CIA Document

Network Operations Division Cryptographic Requirements[1]

Section 2.4, 19

Any transport layer encryption[2] **must** be layered over the cryptography[3] discussed in this document. Because this outer layer may be decrypted by an attacker (e.g., SSL Man-in-the-Middle) any transport encryption **must** be used for traffic blending[4] only and not for secrecy.

1. Top-secret classified document obtained by Wikileaks through Shadow Brokers
2. TLS (e.g. HTTPS)
3. Application level security
4. Request metadata leaks no information

Scenario