UNDERSTANDING DMARC / ARC

Table of Contents

Understanding DMARC

Domain-based Message Authentication, Reporting, and Conformance, or DMARC, is a technical standard that helps protect email senders and recipients from spam, spoofing, and phishing. DMARC allows an organization to publish a policy that defines its email authentication practices and provides instructions to receiving mail servers for how to enforce them. In this edition of "DMARC Explained" you'll learn what DMARC is and how it works. Specifically, DMARC establishes a method for a domain owner to:

- Publish its email authentication practices
- State what actions should be taken on mail that fails authentication checks
- Enable reporting of these actions taken on mail claiming to be from its domain

DMARC itself is not itself an email authentication protocol, but it builds on key authentication standards SPF and DKIM. With them, it supplements SMTP, the basic protocol used to send email, because SMTP does not itself include any mechanisms for implementing or defining policies for email authentication.

How does DMARC work?

DMARC relies on the established SPF and DKIM standards for email authentication. It also piggybacks on the well-established Domain Name System (DNS). In general terms, the process of DMARC validation works like this:

1. A domain administrator publishes the policy defining its email authentication practices and how receiving mail servers should handle mail that violates this policy. This DMARC policy is listed as part of the domain's overall DNS records.
2. When an inbound mail server receives an incoming email, it uses DNS to look up the DMARC policy for the domain contained in the message's "From" (RFC 5322) header. The inbound server then checks evaluates the message for three key factors:
    - Does the message's DKIM signature validate?
    - Did the message come from IP addresses allowed by the sending domain's SPF records?
    - Do the headers in the message show proper "domain alignment"?
3. With this information, the server is ready to apply the sending domain's DMARC policy to decide whether to accept, reject, or otherwise flag the email message.
4. After using DMARC policy to determine the proper disposition for the message, the receiving mail server will report the outcome to the sending domain owner.

What is a DMARC record?

A DMARC record is included in an organization's DNS database. An DMARC record is a specially-formatted version of a standard DNS TXT record with a particular name, namely "_dmarc.mydomain.com" (note the leading underscore). A DMARC record looks something like this:

_dmarc.mydomain.com. IN TXT "v=DMARC1\; p=none\; rua=mailto:dmarc-aggregate@mydomain.com\; ruf=mailto:dmarc-afrf@mydomain.com\; pct=100"
Reading left-to-right in plain English, this record says:

- **v=DMARC1** specifies the DMARC version
- **p=none** specifies the preferred treatment, or DMARC policy
- **rua=mailto:dmarc-aggregate@mydomain.com** is the mailbox to which aggregate reports should be sent
- **ruf=mailto:dmarc-afrf@mydomain.com** is the mailbox to which forensic reports should be sent
- **pct=100** is the percentage of mail to which the domain owner would like to have its policy applied

Additional configuration options are available for a domain owner to use in its DMARC policy record as well, but these are the basics.

What does DMARC domain alignment mean?

"Domain alignment" is a concept in DMARC that expands the domain validation intrinsic to SPF and DKIM. DMARC domain alignment matches a message's "from" domain with information relevant to these other standards:

- For SPF, the message's From domain and its Return-Path domain must match
- For DKIM, the message's From domain and its DKIM d= domain must match

The alignment can be relaxed (matching base domains, but allowing different subdomains) or strict (precisely matching the entire domain). This choice is specified in the published DMARC policy of the sending domain.

What are DMARC p= policies?

The DMARC specification provides three choices for domain owners to use to specify their preferred treatment of mail that fails DMARC validation checks. These "p= policies" are:

- **none**: treat the mail the same as it would be without any DMARC validation
- **quarantine:** accept the mail but place it somewhere other than the recipient's inbox (typically the spam folder)
- **reject:** reject the message outright

Remember that the domain owner can only request, not force, enforcement of its DMARC record; it's up to the inbound mail server to decide whether or not to honor the requested policy.

What is a DMARC report?

DMARC reports are generated by inbound mail servers as part of the DMARC validation process. There are two formats of DMARC reports:

- **Aggregate reports**, which are XML documents showing statistical data about the messages received that claimed to be from a particular domain. Date reported includes authentication results and message disposition. Aggregate reports are designed to be machine-readable.
- **Forensic reports**, which are individual copies of messages which failed authentication, each enclosed in a full email message using a special format called

AFRF. Forensic report can be useful both for troubleshooting a domain's own authentication issues and for identifying malicious domains and web sites.

How is DMARC related to SPF, DKIM, or other standards?

DKIM, SPF, and DMARC are all standards that enable different aspects of email authentication. They address complementary issues.

- SPF allows senders to define which IP addresses are allowed to send mail for a particular domain.
- DKIM provides an encryption key and digital signature that verifies that an email message was not faked or altered.
- DMARC unifies the SPF and DKIM authentication mechanisms into a common framework and allows domain owners to declare how they would like email from that domain to be handled if it fails an authorization test.

Do I need DMARC?

If you are a business sending commercial or transactional email, you definitely need to implement one or more forms of email authentication to verify that an email is actually from you or your business. Properly configuring DMARC helps receiving mail servers determine how to evaluate messages that claim to be from your domain, and it is one of the most important steps you can take to improve your deliverability. However, standards like DMARC only go so far; XgenPlus and other email experts recommend implementing a DMARC email authentication policy in context of a complete messaging strategy.

Does XgenPlus support DMARC?

Yes. XgenPlus implements and adheres to email authentication standards, including DMARC. In fact, all email we deliver for our users includes a default DMARC policy that can be customized to your needs.

Understanding ARC

It helps preserve email authentication results and verifies the identity of email intermediaries that forward a message on to its final destination. It's an important step forward in helping receivers of indirect messages trace the path of intermediaries and make a safer, more informed delivery decision.