paloalto TECHDOCS

復号化のベストプラクティス

Version 10.2

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

January 18, 2022

Table of Contents

復号化のベストプラクティス

表示および検査できない脅威からネットワークを保護することはできません。Gartnerは、2020年には、新しいマルウェアキャンペーンの約70%がさまざまな形式の暗号化を使用したと述べています。Googleの 透明性レポート は、GoogleのWebトラフィックをどのように分析しても、ほとんどの場合、最大95%が暗号化されていることを示しています。復号化 そのトラフィックは、隠れた脅威からネットワークを保護します。

このドキュメントは、復号化を実装するために従うことができる、展開前、展開、および展開後のベストプラクティスの合理化されたチェックリストです。各セクションには、復号化ポリシーのルールとプロファイルの構成方法など、PAN-OS管理ガイドの詳細情報へのリンクが含まれています。

- SSL復号化のベストプラクティスの導入を計画する
- ベストプラクティスを使用してSSL復号化を展開する
- 導入後のSSL復号化のベストプラクティスに従う

SSL 復号化のベストプラクティスの展開を計画する

復号化を展開する準備をする 復号化戦略とロールアウト計画を策定することによって。復号化を有効にすると、ユーザーが一部のアプリケーションや Web サイトを操作する方法が変わる可能性があるため、計画、テスト、およびユーザー教育は、展開を成功させるために不可欠です。

STEP 1 | 目標を設定します。

- プライベートでも機密でもないトラフィックをファイアウォールと同じだけ復号化するように計画する リソース 許可する。これにより、暗号化された脅威を暴露して防止することにより、攻撃対象領域が減少します。法的に復号化できるトラフィックとユーザー通知要件に関する現地の法律と規制を理解します。
- ポートベースからアプリケーションベースへの移行 セキュリティー 復号化ポリシールールを作成して展開する前に、ポリシールールを作成します。ポートベースのセキュリティポリシーに基づいて復号化ルールを作成し、アプリケーションベースのセキュリティポリシーに移行すると、セキュリティポリシールールがアプリケーションのデフォルトポートを使用してトラフィックが非標準ポート。復号化を展開する前にアプリ ID ベースのルールに移行すると、復号化の展開をテストするときに、セキュリティポリシーの設定ミスを発見し、復号化を一般ユーザーに展開する前に修正できます。

STEP 2 | 利害関係者と協力して教育する 法務、財務、人事、役員、セキュリティ、IT/サポートなど、復号化の展開戦略を策定します。

- 企業を保護するためにトラフィックを復号化するために必要な承認を取得します。
- 復号化するトラフィックを特定し、優先順位を付けます。
  - 復号化するアプリケーション (認可済み、非認可) を決定します。暗号化された認可されていないアプリケーションは許可しないでください。
  - 復号化するデバイス (企業、BYOD、モバイルなど) を決定します。

    企業は*BYOD*デバイスを制御しません。ネットワーク上で *BYOD* デバイスを許可する場合は、そのトラフィックを復号化し、他のネットワークトラフィックに適用するのと同じセキュリティポリシーを適用します。これを行うには、認証ポータルを介して *BYOD* ユーザーをリダイレクトし、*CA* 証明書をダウンロードしてインストールする方法を指示し、トラフィックが復号化されることをユーザーに明確に通知します。プロセスについて*BYOD*ユーザーを教育し、それを会社のプライバシーおよびコンピューター使用ポリシーに含めます。
  - 異なる従業員グループ、請負業者、パートナー、ゲストなど、異なるグループに同じ復号化ポリシーを使用するかどうかを決定します。
- 復号できないトラフィックを特定する:
  - 復号化を中断するトラフィック 技術的な理由 証明書のピン留め、サポートされていない暗号、相互認証などです。
  - あなたがするトラフィック 復号化しないことを選ぶ 財務、健康、政府、その他のデリケートなカテゴリ（ユーザーやエグゼクティブなどのグループを含む）など。
  - 復号化以外のトラフィックを完全に理解する。暗号化されたトラフィックを可視化できず、ファイアウォールは暗号化されたトラフィックに脅威防止プロファイルを適用できません。
- すべての従業員、請負業者、パートナー、ゲスト、およびその他のネットワークユーザーに配布する最新の法律および人事コンピューター使用ポリシーを準備して、復号化を展開したときに、ユーザーがデータを復号化して脅威をスキャンできることをユーザーが理解できるようにします。
- 方法を決める 証明書検証を処理する.ビジネスモデルでは、セキュリティとユーザーエクスペリエンスのトレードオフが必要になる場合があります。証明書検証の処理方法を理解することは、SSL 転送プロキシ復号化プロファイルの設定方法を決定するのに役立ちます。
- ログに記録するトラフィックを特定します。地域の法的および規制の違いと、それらがログに記録できるトラフィックとログを保存できる場所にどのように影響するかを認識してください。

すべてのネットワークトラフィックを確認できる場所にファイアウォールを配置し、暗号化されたトラフィックがファイアウォールをバイパスしてネットワークに不注意でアクセスしないようにします。

STEP 3 | ロールアウトの計画を策定する 公開鍵基盤 (PKI).

- 既存の PKI がある場合は、エンタープライズルート CA から SSL 転送信頼 CA 証明書を下位証明書として生成します。これにより、ネットワークデバイスはすでにエンタープライズルートCAを信頼しているため、証明書の問題が発生しないため、展開が容易になります。エンタープライズルート CA がない場合は、取得することを検討してください。

  または、ファイアウォールで自己署名のルート CA 証明書を生成し、そのファイアウォールに従属する Forward Trust CA 証明書を作成してネットワークデバイスにインストールします。自己署名証明書は、エンタープライズルート CA を持たない小規模企業や、概念実証 (POC) トライアルに最適です。

  BYOD デバイスと同様に、企業はゲストデバイスを制御しません。ネットワーク上でゲストデバイスを許可する場合は、そのトラフィックを復号化し、他のネットワークトラフィックに適用するのと同じセキュリティポリシーを適用します。これを行うには、認証ポータルを介してゲストユーザーをリダイレクトし、*CA* 証明書をダウンロードしてインストールする方法を指示し、トラフィックが復号化されることをユーザーに明確に通知します。会社のプライバシーとコンピュータの使用に関するポリシーにそのプロセスを含めてください。

- 生成 別れる 前方信頼と前方不信用のCA証明書。両方の証明書に同じ PKI 下位 CA を使用しないでください。また、信頼されたルート CA で Forward Untrust 証明書に署名しないでください。Forward Untrust証明書は、サーバーに署名する証明書が正当ではないため、サイトに移動してはならないことをユーザーに警告します。信頼されたルート CA が Untrust 証明書に署名すると、クライアントはルート CA を信頼するため、信頼できないはずの証明書を信頼します。
- ファイアウォールごとに個別の下位Forward Trust CA証明書を生成します。個別の下位 CA を使用すると、次のことが可能になります。 証明書を取り消す 展開の残りの部分に影響を与えずにデバイス（またはデバイスペア）を使用停止し、証明書を取り消す必要がある場合の影響を軽減します。証明書エラーメッセージには、トラフィックが通過したファイアウォールに関する情報が含まれているため、個別の CA 証明書はテクニカルサポートがユーザの問題のトラブルシューティングに役立ちます。すべてのファイアウォールで 1 つの Forward Trust 下位 CA を使用する方が簡単に展開できますが、各ファイアウォールで個別の証明書を使用すると最高のセキュリティが得られます。
- 秘密鍵のセキュリティを強化する必要がある場合は、 それらをHSMに保存する.

STEP 4 | ファイアウォールパフォーマンスのベースライン測定を行い、リソース消費量と使用可能なファイアウォールリソースを把握し、復号化を展開した後にパフォーマンスを比較し、ファイアウォール展開のサイズ 復号化するトラフィック量をサポートするために必要です。

- パロアルトネットワークスのSE/CEと協力して、ファイアウォールの配置をサイジングし、サイジングミスを回避します。

- 現在利用可能なファイアウォールリソースをメモします。一般に、セキュリティが厳しくなればなるほど、復号化により多くのリソースが消費されます。復号化できるトラフィックの量に影響する要因には、次のものがあります。
  - 復号化する SSL トラフィックの量。
  - TLS プロトコルバージョン。
  - キーサイズ。
  - キー交換アルゴリズム。DHE や ECDHE などの完全転送秘密 (PFS) エフェメラルアルゴリズムは RSA よりも多くのリソースを消費しますが、ファイアウォールがセッションごとに新しい暗号鍵を生成するため、セキュリティが向上します。攻撃者がセッションキーを侵害した場合、PFSは攻撃者がそれを使用して同じクライアントとサーバー間の他のセッションを復号化するのを防ぎますが、RSAはそうしません。
  - 証明書認証。RSA 証明書認証（これは RSA キー交換アルゴリズムとは異なります）は、ECDSA 証明書認証よりも消費する CPU サイクルが少なくなりますが、ECDSA は最高レベルのセキュリティを提供します。
  - 暗号化アルゴリズム。鍵交換アルゴリズムは、暗号化アルゴリズムがPFSかRSAかを決定します。
  - の ファイアウォールのモデルとリソース.新しいファイアウォールモデルには、古いモデルよりも多くのリソースがあります。
- トランザクションサイズはパフォーマンスに影響します。すべてのトラフィックの平均トランザクションサイズを測定し、ポート 443（HTTPS 暗号化トラフィックのデフォルトポート）のトラフィックの平均トランザクションサイズを測定して、総トラフィックと平均トランザクションサイズに対するファイアウォール上の暗号化トラフィックの割合を把握します。

これらの要素の組み合わせによって、復号化がファイアウォールの処理リソースを消費する方法が決まります。ファイアウォールリソースに問題がある場合は、優先順位が高くリスクの高いトラフィックにはより強力な復号化を使用し、使用可能なリソースを増やすことができるまで、プロセッサ負荷の低い復号化を使用して優先順位の低いトラフィックを復号化および検査します。

毎日暗号化されるトラフィックが増えるため、復号化するトラフィック量の増加に備えてファイアウォールのサイズを調整します。

STEP 5 | 段階的で優先順位付けされた展開を計画する.

- 復号化を推進するアーリーアダプターを特定し、部門マネージャーに計画を組み込ませます。
- POCをセットアップして、一般ユーザー集団に展開する前に展開戦略をテストします。復号化POC展開がファイアウォールのCPUとメモリの使用率にどのように影響するかを測定し、ファイアウォールのサイジングが正しいかどうかを理解するのに役立ちます。POCは、技術的に復号化を破るアプリケーションを明らかにすることもできます。
  - POC参加者に変更点とテクニカルサポートへの連絡方法を教育します。
  - 復号化POCのテクニカルサポートPOCを設定し、サポートがロールアウトをサポートする最善の方法を開発する機会を得られるようにします。

- 復号化のフェーズ。最初に最もリスクの高いトラフィック（ゲームや高リスクなどの悪意のあるトラフィックを含む可能性が最も高い URL カテゴリ）を復号化し、経験を積むにつれてさらに復号化することを計画します。または、ニュースフィードなど、ビジネスに影響を与えないURLカテゴリを最初に復号化します（何か問題が発生しても、ビジネスには影響しません）。どちらの場合も、いくつかの URL カテゴリを復号化し、ユーザーのフィードバックを聞き、レポートを実行して、 復号化ログ 復号化が期待どおりに機能していることを確認し、さらにいくつかの URL カテゴリなどを徐々に復号化します。作る計画 復号化除外 技術的な理由または復号化しないことを選択したためにサイトを復号化できない場合に、サイトを復号化から除外します。
- POCの成功を評価し、導入方法を微調整します。

- 一般的なロールアウトの前にユーザー人口を教育します。POCは、コミュニケーションの最も重要なポイントを特定するのに役立ちます。
- すべての従業員、請負業者、パートナー、ゲスト、およびその他のネットワークユーザーに、最新の法律および人事コンピューター使用ポリシーを配布します。各部門またはグループに復号化をロールアウトするときに、データを復号化して脅威をスキャンできることを全員に理解してもらいます。
- ロールアウトの各段階を評価する時間を確保する現実的なスケジュールを作成します。

ベストプラクティスを使用して SSL 復号化をデプロイする

STEP 1 | 生成して配布 復号化ポリシーのキーと証明書.

- エンタープライズ PKI がある場合は、エンタープライズルート CA からの転送プロキシトラフィック用の Forward Trust CA 証明書を生成します。それ以外の場合は、ファイアウォールで自己署名のルート CA 証明書を生成し、そのファイアウォールで下位 CA を作成し、自己署名証明書をすべてのクライアントシステムに配布します。自己署名証明書は、ラボテスト、小規模な展開、および POC を対象としています。
- ファイアウォールごとに一意の下位Forward Trust CA（または、すべてのファイアウォールに対して 1 つの転送信頼 CA）を生成します。 計画—1 つの証明書は展開が簡単ですが、別々の証明書が最高のセキュリティとその他の利点を提供します)。PKI プラットフォームが異なれば、証明書管理を拡張するための機能が異なります。
- エンタープライズ CA を使用しない場合は、Forward Trust CA 証明書をクライアントシステムの信頼 CA ストレージにインポートします。
- Forwardをインポートしないでください 信用できない クライアントシステムの CA 信頼ストレージへの CA 証明書または信頼できない証明書は、信頼できないサイトのトリガーとして機能しません。ただし、ファイアウォールの自己署名ルート CA がクライアントシステムに信頼された発行元としてインストールされていない場合は、自己署名の Forward Untrust 証明書を使用できます。
- を使う 自動化された方法 Forward Trust 証明書を、パロアルトネットワークスの GlobalProtect ポータル、Microsoft AD 証明書サービス (グループポリシーオブジェクトを使用)、商用ツール、またはオープンソースツールなどの接続されたデバイスに配布します。
- エンタープライズルート CA から証明書を生成する場合は、ファイアウォールに証明書をインポートします。
- ファイアウォールの Forward Trust CA 証明書 (ファイアウォールのマスターキーではない) の秘密キーを安全なリポジトリにバックアップして、問題が発生した場合でも Forward Trust CA 証明書にアクセスできるようにします。
- エンタープライズルート CA から証明書と秘密キーを生成する場合、秘密鍵のエクスポートをブロックする.（エンタープライズ CA から新しいファイアウォールやパノラマにインストールできるので、PAN-OS からエクスポートする必要はありません）。
- あなたのプランでHSMの使用が必要な場合、プライベートキーを HSM に保存する.

STEP 2 | 復号化プロファイルを構成する プロトコル、証明書検証、障害処理を制御します。

- SSL フォワードプロキシ復号化プロファイル サーバー証明書の検証、セッションモード、アウトバウンドトラフィックの障害チェックを制御します。期限切れの証明書、信頼できない発行者、サポートされていないバージョン、およびサポートされていない暗号スイートを含むセッションをブロックします。重要なアプリケーションで要求されない限り、クライアント認証によるセッションをブロックします。その場合は、クライアント認証を許

可する別の復号化プロファイルを作成し、クライアント認証を必要とするトラフィックにのみ適用する必要があります。

- SSL インバウンド検査復号化プロファイル インバウンドトラフィックのセッションモードと障害チェックを制御します。サポートされていないバージョンとサポートされていない暗号スイートを含むセッションをブロックします。
- SSL プロトコル設定 制御暗号スイート要素：プロトコルバージョン、キー交換アルゴリズム、暗号化アルゴリズム、SSL Forward Proxy および SSL インバウンドインスペクショントラフィックの認証アルゴリズム。できる限り強力な暗号を使用してください。[転送プロキシ] で、プロトコルを設定します 最小バージョン に **TLSv1.2** そして 最大バージョン にマックス 弱いプロトコルをブロックする。SSL インバウンドインスペクションの場合は、インバウンドトラフィックを検査するサーバの機能と一致するプロトコル設定を持つ個別のプロファイルを作成します。

  できる限り強力な暗号スイートを使用してください。セキュリティを最大化するために、個別の復号化ポリシーとプロファイルを作成します。ビジネス目的で必要なレガシーサイトがより弱い暗号のみをサポートしている場合は、別の復号化プロファイルを作成してそのトラフィックを許可し、復号化ポリシーで必要なサイトのみに適用します。同じ手法を使用して、さまざまな *URL* カテゴリのセキュリティとパフォーマンスを微調整します。

  多くのモバイルアプリケーションは、ピン留めされた証明書を使用します。*TLSv1.3*は証明書情報を暗号化するため、ファイアウォールはこれらのモバイルアプリケーションを*SSL*復号除外リストに自動的に追加できません。これらのアプリケーションでは、復号化プロファイルが 最大バージョン が *TLSv1.2* に設定されているか、*No Decryption* ポリシーをトラフィックに適用します。

- 復号化プロファイルなし 復号化しないことを選択したトラフィックのサーバー証明書検証を制御します。期限切れの証明書と信頼できない発行者とのセッションをブロックします。

  復号化なしプロファイルを *TLSv1.3* トラフィックに適用しないでください。証明書情報は暗号化されているため、ファイアウォールは証明書情報に基づいてセッションをブロックできません。

- SSL 転送プロキシトラフィックと復号化なしトラフィックの場合は、証明書失効リスト (CRL) とオンライン証明書ステータス失効 (OCSP) の両方を構成します。 証明書失効 サイト証明書が取り消されていないことを確認します。
- SSH プロキシプロファイル SSH トンネルトラフィックのセッションモードと障害チェックを制御します。サポートされていないバージョンとサポートされていないアルゴリズムを含むセッションをブロックします。

の復号化プロファイル設定のベストプラクティス データセンター そして周囲 (インターネットゲートウェイ) ユースケースは、一般的なベストプラクティスの設定とは少し異なります。

STEP 3 | 環境設定 復号化ポリシールール 復号化して作るトラフィックを定義する ポリシーベースの例外 交通のせい 選ぶ 解読しないで。

- 特定の宛先IPアドレス（財務サーバなど）、ソースユーザーとグループ（エグゼクティブや人事担当者など）、ソースデバイス、および復号化しないことを選択したアプリケーションポートを除外するポリシールールを作成します。これらのルールは、トラフィックを復号化するルールの前に、復号ルールベースの最上部に配置します。TLSv1.3トラフィックを除くすべてのトラフィックに対して、復号化なしのプロファイルをアタッチしてSSLを適用します サーバー証明書検証コントロール 暗号化されたトラフィックに。これにより、復号したくないトラフィックが不注意に復号化されるのを防ぎます。
- [URL カテゴリ]、[カスタム URL カテゴリ]、および [外部動的リスト (EDL)] を使用して、復号しない URL を指定します。たとえば、金融サービス、医療機関、政府、およびビジネス、法律、規制上の理由で復号したくないその他のカテゴリなどです。IP アドレスが動的に変更される環境 (Office 365 など) や、メンバーシップが頻繁に変更される環境で EDL を使用すると、コミットせずに更新できます。

  復号化しないことを選択したすべてのカテゴリを含む EDL またはカスタム URL カテゴリを作成します。これにより、復号化ポリシールールが 1 つだけ必要になります。

  これらのルールは、復号ルールベースのトラフィックを復号化するルールの上に配置します。
- 環境設定 復号化ログとログ転送.
- あなたが使うなら 復号化ミラーリング 復号化されたトラフィックをコピーしてトラフィック収集ツールに送信するには、ミラーリングを禁止したり、ミラーリングできるトラフィックを制御したりする地域のプライバシー規制に注意してください。
- 構成することにより、残りのトラフィックを復号するポリシーを作成します SSL フォワードプロキシ,SSL インバウンド検査、および SSH プロキシ ルール。オンラインストレージとバックアップ、Webベースの電子メール、Webホスティング、個人用サイトとブログ、コンテンツ配信ネットワーク、およびリスクの高いURLカテゴリを常に復号化します。SSH プロキシをネットワークデバイスを管理する管理者に制限し、すべての SSH トラフィックをログに記録し、 多要素認証 不正な SSH アクセスを防ぐため。

STEP 4 | サイトを SSL 復号化除外リスト (端末 > 証明書管理 > **SSL** 復号化除外）は、POCテスト中に技術的に復号化を破り、まだ除外リストに含まれていない場合。（復号化をブロックするサイトを復号化すると、技術的にはそのトラフィックがブロックされます）。

STEP 5 | セキュリティポリシーでは、クイック UDP インターネット接続 (QUIC) プロトコルをブロックする.

Chromeや他の一部のブラウザは、TLSの代わりにQUICを使用してセッションを確立しますが、QUICはファイアウォールが復号化できない独自の暗号化を使用しているため、潜在的に危険なトラフィックが暗号化されたトラフィックとしてネットワークに入る可能性があります。2 つのルールを作成します。1 つは標準ポートで QUIC アプリケーションをブロックし、もう 1 つは UDP ポート 80 と 443 をブロックするルールです。QUIC をブロックすると、ブラウザは TLS を使用するようになります。

STEP 6 | 復号化されたトラフィックをWildFireに転送する マルウェアの有無を検査します。

STEP 7 | 復号化をゆっくりロールアウトする.

いくつかの URL カテゴリを復号化し、ユーザーのフィードバックを確認し、レポートを実行して、復号化が期待どおりに機能することを確認します。目標に到達するまで、徐々に多くの URL カテゴリを復号化します。優先度が最も高いトラフィック (ゲームなどの悪意のあるトラフィックを潜んでいる可能性が最も高い URL カテゴリ) から始めて、経験から学び、プロセスを改善するにつれてさらに暗号化を解除します。より控えめな代替手段は、ビジネスに影響を与えないURLカテゴリ（ニュースフィードなど）を最初に復号化することです。

導入後の SSL 復号化のベストプラクティスに従う

復号化を展開したら、すべてが期待どおりに機能していることを確認し、期待どおりに機能し続けるための手順を実行します。

STEP 1 | 検証 その復号化は期待どおりに機能します。

STEP 2 | ファイアウォールのパフォーマンスを測定して、許容範囲内にあることを確認し、復号化がパフォーマンスに及ぼす影響を理解できるようにします。

ファイアウォールリソースがサポートするよりも多くのトラフィックを復号化する場合は、復号化するすべてのトラフィックを復号化してネットワークを保護するのに十分なリソースを確保できるようにスケールアップします。

STEP 3 | 採用時に新入社員を教育して、復号ポリシーを理解してもらい、弱い暗号スイートを使用しているために特定のサイトにアクセスできなくても驚かないようにします。

STEP 4 | 復号化ポリシーとプロファイルを定期的に確認して更新します。

STEP 5 | 使う 復号化トラブルシューティングツール アプリケーションコマンドセンターの **SSL** アクティビティ ウィジェットと復号化ログ (モニター > ログ > 復号化) を使用して、復号トラフィックを監視し、復号化の問題を解決します。

復号化トラブルシューティングワークフローの例 ツールを使用して問題を調査する方法を示します。

STEP 6 | ファイアウォールが実行するサーバー上の証明書を変更する必要がある場合 SSL インバウンド検査,新しい証明書を追加する サーバーに変更を加える前に、そのサーバーの復号化ポリシールールに追加します。復号化ポリシールールは複数のサーバー証明書をサポートしているため、古い証明書を保持し、新しい証明書をルールに追加することもできます。これにより、ファイアウォールに古い証明書しかない場合に、サーバー上の証明書を変更することによる復号化の中断を回避できます。新しいサーバー証明書を復号化ポリシールールに追加すると、サーバー上の証明書を変更したときに、トラフィックをシームレスに復号化し続けるための適切な証明書がファイアウォールに確保されます。

サーバー証明書を変更した後は、必ず復号化ポリシールールとファイアウォールから無効な証明書を削除してください。

STEP 7 | パロアルトネットワークスのドキュメントやその他のリソースを使用して、復号化の詳細を学び、情報を調べてください。

- の PAN-OS 管理者ガイド では、パロアルトネットワークスの次世代ファイアウォールに関する詳細情報を提供しています。
- パロアルトネットワークスのライブコミュニティには 復号化リソースリスト 復号化の構成、設定、および管理に関する記事の。
- 不足している中間証明書を見つけるには、 SSL ラボ (クアリス).
- サーバーがサポートする暗号スイートを確認するには、Qualys SSL Labs にアクセスしてください。 サーバー SSL テストページ.
- 世界で最も人気のある150,000のサイトで使用されているさまざまな暗号とプロトコルの割合に関する最新の統計情報を確認し、傾向を確認し、より安全な暗号とプロトコルに対する世界的なサポートがどれほど広まっているかを理解するには、Qualys SSL Labsにアクセスしてください。 SSL パルスページ.