復号化のベストプラクティス

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

October 28, 2020

Table of Contents

復号化のベスト プラクティス

見ることも検査することも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、70パーセントを超える新たなマルウェアキャンペーンがさまざまな形態の暗号化を使用するだろうと予測しています。GoogleのTransparency Report（透過性レポート）は、Google Webトラフィックをどのように解析したとしても、たいていの場合その90パーセントが暗号化されていると報告しています。隠れている脅威からネットワークを保護するためにトラフィックを復号化

この文書は復号化を実装するために段階的に行うことが可能なデプロイメント前、デプロイメント時、およびデプロイメント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。それぞれのセクションには、復号化ポリシールールおよびプロファイルの設定方法を含む PAN-OS Admin ガイドについての詳細な情報へのリンクが含まれています。

- SSL 復号化のベスト プラクティスのデプロイメントを計画する
- ベストプラクティスを用いてSSL復号化を展開する
- SSL 復号化デプロイメント後のベスト プラクティスをフォローする

SSL 復号化のベスト プラクティスのデプロイメントを計画する

復号化戦略とロールアウトプランを開発することで復号化の展開を準備します。復号化をオンにすることは、ユーザーによるアプリケーションやウェブサイトへのかかわり方を変える場合があるので、計画、テスト、さらにユーザー教育がデプロイメントの成功に不可欠です。

STEP 1 | ゴール設定。

- ファイアウォールのリソースが許す限り、プライベートまたは機密情報ではないトラフィックをできる限り復号化するようにしてください。そうすることによって、暗号化された脅威を検出、防止することで、攻撃面を減らします。合法的に復号化できるトラフィックおよびユーザー通知要件についての現地法と規制を理解します。
- 復号化ポリシー ルールを作成してデプロイする前に、ポートベースからアプリケーション ベースのセキュリティポリシールールへと移行します。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、その後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 ポートを使用して標準以外のポートを使用するトラフィックを防止する可能性が高いため、その変更により、許可する予定のトラフィックが復号化ルールによってブロックされる可能性があります。復号化の展開前にアプリIDベースのルールに移行することにより、復号化の展開をテストし、セキュリティポリシーの誤設定を見つけ出し、一般ユーザーに復号化を展開する前にそれらを修正することが可能です。

STEP 2 | 法務、財務、HR、経営陣、セキュリティ、および IT/サポートなどの意思決定者と共に作業し教育して 復号化の展開戦略を開発します。

- 企業を保護するためにトラフィックを復号化するための必要な許可を得ます。
- 復号化するトラフィックを特定し優先付けます：
  - 復号化するアプリケーションを決定します (認可済、未認可)。未認可アプリケーションの復号化は許可しません。
  - 復号化するデバイスを決定します (コーポレート、BYOD、モバイルなど)。

    企業は *BYOD* デバイスをコントロールできません。*BYOD* デバイスをネットワークで許可する場合、それらのトラフィックを復号化して、その他のネットワークトラフィックに適用しているものと同じセキュリティポリシーを課します。これを行うには、*BYOD* ユーザーを認証ポータル経由でリダイレクトして、ダウンロード方法を指示して *CA* 証明書をインストールし、ユーザーにそれらのトラフィックが復号化されることを明確に通知します。*BYOD* ユーザーに対して、プロセスを教育し、それを御社のプライバシーポリシーおよびコンピューター利用ポリシーに含めます。
  - 同じ復号化ポリシーを、異なる従業員グループ、請負業者、パートナー、ゲストなどの異なるグループにも使用するかどうかを決定します。
- 復号化できないトラフィックを特定します：
  - 証明書のピン留め、サポートされていない暗号、相互認証などの技術的な理由で復号化を中断するトラフィック。
  - Financial(財務)、Health(健康)、Government(政府)、およびその他の機密カテゴリで、ユーザーおよび、経営陣などのグループを含む復号化しないことを選択したトラフィック。
  - 復号化から除外したトラフィックを完全に把握します。暗号化されたトラフィックは閲覧不可能で、ファイアウォールは脅威防止プロファイルを暗号化されたトラフィックには適用できません。

- 最新の法務および人事部のコンピューター使用規則を用意してすべての従業員、取引先、提携先、ゲスト、その他のネットワークユーザーに配布し、復号化をロールアウトする際に、脅威をスキャンするために自身のデータが復号化されるかもしれないということをユーザーに知らせます。
- 証明書の検証処理方法を決定します。御社ビジネスモデルによっては、セキュリティとユーザーエクスペリエンスを相殺する必要がある場合があります。証明書の検証処理方法を理解することは、SSL フォワード プロキシ復号化プロファイルの設定方法の決定に役立ちます。
- 記録対象の統計情報を確認します。現地の法務と規制の違い、さらにそれらが記録できるトラフィック、ログの保管場所にどのように影響するかを理解します。

すべてのネットワークトラフィックを監視できる場所にファイアウォールを設置します。そうすれば、暗号化されていないトラフィックがファイアウォールを迂回して、不注意によりネットワークへのアクセスを得ることがありません。

STEP 3 | 公開鍵基盤(PKI)の展開計画を作成します。

- 既存の PKI がある場合、SSL Forward Trust Ca 証明書をエンタープライズ ルート CA から従属証明書として生成します。これによりデプロイメントが簡単になります。なぜなら、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 を信頼しているので、証明書の問題はなくなります。エンタープライズ ルート CA がない場合、入手することをご検討ください。

  あるいは、自己署名ルート CA 証明書をファイアウォールで生成し、従属 Forward Trust CA 証明書をそのファイアウォールに作成して、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、概念実証(POC)トライアルにエンタープライズ ルート CA を持たない小規模企業に最適です。

  

  BYOD と同様に、エンタープライズはゲストデバイスを制御しません。ゲストデバイスをネットワークで許可する場合、それらのトラフィックを復号化して、その他のネットワークトラフィックに適用しているものと同じセキュリティポリシーを課します。そうするには、ゲストユーザーをキャプティブポータル経由でリダイレクトして、ダウンロード方法を指示して*CA*証明書をインストールし、ユーザーにそれらのトラフィックが復号化されることを明確に通知します。それを御社のプライバシーポリシーおよびコンピューター利用ポリシーに含めます。
- Forward Trust と Forward Untrust には別個の CA 証明書を生成します。同じ PKI 従属 CA を両方の証明書に使用してはいけません。さらに、信頼されたルート CA を利用して Forward Untrust 証明書には署名してはいけません！Forward Untrust 証明書はユーザーに、証明書が署名しているサーバーは合法ではなく、サイトに進んではいけないことを警告しています。もし信頼できるルートCAが信頼できない証明書に署名した場合、クライアントはルートCAを信頼しているので、信頼できない証明書を信頼できると信じてしまいます。
- 各ファイアウォールに個別の従属 Forward Trust 証明書を生成します。個別の下位 CA を使用することにより、1 つのデバイス (またはデバイスペア) を廃止する際に、他のデプロイメントに影響することなく、証明書を無効にすることが可能になるので、証明書を無効にすることが必要な場合でも影響を抑えることができます。別個の CA 証明書は、証明書のエラーメッセージにトラフィックが横断したファイアウォールについての情報を含むので、テクニカルサポートがユーザーの問題を解決する際に役立ちます。全ファイアウォールでの 1 つの Forward Trust 従属 CA の使用は展開が簡単ですが、各ファイアウォールでの別の証明書の使用は最高のセキュリティを提供します。
- 秘密鍵のセキュリティをさらに高める必要がある場合は、秘密鍵を HSM に保存することをご検討ください。

STEP 4 | リソースの消費と利用可能なファイアウォールリソースを理解し、復号化デプロイ後のパフォーマンスを比較するために、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、復号化したいトラフィック量をサポートするために必要なファイアウォールデプロイメントの規模を予測します。

- 最寄りの Palo Alto Networks SE/CE と共に、ファイアウォールのデプロイメントの規模を把握し、間違いを防ぎます。

- 現在利用可能なファイアウォールリソースを記録します。一般的に、セキュリティが高いほど、消費する復号化リソースは多くなります。復号化できるトラフィック用に影響する要因は以下のとおりです：
  - 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。
  - 鍵のサイズ。
  - キー交換アルゴリズム。DHEやECDHEなどの、PFS（Perfect Forward Secrecy）一時アルゴリズムは、RSAよりもリソースを消費しますが、ファイアウォールが各セッションに対して新たな暗号鍵を生成するため、より強力なセキュリティを提供しています。もし攻撃者がセッション鍵に不正にアクセスしたら、PFS は同じクライアントとサーバーとの間の別のセッションを復号化するために攻撃者がそれを使用することを防ぎます。一方、RSAはそれは行いません。
  - 証明書の認証。RSA 証明書の認証（これは RSA 鍵交換アルゴリズムとは同じではありません）は ECDSA 証明書認証よりも使用する CPU サイクルは少ないですが、ECDSA のほうが高い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。キー交換アルゴリズムは、暗号化アルゴリズムが PFS と RSA のどちらなのかを決定します。
  - ファイアウォール モデルおよびリソース。古いモデルよりも新しいファイアウォールモデルの方により多くのリソースがあります。
- トランザクション サイズがパフォーマンスに影響します。全トラフィックの平均トランザクションサイズを測定し、次にポート 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、合計トラフィックおよび平均トランザクションサイズに関連するファイアウォールでの暗号化された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り、復号化によってファイアウォールの処理リソースがどのように消費されるのかが異なってきます。ファイアウォール リソースに問題があれば、優先度が高い高リスクのトラフィックに対しては強力な復号化を使い、優先度の低いトラフィックに対しては処理量の小さい復号化を使用して復号· 検査を行い、空きリソースを増やしていきます。

より多くのトラフィックが毎日暗号化されているので、復号化するトラフィック量の成長の伸びしろを含めてファイアウォールのサイズを決定します。

STEP 5 | ステージ分けし、優先付けしたデプロイメントを計画します。

- アーリーアダプタを復号化チャンピオンに特定し、部門管理者を計画に参加させます。
- POC をセットアップしデプロイ戦略をテストしてから、ユーザー全般に展開します。復号化 POC 展開がファイアウォール CPU やメモリ使用量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ズが適正かどうかを理解するのに役立ちます。POC は復号化を技術的に破るアプリケーションも明らかにできます。
  - POC 参加者に変化について教え、テクニカルサポートへの連絡方法も伝えます。
  - サポートが展開を支援する最適な方法を開発する機会が持てるように、復号化 POC 向けのテクニカルサポート POC をセットアップします。
  - フェーズごとの復号化最もリスク度の高いトラフィックを最初に復号化し（ゲームあるいは高リスクなど、悪意あるトラフィックが含まれている可能性が高い URL カテゴリ）、経験を積みながらさらに復号化するように計画します。代替策としては、最初にビジネスに影響しないURLカテゴリを復号化します（もし失敗してもビジネスには影響しません）。例としては、ニュースのフィードが挙げられます。両方のケースで、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、レポートを作成し復号化ログを確認して、復号化が期待どおり動作していることを確認してから、少しずつ URL カテゴリなどを復号化します。技術的な理由で復号化できない、または復号化しないことを決めた多売に、復号化から除外するために復号化除外 の作成を計画します。
  - POCの成功度を測定し、展開方法を微調整します。
- 一般的なロールアウト前に、ユーザー全体を教育します。POCは、伝える上で最も重要なポイントを見極めるのに役立ちます。

- すべての従業員、契約社員、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、更新された法務および人事コンピュータ使用ポリシーを配布します。復号化を各部門やグループに展開していくにつれて、誰もが各自のデータを復号化して、脅威がないかどうかスキャンできることを理解させてください。
- 展開の各ステージを評価する十分な時間を取った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用いてSSL復号化を展開する

STEP 1 | 復号化ポリシーのキーおよび証明書を生成して配布する。

- Enterprise PKI がある場合、エンタープライズ ルート CA からのフォワードプロキシトラフィック向けの Forward Trust CA 証明書を生成します。あるいは、自己署名 Root CA 証明書をファイアウォールで生成し、従属 CA をファイアウォールで作成し、次に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、小規模デプロイメント、およびPOC向けです。
- 各ファイアウォールに対して、独自の従属するForward Trust CA（転送信頼CA）を生成します（または、プランニング内容に応じて、すべてのファイアウォールに対して1つのForward Trust CA、証明書が1つのほうがデプロイは簡単になりますが、個別の証明書を用意するとセキュリティを強化でき、その他の利点も存在しています）。異なるPKIプラットフォームには、証明書管理の拡張向けの異なる機能があります。
- Enterprise 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Trust CAストレージにインポートします。
- Forward *Untrust* CA 証明書をCAトラストストレージにインポートしないでください。さもないと、非トラスト証明書は非トラストサイトのトリガーとして動作しません。（ただし、ファイアウォールの自己署名 Root CA が信頼できる発行者としてクライアントシステムにインストールされていない場合、自己署名 Forward Untrust 証明書を使用できます。）
- 自動化メソッド を使用して Forward Trust 証明書を、Palo Alto Networks Global Protect Portal、Microsoft AD Certificate Services（グループポリシーオブジェクト使用）、商用ツール、またはオープンソースツールなどの接続デバイスに配布します。
- 証明書をエンタープライズ ルート CA から生成する場合、証明書をファイアウォールにインポートします。
- 何か問題があった場合でも Forward Trust CA 証明書にアクセスできるように、ファイアウォールの Forward Trust CA 証明書の秘密鍵（ファイアウォールのマスターキーではなく）、安全なリポジトリにバックアップします。
- エンタープライズルートCAから証明書と秘密鍵を生成した場合、秘密鍵のエクスポートをブロックしてください。（エンタープライズCAからそれらを新しいファイアウォールやPanoramaにインストールできるため、PAN-OSからエクスポートする必要はありません。）
- HSM を使用するコールを計画している場合、 秘密鍵を HSM に保存します。

STEP 2 | 復号化プロファイルを設定して プロトコルの制御、証明書の検証、不具合の処理を行います。

- SSL フォワードプロキシ復号化プロファイル はサーバー証明書の検証、セッションモード、さらに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一連の暗号を伴うセッションをブロックします。重要なアプリケーションが必要としない限り、クライアント認証を伴うセッションをブロックします。この場合、クライアント認証を許可する個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だけに適用します。
- SSL インバウンド インスペクション復号化プロファイル はセッションモードとインバウンド トラフィックの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およびサポートされていない一連の暗号を伴うセッションをブロックします。
- SSL プロトコル設定暗号スイートエレメントの制御:SSLフォワードプロキシと SSLインバウンド検査トラフィック用の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、および認証アルゴリズム。可能な限りもっとも強力な暗号を使用してください。フォワードプロキシについては、脆弱なプロトコルをブロックするために、**Min Version**（最小バージョン）を**TLSv1.2**に、

またMax Version（最大バージョン）をMax（最大）に設定します。SSL インバウンド インスペクションでは、インスペクションするインバウンドトラフィックがあるサーバーの容量に一致するプロトコル設定で別のプロファイルを作成します。

可能な限りもっとも強力な暗号スイートを使用してください。個別の葉復号化ポリシーとプロファイルを作成して、最大限のセキュリティを確保します。ビジネス目的で必要なレガシーサイトがそれより弱い暗号しかサポートしていない場合、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受け入れて、復号化プロファイル内で必要なサイトだけに適用します。異なるURLカテゴリのセキュリティとパフォーマンスをきめ細かく調整する場合にも、同じテクニックを使用してください。

多くのモバイルアプリケーションがピニングされた証明書を使用しています。*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 Decryption Exclusion List*（*SSL*復号化除外リスト）に自動的に追加することはできません。これらのアプリケーションに対して、復号化プロファイルの*Max Version*（最大バージョン）が*TLSv1.2*に設定されていることを確認するか、またはトラフィックに対して*No Decryption*（復号化なし）ポリシーを適用します。

- 復号化しないことを選んだトラフィックのサーバー証明書検証を制御する復号化プロトコルはありません。期限切れ証明書、信頼できない発行者を伴うセッションをブロックします。

No Decryption（復号化なし）プロファイルを*TLSv1.3*トラフィックには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、ファイアウォールが証明書情報に基づいてセッションをブロックできなくなります。

- SSL フォワード プロキシおよび復号化なしトラフィックについては、証明書失効リスト(CRL) および Online Certificate Status Revocation (OCSP) 証明書失効 は、サイトの証明書が失効していないかどうかを確認します。
- SSH プロキシ プロファイル はセッションモードと SSH トンネルトラフィックの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およびサポートされていないアルゴリズムを伴うセッションをブロックします。

データセンター および周辺機器（インターネット ゲートウェイ）向けのベストプラクティス復号化プロファイル設定の使用事例は、一般的なベストプラクティス設定とは若干異なります。

STEP 3 | 復号化するトラフィックを定義し、復号化しないことを 選択したトラフィックにポリシーに基づく例外を適用するよう、復号化ポリシールールを設定します。

- ポリシールールを作成して、復号化しないことを選択した固有の受信者 IP アドレス（例えば、財務サーバー）、送信元ユーザーおよびグループ（例えば、経営陣または HR スタッフ）、送信元デバイス、およびアプリケーションポートを除外します。これらのルールは、Decryption（復号化）ルールベースの上部、トラフィックを復号化するルールの前に配置してください。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、No Decryption（復号化なし）プロファイルをアタッチして、暗号化トラフィックにSSLサーバー証明書検証コントロールを適用してください。これにより、復号化したくないトラフィックの不注意による復号化を割けます。
- URLカテゴリ、カスタムURLカテゴリ、およびExternal Dynamic Lists（EDL）を使用して、財務サービス、健康· 医療、政府関係およびその他の、ビジネス、法的または規制上の理由で復号化したくない URL を、復号化しないように指定します。動的に変化するIPアドレス（例えばOffice 365）または、頻繁なメンバーシップ変更を伴う環境ではEDLを使用して、コミット操作をすることなく更新できます。

  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 カテゴリを生成します。それにより、これらに対して単一の復号化ポリシールールをもつだけで済みます。

  これらのルールは、これらの復号化ルールベース内で、トラフィックを復号化するルールの後に配置します。

- 復号化のロギングとログ転送を設定します。
- 復号化ミラーリング を使用して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場合、ミラーリング可能なトラフィックのミラーリングまたは制御を禁止している場合がある現地のプライバシー規制に留意してください。
- SSLフォワードプロキシ、 SSLインバウンド検査、およびSSHプロキシルールを設定することで、残りのトラフィックを復号化するポリシーを作成します。オンラインストレージおよびバックアップ、Webベース電子メール、Webホスティング、個人サイトおよびブログ、コンテンツデリバリーネットワークならびに高リスクURLカテゴリは常に復号化します。SSH プロキシはネットワークデバイスを管理し、すべてのSSHトラフィックを記録する管理者だけに制限し、多要素認証を設定して未承認のSSHアクセスを防ぎます。

STEP 4 | POCテスト時に復号化に技術的問題があり、除外リストにまだ記載されていない場合は、それらサイトをSSL復号化除外リスト(**Device**（デバイス）> **Certificate Management**（証明書管理）> **SSL Decryption Exclusion**（**SSL**復号化除外)）に追加します。（技術的に復号化をブロックするサイトを復号化すると、そのトラフィックをブロックする結果になります。）

STEP 5 | セキュリティポリシーで、Quick UDP Internet Connections（QUIC）プロトコルをブロックします。

Chrome およびその他の一部のブラウザは TLS ではなく QUIC を使っ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プロプライエタリな暗号化を使用するため、危険があるトラフィックが暗号化されたトラフィックの状態でネットワークに侵入するおそれがあります。標準ポートのQUICアプリケーションをブロックするルールと、UDPポート80および443をブロックするルールの、2つのルールを作成します。QUICをブロックするとブラウザでは強制的に TLSが使用されます。

STEP 6 | 復号化されたトラフィックをWildFireに転送し マルウェアがないか検査します。

STEP 7 | 復号化は時間をかけて展開します。

いくつかの URL カテゴリを復号化し、ユーザーフィードバックをレビューして、レポートを作成し復号化が予想どおり動作していることを確認します。ゴールに達するまで、さらに多くの URL カテゴリを徐々に復号化します。優先度の最も高いトラフィック（ゲームなど、悪意あるトラフィックが含まれている可能性が高い URL カテゴリ）から始めて、経験を積みながらさらに復号化を進め、工程を調整します。さらに保守的な方法としては、例えばニュースフィードなどビジネスに影響しない URL カテゴリから復号化をまず始めることです。

SSL 復号化デプロイメント後のベスト プラクティスをフォローする

暗号化の展開後、すべてが予想どおり動作していることを確認し、予想通り動作しつづけることを保証するための措置を取ります。

STEP 1 | 復号化が予想どおり動作することを検証 します。

STEP 2 | ファイアウォール性能を測定しそれが受け入れ可能な基準内であることを確認し、復号化の効果が発揮されていることを理解します。

お使いのファイアウォールリソースのサポートを超えた量のトラフィックを復号化したい場合、復号化すべきすべてのトラフィックを復号化するために十分なリソースへスケールアップし、ネットワークを保護してください。

STEP 3 | 新しい従業員を雇ったら教育を実施し、復号化ポリシーを理解させ、弱い暗号スイートを使用しているサイトにアクセスできなくても驚かないように理解させてください。

STEP 4 | 定期的に復号化ポリシーとプロファイルを見直し、更新します。

STEP 5 | 復号化トラフィックを監視して、復号化に関する問題を解決するには、Application Command Centerの**SSL Activity**（**SSL**アクティビティ）ウィジェットなどの復号化トラブルシューティングツール、および復号化ログ（**Monitor**（監視）> **Logs**（ログ）> **Decryption**（復号化））を使用します。

復号化トラブルシューティングワークフローの例は、ツールを使った問題の調査方法を示しています。

STEP 6 | Palo Alto Networks 文書およびその他リソースを使用してさらに復号化を理解し情報を検索します：

- 『PAN-OS 管理者ガイド』 はPalo Alto Networks 次世代ファイアウォールについての詳細情報を提供します。
- Palo Alto Networks Live コミュニティには 復号化リソースリスト という、復号化設定、セットアップ、および管理についての記事があります。
- 不足している中間認証を検索するには、SSL Labs (Qualys)に進みます。
- サーバーサポートに適した暗号を検索するには、Qualys SSL Labs サーバー SSL テストページに進みます。
- 世界で最も人気ある 150,000 のサイトで使用されている様々な暗号やプロトコルの割合についての最新の統計を確認し、トレンドを把握し、より安全な暗号とプロトコルのために世界的なサポートがどの程度受け入れられているかを理解するには、Qualys SSL LabSSL Pulse ページに進みます。