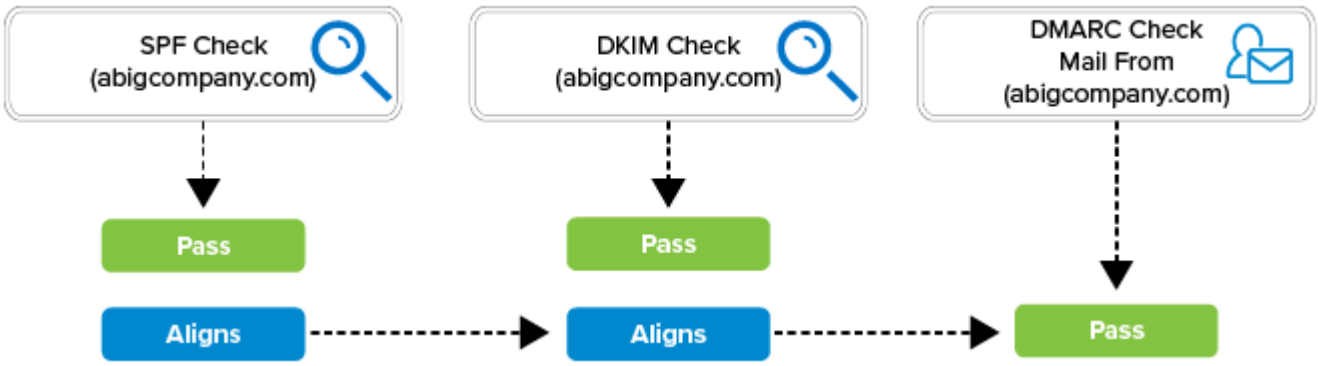
   For the ABigCompany example, the customer could create a subdomain, such as bids.abigoffice.com. Within ABigCompany, they can change the mail from address to something like no-reply@bids.abigoffice.com. Now, emails coming from ABigCompany can use the sub-domain. You would also need to create a new DMARC policy.

Example: SPF and DKIM Both Pass and Align with DMARC

The only way for DMARC to pass is to have proper alignment. The simplest way to accomplish this is to change the envelope for the service sending the emails. Most email service providers have configuration options that enable you to change the envelope address to match your domain (in this example, abigcompany.com), allowing SPF and DKIM to align and DMARC to pass.

Figure 4.

SPF, DKIM, and DMARC checks are made against ABigCompany's email. Both SPF and DKIM checks pass. This time the mail from domain aligns with the SPF and DKIM domains and the DMARC check passes.



If you cannot change the envelope, you can alternatively create a sub-domain and have your emails originate from it. On the **Remediate** tab, you can click the *Recommendation* icon to obtain recommendations for how to resolve the issue.

Example: Forwarded Email Aligns with DMARC

The following example illustrates how DMARC alignment can succeed with forwarded emails, even though SPF fails to align with DMARC.

You send a message to jdoe@domain.com with the following email header:

From: janed@barracuda.com
To: jdoe@domain.com
Envelope From: janed@barracuda.com
DKIM: Signed d=barracuda.com

The jdoe@domain.com email account receives the email and DMARC passes. However, jdoe has an automatic forwarding policy for his personal email, sending all messages to jdoe@gmail.com.

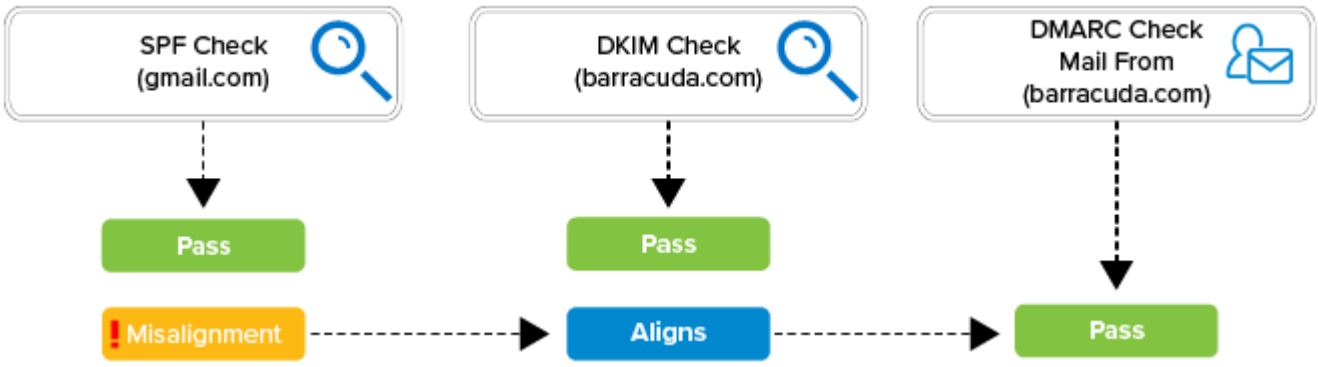
The forwarded message now has the following email header:

From: janed@barracuda.com
To: jdoe@gmail.com
Envelope from: jdoe@domain.com
DKIM: Signed d=barracuda.com

As shown here, although the SPF check passes, DMARC cannot align based on this alone (@gmail.com is a valid domain but does not align with @domain.com). However, since the DKIM check also passes, DMARC can align.

Figure 5.

SPF and DKIM both pass, but SPF does not align. Since DKIM still does align, DMARC passes.



This type of scenario is common and the Barracuda reports could show the sender as ISPs, free mail providers, and other hosting services.

Without DKIM, it is impossible to align DMARC in this scenario, which is likely to break automatic forwarding for most users. If you handle your email through an on-premises Microsoft Exchange server, you have to deploy a 3rd-part tool to properly sign your emails.

Figures