Evaluate the Performance Impact and Best Practices for SSL/TLS Decryption on FTD

Contents

Issue

A user is planning to enable SSL/TLS Decryption on a Firewall Threat Defense (FTD) device and needs to understand the potential impact on device performance before implementation. Key concerns include:

- Impact on firewall throughput, latency, and overall traffic processing performance.
- Expected CPU and memory utilization increase after enabling decryption.
- Sizing guidelines and performance benchmarks for specific FTD models.
- Recommended limits on concurrent decrypted sessions.
- Best practices and prerequisites for production deployment.

Environment

- Firepower 4115. Other hardware platforms can be also affected.
- FTD Version 7.4.2 (Build 172). Other software versions can be also affected.
- SSL/TLS Decryption feature consideration.
- Production environment deployment planning.

Resolution

SSL/TLS decryption does add processing overhead to the Firepower 4115, but the actual impact depends heavily on how much traffic is decrypted and what inspection is applied after decryption.

Performance Impact Analysis

SSL/TLS decryption impacts include:

- Lower effective throughput.
- Higher latency.
- Increased Snort/inspection CPU usage.
- CPU and memory increase that cannot be accurately predicted as a fixed percentage without real traffic profile analysis.

FPR 4115 Performance Benchmarks

Published Cisco Firepower 4115 benchmark specifications:

- TLS hardware decryption throughput: 6.5 Gbps.
- FW + AVC throughput: 33 Gbps.
- Maximum concurrent sessions with AVC: 15 million.
- Maximum new connections per second with AVC: 210K.

Important sizing note: The 6.5 Gbps TLS hardware decryption benchmark is based on specific test conditions. Production throughput can be lower if you decrypt a large percentage of traffic, inspect decrypted traffic with Intrusion/File/Malware policies, or process many short-lived TLS sessions.

Cisco does not publish a separate "maximum concurrent decrypted sessions" number for Firepower 4115 on FTD 7.4.2. In practice, capacity is validated using traffic mix, concurrent sessions, connection rate, cipher suites, and inspection policy load.

Recommended Production Deployment Approach

Step 1: Start with a Limited Pilot

- Do not enable broad "decrypt all" rules initially.
- Start with selected users, subnets, or destination categories.
- Keep default handling conservative with Do Not Decrypt for traffic that does not require inspection.

Step 2: Exclude Traffic that Commonly Breaks with Decryption

Banking/financial sites.

- Healthcare portals.
- Certificate-pinned applications.
- Some Software as a Service (SaaS) and endpoint security/cloud applications.
- Sensitive business-critical applications unless explicitly tested.

Step 3: Keep SSL Rules simple and Ordered Carefully

- Put specific Do Not Decrypt exclusions beyond broader decrypt rules.
- Avoid overly broad or complex matching where possible.
- Do not use TLS version or cipher-suite conditions for Decrypt-Resign/Known-Key rules, as Cisco documents this can cause unpredictable behavior.

Step 4: Validate Certificate Readiness

- For outbound Decrypt-Resign, the signing CA certificate must be trusted by client endpoints.
- For inbound Known-Key decryption, the firewall must have the correct server certificate/private key material.

Step 5: Monitor during Rollout

- Track overall CPU and, more importantly, Snort/inspection CPU utilization.
- Track concurrent connections and new connections per second.
- Review SSL flow status/handshake errors in connection events.
- Watch for TLS oversubscription indicators and application-specific failures.

For more information on how to monitor the CPU check:

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- Think Like a TAC Engineer: A guide to Cisco Secure Firewall most common pain points

For tracking connections and new connections per second check:

- Logging Best Practices

For tracking SSL flow status/handshake errors in connection events check and TLS oversubscription indicators check:

- Troubleshoot TLS/SSL oversubscription

Step 6: Roll Back or Narrow Scope

Roll back or narrow scope if you see:

- Sustained inspection CPU saturation.
- User-visible latency increase.
- TLS handshake failures.
- Business applications failing after decryption.
- Oversubscription or excessive SSL errors.

Step 7: Consider TLS 1.3 Impact

TLS 1.3 adoption can affect visibility and behavior, as certain handshake and inspection characteristics

differ from TLS 1.2.

Cause

SSL/TLS decryption requires additional computational resources to decrypt, inspect, and re-encrypt traffic flows. The performance impact varies significantly based on traffic patterns, inspection policies applied to decrypted traffic, and the specific deployment configuration. Without proper planning and gradual implementation, organizations can experience unexpected performance degradation in production environments.

Related Content

- Cisco Secure Firewall Management Center Device Configuration Guide - Decryption Rules
- Cisco Secure Firewall Decryption Policy Guidance
- Best Practice for Decryption Policy Rule Order
- Simplifying Decryption With Cisco Secure Firewall 7.7
- Decryption Rules Best Practices
- Cisco Firepower 4100 Series Data Sheet
- Cisco Technical Support & Downloads