Email Security & Authentication Assessment

Zone: example.com

Weak
Score 57/100

Control snapshot
Pass 4 Warn 2 Fail 3 | Findings 5 | MX 0 | DKIM hits 26

Gaps and risks

MX records published: No MX records at apex. Aggregate reporting (rua): No rua= configured. MTA-STS: Not configured. 1 critical/high findings in the detailed table.

What is working

SPF default is hard fail (-all); SPF DNS lookup budget; DMARC organizational policy; DKIM DNS for probed selectors.

Executive actions

1. Publish MX records pointing at your inbound mail gateways.
2. Add rua=mailto:dmarc@yourdomain (and verify the mailbox).
3. Deploy MTA-STS (DNS TXT + HTTPS policy) to encourage encrypted SMTP between MTAs.
4. Publish TLSRPT v=TLSRPTv1 with rua= for visibility into SMTP TLS failures.

Control compliance matrix

Area	Control	Status	Detail
Inbound routing	MX records published	FAIL	No MX records at apex.
Sender policy (SPF)	SPF default is hard fail (-all)	PASS	Strongest SPF stance for unauthorized senders.
Sender policy (SPF)	SPF DNS lookup budget	PASS	Estimated 0 DNS lookups (under RFC 7208 limits).
Domain DMARC	DMARC organizational policy	PASS	p=reject protects the domain from unauthenticated use in many receivers.
Domain DMARC	Aggregate reporting (rua)	FAIL	No rua= configured.
DKIM	DKIM DNS for probed selectors	PASS	26 selector(s) publish DKIM keys.
Transport (MTA-STS)	MTA-STS	FAIL	Not configured.
Transport (TLS-RPT)	SMTP TLS reporting	WARN	No _smtp._tls record.
Brand (BIMI)	BIMI indicator record	WARN	Optional: no default._bimi record.

Inbound mail routing (MX)

No MX records returned for the zone apex.

Sender Policy Framework (SPF)

Attribute	Value
SPF record(s)	v=spf1 -all

Estimated DNS lookups	0
All mechanism	-all
Uses ptr	false

Domain-based Message Authentication (DMARC)

Tag / field	Value
Raw record	v=DMARC1;p=reject;sp=reject;adkim=s;aspf=s
p (policy)	reject
sp (subdomain)	reject
adkim	s
aspf	s

DKIM DNS discovery

Probed 26 common selectors. Matches: 26.

Selector	Found	Record / notes
default	yes	v=DKIM1; p=
google	yes	v=DKIM1; p=
selector1	yes	v=DKIM1; p=
selector2	yes	v=DKIM1; p=
k1	yes	v=DKIM1; p=
k2	yes	v=DKIM1; p=
s1	yes	v=DKIM1; p=
s2	yes	v=DKIM1; p=
mail	yes	v=DKIM1; p=
smtp	yes	v=DKIM1; p=
dkim	yes	v=DKIM1; p=
mandrill	yes	v=DKIM1; p=
cm	yes	v=DKIM1; p=
pic	yes	v=DKIM1; p=
hs1	yes	v=DKIM1; p=
hs2	yes	v=DKIM1; p=
protonmail	yes	v=DKIM1; p=
pm	yes	v=DKIM1; p=
resend	yes	v=DKIM1; p=
zendesk1	yes	v=DKIM1; p=
everlytic	yes	v=DKIM1; p=
mxvault	yes	v=DKIM1; p=
fm0	yes	v=DKIM1; p=
smtpapi	yes	v=DKIM1; p=
scph0823	yes	v=DKIM1; p=

amazonses	yes	v=DKIM1; p=

Mail transport security (MTA-STS, TLS-RPT, BIMI)

Control	Details
MTA-STS	Not configured (_mta-sts TXT missing).
TLS-RPT	No _smtp._tls TXT.
BIMI	Optional record not present.

Detailed findings

Severity	Category	Title	Detail / fix
HIGH	email_transport	No MX records	This apex has no MX; inbound SMTP may be undefined or use A/AAAA fallback only. Fix: Publish MX records pointing at your inbound mail gateways.
MEDIUM	email_auth	DMARC has no rua= aggregate reporting address	Without rua, you will not receive DMARC aggregate reports. Fix: Add rua=mailto:dmarc@yourdomain (and verify the mailbox).
MEDIUM	email_transport	MTA-STS not configured	No _mta-sts TXT or policy fetch attempted. Fix: Deploy MTA-STS (DNS TXT + HTTPS policy) to encourage encrypted SMTP between MTAs.
LOW	email_transport	TLS reporting (SMTP TLS) TXT not found	No _smtp._tls.example.com record. Fix: Publish TLSRPT v=TLSRPTv1 with rua= for visibility into SMTP TLS failures.
INFO	email_auth	DMARC DKIM alignment is strict (adkim=s)	Strict alignment can cause legitimate mail to fail if DKIM d= does not match From domain. Fix: Confirm all sending systems sign with aligned DKIM domains.

Prioritized remediation

1. Publish MX records pointing at your inbound mail gateways.
2. Add rua=mailto:dmarc@yourdomain (and verify the mailbox).
3. Deploy MTA-STS (DNS TXT + HTTPS policy) to encourage encrypted SMTP between MTAs.
4. Publish TLSRPT v=TLSRPTv1 with rua= for visibility into SMTP TLS failures.
5. Confirm all sending systems sign with aligned DKIM domains.
6. Resolve failed controls in the compliance matrix first, then tighten warn-level items.