Resolve DMARC Failures by Correcting SPF and DKIM Alignment

Contents

Issue

Emails from specific domains are blocked by the Cisco Secure Email Gateway (CES/ESA) due to DMARC verification failures. Analysis of message tracking indicates that these emails are held in the work queue and placed in quarantine or rejected, which prevents them from reaching the intended recipients.

Environment

- Cisco Secure Email Gateway (CES/ESA) appliances
- SPF, DKIM, and DMARC policies are configured and enforced

Resolution

SPF/DKIM Alignment Summary Table (Examples)

Mechanism	Alignment Status	Envelope/Signature Domain	From Header Domain	Logic
SPF	In Alignment	sender@example.com	sender@example.com	Direct match
SPF	In Alignment	sender@child.example.com	sender@example.com	Parent domain match
SPF	Not in	sender@test.com	sender@example.com	Domain mismatch

	Alignment			
DKIM	In Alignment	example.com	sender@example.com	Direct match
DKIM	In Alignment	example.com	sender@child.example.com	Relaxed mode match
DKIM	Not in Alignment	example.com	sender@test.com	Domain mismatch

Coordinate with Sender (Recommended)

- Collaborate with the sender domain administrators to remediate DMARC failures by ensuring proper SPF and DKIM alignment at the header level.
- The sender must:
  - Ensure the domain used in the SPF-validated MAIL FROM or HELO/EHLO identity aligns with the domain in the **From** header of the email.
  - Implement DKIM signing where the domain specified in the DKIM signature's d= tag aligns with the **From** header domain.
  - Verify the DMARC policy is correctly configured to enforce the desired alignment mode (strict or relaxed) and reporting options.
- This approach addresses the root cause of DMARC failures by focusing on the alignment of authenticated domains with the visible From header domain, which is critical for long-term email deliverability.

Create DMARC Exception (Alternative)

- If remediation by the sender is not feasible, create an exception on the ESA device for the specific sender address to bypass DMARC checks.
- This is a temporary workaround and must be accompanied by monitoring.

Monitor and Validate

- After implementing changes, monitor the delivery of alert emails to the intended recipients.
- Review message tracking logs to confirm that DMARC failures have been resolved.
- Continue to analyze updated message tracking data if delivery issues persist.

Cause

The primary cause of email quarantine or rejection is DMARC verification failure due to SPF and DKIM alignment issues. These failures indicate that although SPF and DKIM records can be correctly published, the domains authenticated during the email exchange do not align with the From header domain, resulting in quarantine of emails.

Understanding DMARC, SPF, and DKIM Alignment:

- SPF authenticates the domain in the MAIL FROM or HELO/EHLO SMTP commands and requires this domain aligns with the domain in the **From** header for DMARC compliance.
- DKIM uses cryptographic signatures with a signing domain specified in the d= tag, which must align with the **From** header domain.
- DMARC builds on SPF and DKIM by requiring that at least one of these authenticated domains aligns with the **From** header domain, either exactly (strict mode) or as a subdomain (relaxed mode).

Failure of this domain alignment leads to DMARC failures and subsequent email rejection or quarantine, even if the SPF and DKIM records themselves are correctly published and valid.

This alignment focus ensures the authenticated identity matches the visible sender identity, preventing spoofing and improving email trustworthiness.

Related Content

- SPF Alignment Information
- DKIM Alignment Information
- Best Practice for Email Authentication - Optimal Ways to Deploy SPF, DKIM and DMARC - Cisco
- Configure Incoming Filter Based on DKIM Verification in ESA - Cisco