TLS & Misconfiguration Baseline for SMEs

Version: 1.0
Audience: Small and Medium Enterprises (SMEs), IT & Security Teams
Purpose: Define a practical, low-cost baseline for securing TLS and eliminating common security misconfigurations in SME environments.

---

1. Introduction

Transport Layer Security (TLS) and secure configuration are critical to protecting data in transit and reducing exposure to common cyber attacks such as credential theft, session hijacking, and downgrade attacks.

This baseline provides **practical and achievable** recommendations for SMEs to:

- Enforce modern TLS versions
- Disable weak and deprecated protocols and ciphers
- Harden web servers and applications against common misconfigurations
- Improve overall security posture without expensive tooling

---

2. TLS Version Baseline

2.1 Required TLS Versions

- **Recommended to Allow:**
    - TLS **1.2**
    - TLS **1.3** (where supported)
- **Must Not Allow:**
    - SSLv2, SSLv3
    - TLS 1.0
    - TLS 1.1

These older protocols are considered insecure and may be rejected by modern browsers and compliance programs (e.g., PCI DSS).

---

3. Cipher Suite Baseline

3.1 Recommended Principles

- Prefer **strong, modern cipher suites** with:
    - Forward secrecy (ECDHE)
    - AES-GCM or CHACHA20-POLY1305
- Avoid or disable:
    - NULL ciphers
    - RC4, DES, 3DES
    - Export-grade ciphers
    - Anonymous or unauthenticated cipher suites

> For most SMEs using managed platforms (e.g., modern reverse proxies, cloud load balancers), selecting a modern “secure profile” is often sufficient.

---

4. Certificate Management Baseline

- Use certificates issued by **trusted Certificate Authorities (CAs)**.
- Ensure certificates:
    - Are valid (not expired)
    - Match the correct domain name
    - Use at least **2048-bit RSA** or equivalent ECC strength
- Use **Let's Encrypt** or similar services where cost is a concern.
- Implement certificate renewal processes and monitoring (e.g., alerts before expiry).

---

5. Web Server Configuration Baseline

5.1 Minimum Hardening Checklist

- ☐ Redirect all HTTP traffic to HTTPS (301 redirect)
- ☐ Disable weak protocols (SSLv2, SSLv3, TLS 1.0, TLS 1.1)
- ☐ Disable directory listing unless explicitly required
- ☐ Disable default/test pages (e.g., “It works!” pages)
- ☐ Remove or restrict access to admin consoles from the internet
- ☐ Restrict management interfaces to VPN or specific IPs
- ☐ Ensure error pages do not leak stack traces or internal paths

---

6. Security Headers Baseline

Add the following HTTP response headers where possible:

- `Strict-Transport-Security` (HSTS)
  - Example:
    `Strict-Transport-Security: max-age=31536000; includeSubDomains`
- `X-Content-Type-Options: nosniff`
- `X-Frame-Options: SAMEORIGIN` or `Content-Security-Policy` frame-ancestors equivalent
- `Referrer-Policy: strict-origin-when-cross-origin`
- `Content-Security-Policy` (CSP) – at least a basic policy to reduce XSS risk

These headers add layers of protection for browsers interacting with your applications.

---

7. Common Misconfigurations to Avoid

- Leaving **default credentials** enabled on admin interfaces
- Leaving **test or staging endpoints** exposed to the internet
- Exposing management ports (RDP, SSH, WinRM, SQL) directly to the internet
- Using self-signed certificates for public-facing systems
- Exposed `.git` or backup directories on web servers
- Allowing unrestricted file uploads without validation
- Misconfigured CORS policies allowing `*` from any origin

---

8. TLS & Misconfiguration Checks (Practical Steps)

8.1 External TLS Checks

Use tools such as:

- SSL Labs Server Test
- Built-in scanner scripts or open-source tools
- `openssl s_client` for basic checks

Verify:

- Only TLS 1.2 and 1.3 are enabled
- No weak ciphers are presented
- Certificate chain is valid

8.2 Internal Configuration Checks

- Periodically review web server configs (IIS, Nginx, Apache)
- Use security benchmarks (e.g., CIS Hardened Profiles)
- Scripted checks for:
  - Open management ports
  - Anonymous shares or exposed admin panels

---

9. Baseline for SMEs (Summary Table)

Area	Baseline Requirement
TLS Versions	Only TLS 1.2 and 1.3 enabled
Protocols	SSLv2/3, TLS 1.0/1.1 disabled
Ciphers	No RC4, DES, 3DES, EXPORT, NULL

Area	Baseline Requirement
Certificates	Publicly trusted, valid, ≥ 2048-bit RSA
HTTP	HTTP → HTTPS enforced
Security Headers	HSTS, X-Content-Type-Options, X-Frame-Options, CSP, Referrer-Policy
Management Interfaces	Not exposed directly to internet
Error Handling	No detailed error messages in production

---

10. Alignment to Standards

- **ISO 27001:** Supports controls related to secure communications and system hardening.
- **NIST CSF:** Aligns with Protect (PR), particularly PR.DS and PR.IP categories.
- **CIS Controls:** Supports secure configuration, boundary defence, and application security controls.

---

11. Implementation Roadmap for SMEs

1. **Phase 1 – Discovery (Week 1–2)**
    - Identify all public-facing domains and services
    - Run initial TLS / configuration checks
2. **Phase 2 – Remediation (Week 3–6)**
    - Disable legacy protocols and ciphers
    - Fix certificates and renew as needed
    - Lock down admin interfaces
3. **Phase 3 – Hardening (Week 7–10)**
    - Implement security headers
    - Review web/app configurations against baseline
4. **Phase 4 – Continuous Monitoring (Ongoing)**
    - Re-scan quarterly or after changes
    - Review certificates and renewals
    - Keep documentation updated

---

12. Document Control

Version	Date	Author	Notes
1.0	(Insert Date)	(Insert Name)	Initial baseline created