FTDでのSSL/TLS復号化のパフォーマンスへの影響とベストプラクティスの評価

内容

お問い合わせ内容

ユーザは、ファイアウォール脅威対策(FTD)デバイスでSSL/TLS復号化を有効にすることを計画しており、実装前にデバイスのパフォーマンスに対する潜在的な影響を理解する必要があります。主な懸念事項は次のとおりです。

- ファイアウォールのスループット、遅延、全体的なトラフィック処理パフォーマンスに影響を与える。
- 復号化を有効にすると、予想されるCPUとメモリの使用率が増加します。
- 特定のFTDモデルのサイジングガイドラインとパフォーマンスベンチマーク
- 同時復号化セッションに推奨される制限。
- 実稼働導入のベストプラクティスと前提条件

環境

- Firepower 4115。他のハードウェアプラットフォームも影響を受ける可能性があります。
- FTDバージョン7.4.2（ビルド172）。 他のソフトウェアバージョンも影響を受ける可能性があります。
- SSL/TLS復号化機能の考慮事項。
- 実稼働環境の導入計画。

解決策

SSL/TLS復号化はFirepower 4115に処理のオーバーヘッドを追加しますが、実際の影響は復号化されるトラフィックの量と復号化後に適用される検査によって大きく異なります。

パフォーマンス影響分析

SSL/TLS復号化の影響には、次のようなものがあります。

- 有効スループットの低下。
- 遅延の増大
- Snort/インスペクションのCPU使用率の向上
- CPUとメモリの増加は、実際のトラフィックプロファイル分析なしでは一定の割合として正確に予測できません。

FPR 4115パフォーマンスベンチマーク

シスコが公開したFirepower 4115ベンチマーク仕様：

- TLSハードウェア復号スループット：6.5 Gbps
- FW + AVCスループット：33 Gbps
- AVCとの最大同時セッション数：1,500万
- AVCでの1秒あたりの最大新規接続数：210K

重要なサイジングに関する注意事項：6.5 Gbps TLSハードウェア復号化ベンチマークは、特定のテスト条件に基づいています。実稼働スループットは、大量のトラフィックの復号化、侵入/ファイル/マルウェアポリシーを使用した復号化されたトラフィックの検査、または短時間のTLSセッションを多数処理する場合に低くなる可能性があります。

シスコは、FTD 7.4.2でFirepower 4115の個別の「最大同時復号化セッション」数を公開していません。実際には、トラフィックミックス、同時セッション、接続レート、暗号スイート、およびインスペクションポリシーのロードを使用して容量が検証されます。

推奨される実稼働導入アプローチ

ステップ1：限定的なパイロット運用の開始

- 最初は幅広い「すべて復号化」ルールを有効にしないでください。
- 選択したユーザ、サブネット、または宛先カテゴリから開始します。
- 検査を必要としないトラフィックについては、「復号化しない」を使用してデフォルトの処理を控えめに行ってください。

手順2：復号化で中断されることが多いトラフィックを除外します

- 銀行/金融サイト
- 医療ポータル
- 証明書で固定されたアプリケーション。
- 一部のSoftware as a Service(SaaS)およびエンドポイントセキュリティ/クラウドアプリケーション
- 明示的にテストされていない限り、ビジネスに不可欠な機密アプリケーション。

ステップ3:SSLルールをシンプルにし、慎重に並べ替える

- より広範な復号化ルールの上に、特定の非暗号化除外を置きます。
- 可能な限り、過度に広い範囲での照合や複雑な照合は避けてください。
- Ciscoがドキュメントで説明しているように、復号化 – 再署名/既知キーのルールにTLSバージョンや暗号スイートの条件を使用しないでください。使用すると、予期しない動作が発生する可能性があります。

ステップ4：証明書の準備状況の検証

- 発信側での復号化 – 再署名の場合、署名CA証明書はクライアントエンドポイントによって信頼されている必要があります。
- 着信の既知のキーの復号化では、ファイアウォールに正しいサーバ証明書と秘密キーの内容

が必要です。

ステップ5：ロールアウト中のモニタ

- 全体的なCPUを追跡し、さらに重要な点として、Snort/inspectionのCPU使用率を追跡します。
- 同時接続と新規接続を1秒あたりに追跡します。
- 接続イベントのSSLフローステータス/ハンドシェイクエラーを確認します。
- TLSオーバーサブスクリプションインジケータとアプリケーション固有の障害に注意してください。

CPUチェックを監視する方法の詳細については、次を参照してください。

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- TACエンジニアのように考える：Cisco Secure Firewallの最も一般的な課題のガイド

接続の追跡および1秒当たりの新規接続のチェックの場合：

- ロギングのベスト プラクティス

接続イベントのチェックおよびTLSオーバーサブスクリプションインジケータのチェックでSSLフローステータス/ハンドシェイクエラーを追跡するには、次の項目をチェックします。

- TLS/SSLのオーバーサブスクリプションのトラブルシューティング

ステップ6：ロールバックまたはスコープの絞り込み（次の場合）：

- CPU飽和状態の継続的なインスペクション。
- ユーザが認識できる遅延の増加
- TLSハンドシェイクの失敗。
- 復号後にビジネスアプリケーションが失敗する。
- オーバーサブスクリプションまたは過剰なSSLエラー。

ステップ7:TLS 1.3の影響の検討

特定のハンドシェイクおよびインスペクションの特性がTLS 1.2と異なるため、TLS 1.3の採用は可視性と動作に影響を与える可能性があります。

原因

SSL/TLS復号化では、トラフィックフローを復号化、検査、および再暗号化するために、追加の計算リソースが必要です。パフォーマンスへの影響は、トラフィックパターン、復号化されたトラフィックに適用されるインスペクションポリシー、および特定の導入設定によって大きく異なります。適切な計画と段階的な実装を行わないと、本番環境で予期しないパフォーマンスの低下が発生する可能性があります。

関連コンテンツ

- Cisco Secure Firewall Management Centerデバイス設定ガイド – 復号ルール
- Cisco Secure Firewall復号ポリシーガイダンス
- 復号ポリシールールの順序に関するベストプラクティス
- Cisco Secure Firewall 7.7で復号化を簡素化
- 復号化ルールのベストプラクティス
- Cisco Firepower 4100シリーズデータシート
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。