paloalto TECHDOCS

高度な WildFire の管理

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

April 8, 2025

Table of Contents

高度な WildFire の概要

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

Advanced WildFire™は、動的/静的解析とインテリジェントランタイムメモリ解析の組み合わせにより、回避性の高い脅威を検出し、マルウェアをブロックする保護を作成するゼロデイ マルウェアの検出と防止を提供します。

Advanced WildFire Analysis Environmentは、これまで知られていなかったマルウェアを特定し、Palo Alto Networks NGFWがマルウェアの検出とブロックに使用できるシグネチャを生成します。Palo Alto Networks のファイアウォールが未知のサンプルを検出すると、ファイアウォールは自動的に、あらゆるアプリケーションから、高度な WildFire分析のためにWildFireパブリッククラウドサービスにサポートされているすべてのファイルタイプを転送します。高度なWildFireは、サンドボックスで分析および実行したときにサンプルが表示するプロパティ、動作、アクティビティに基づいて、サンプルが良性、グレイウェア、フィッシング、または悪意のあるものであるかどうかを判断し、新たに発見されたマルウェアを認識するためのシグネチャを生成して、リアルタイムで最新のシグネチャをグローバルに取得できるようにします。Palo Alto Networks のすべてのファイアウォールは、受信したサンプルをこれらのシグネチャと比較し、1つのファイアウォールで最初に検出されたマルウェアを自動的にブロックできます。

高度な WildFire の詳細、または使用を開始するには、次のトピックを参照してください。

- WildFireの分析、WildFireの判定、WildFireのシグネチャのために提出できるサンプルの種類の詳細については、高度な WildFireの概念を参照してください。
- ファイアウォールで設定できる高度な WildFire の導入の詳細をご覧ください。解析したいサンプルを、Palo Alto NetworksがホストするWildFireクラウド、ローカルにホストされるWildFireプライベートクラウドに送信したり、ファイアウォールが特定のサンプルをパブリッククラウドに、特定のサンプルを送信する、ハイブリッドクラウドを使用したりすることができます。
- アドバンスド WildFireの使用を開始するをクリックして、分析のために送信するサンプルを定義し、WildFire cloud への送信サンプルを開始します。

- WildFireアプライアンスを導入する場合は、「WildFireアプライアンスの管理」を参照してください。

サブスクリプションオプション

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

基本的なWildFireサービスは、Palo Alto Networks次世代ファイアウォールの一部として含まれており、高度なWildFireまたはWildFireサブスクリプションは必要ありません。基本的なWildFireサービスでは、ファイアウォールはPortable Executable（PE）ファイルを高度なWildFireに転送して分析でき、そのシグネチャは、24～48時間毎に入手可能となるアンチウイルスと/やIPSの脅威防御として更新を取得できます。

Palo Alto Networks は、いくつかのサブスクリプション オプションを提供しています。

- **WildFire**:WildFireサブスクリプションは、サンプルを高度な WildFire クラウドに転送することでマルウェアからの保護を提供し、そこで一連の分析環境を使用して、脅威のさらなるインスタンスをブロックする保護を生成することで、未知のマルウェアの脅威を検出および防止します。サブスクリプションの一部として、WildFireシグネチャの定期的な高度なアップデート、高度なファイルタイプ転送、WildFire APIを使用したファイルのアップロード機能をご利用いただけます。オンプレミス ソリューションを必要とする環境を運用している場合は、WildFireサブスクリプションを使用して、ローカルの WildFire アプライアンスにファイルを転送できます。
- **Advanced WildFire**—(PAN-OS 10.0 以降) Advanced WildFire サブスクリプションには、標準の WildFireサブスクリプションにあるすべての機能が含まれており、高度なクラウドベースの検出器を介してサンプル分析を提供することで改善されています。この高度な検知システムは、インテリジェントなリアルタイムランタイムメモリ解析、ランタイムDLLエミュレーション、自動アンパッキング、ファミリー分類、ステルス観測、および他のテクニックを使用してサンプルを解析し、非常に侵食性の高いマルウェアをターゲットにします。
- スタンドアロンの **WildFire API**—SOAR ツール、カスタム セキュリティ アプリケーション、およびその他の脅威評価ソフトウェアを運用しているPalo Alto Networksのお客様は、APIのみのアクセスを提供するスタンドアロン サブスクリプションを使用して、WildFire クラウドの高度なファイル分析機能にアクセスできます。これにより、転送メカニズムとしてAlto Networksのファイアウォールに依存することなく、WildFireベースの分析を活用できます。WildFire スタンドアロン API サブスクリプションを使用すると、悪意のある可能性のあるコンテンツに関する情報を WildFireクラウド脅威データベースに直接クエリし、

組織の特定の要件に基づいて WildFire の高度な脅威分析機能を使用して分析のためにファイルを送信できます。サブスクリプションの強化されたアクセス制限により、さまざまな規模の組織が使用状況に応じてアクセス制限をカスタマイズできます-これには、特定の数のファイル/レポートクエリ、サンプル送信(高度なWildFire分析用)、またはその2つの組み合わせを許可するスケーラブルなライセンスが含まれます。詳細については、WildFire API Reference（WildFire APIリファレンス）を参照してください。

標準のWildFireサブスクリプションは、次の機能のロックを解除します。

- リアルタイム更新:(PAN-OS 10.0 以降) ファイアウォールは、Advanced WildFireパブリック クラウドが生成できるとすぐに、新しく検出されたマルウェアの高度な WildFire シグネチャを取得できます。検体確認中にダウンロードされたシグネチャはファイアウォール キャッシュに保存され、高速（ローカル）検索に使用することができます。さらに、カバレッジの最大化に向けて、リアルタイムのシグネチャが有効化されている場合、ファイアウォールは定期的にシグネチャ パッケージを自動的にダウンロードします。この補足シグネチャはファイアウォール キャッシュに追加され、ステールとなり更新されるか、新しいシグネチャで上書きされるまで使用することができます。リアルタイム高度な WildFire 更新を使用することが、お勧めのベストプラクティス設定です。

  Device（デバイス） > **Dynamic Updates**（ダイナミック更新）の順に選択し、ファイアウォールがリアルタイムで最新の高度な WildFire シグネチャを取得できるようにします。

- **5** 分間の更新:(すべての PAN-OS バージョン) 高度な WildFireパブリック クラウドは、新たに検出されたマルウェアの高度な WildFire シグネチャを 5 分ごとに生成して配布でき、これらのシグニチャを毎分取得してインストールするようにファイアウォールを設定できます(これにより、ファイアウォールは可用性から 1 分以内に最新のシグニチャを取得できます)。

  PAN-OS 10.0 以降を実行している場合は、繰り返し更新をスケジュールする代わりに、リアルタイム高度な *WildFire* 更新の使用がベストプラクティスです。

  Device（デバイス） > **Dynamic Updates**（ダイナミック更新）の順に選択し、ファイアウォールが最新の高度な WildFire シグネチャを取得できるようにします。高度な WildFire のデプロイメントに応じて、次のシグネチャパッケージ更新の一つまたは両方を設定できます。

  - **WildFire**—WildFireパブリッククラウドから最新のシグネチャを入手します。
  - **WF-**プライベート — シグネチャと URL カテゴリをローカルで生成するように設定された WildFire アプライアンスから最新の署名を取得します。

- 高度な **WildFire** インライン **ML:(PAN-OS 10.0** 以降)ファイアウォール データプレーンで機械学習**(ML)**を使用して、ポータブル実行可能ファイル、実行可能およびリンク形式(ELF) ファイル、および PowerShell スクリプトの悪意のあるバリアントがリアルタイムでネットワークに侵入するのを防ぎます。ファイアウォール上で高度な WildFireクラウド解析技術を利用することにより、高度な WildFire インライン MLは、ファイルの高確率分類を定式化するためのデコーダ フィールドとパターンを含むファイルの詳細を評価することにより、特定のタイプの悪意のあるファイルを動的に検出します。この保護により、現在不明であるだけでなく、Palo Alto Networks が悪性であると識別した特性に一致する脅威の将来の亜種にも拡張さ

れます。高度な WildFire インライン ML は、既存のアンチウイルスプロファイル保護設定を補完します。さらに、ファイルハッシュの例外を指定して、発生するあらゆる誤検知を除外することができ、これにより、特定のセキュリティニーズをサポートするために、より詳細なルールをプロファイルに作成することができます。

- ファイル タイプのサポート:PE に加えて、APK、Flash ファイル、PDF、Microsoft Office ファイル、Java アプレット、Java ファイル（.jar および .class）、SMTP および POP3 電子メール メッセージに含まれる HTTP/HTTPS 電子メール リンクなど、高度なファイル タイプを Advanced WildFire 分析用に転送します。（WildFireプライベートクラウド解析は、APK、Mac OS X、Linux（ELF）、アーカイブ (RAR/7-Zip)およびスクリプト(JS、BAT、VBS、Shell Script、PS1、およびHTA)ファイルをサポートしていません）。
- **Advanced WildFire API** — 高度な WildFireパブリック クラウドまたは WildFire プライベート クラウドへの直接プログラムによるアクセスを可能にする WildFire APIへのアクセス。APIを使用して、分析用ファイルの送信や高度な WildFire分析レポートの取得が行えます。高度な WildFire または WildFireサブスクリプションの一部として、1 日に最大 150 件のサンプル送信と最大 1,050 件のサンプル クエリを送信できます。これらの 1 日のサンプル送信制限は、組織の特定のニーズに基づいて拡張できます。詳細については、Palo Alto Networksの営業担当者にお問い合わせください。
- **WildFire**のプライベートおよびハイブリッドクラウドのサポート—高度な WildFire 分析のためのファイルの転送。WildFireプライベートクラウドとWildFireハイブリッドクラウドの両方にサンプルをWildFire アプライアンスに送信できます。WildFireアプライアンスを有効にするには、サポートライセンスのみが必要です。

WildFireサブスクリプションを購入した場合は、サブスクリプションのみの WildFire 機能を利用する前に、ライセンス認証をアクティブ化する必要があります。

高度なWildFireサブスクリプションは、次の機能のロックを解除します。

- インテリジェントなランタイム メモリ分析—インテリジェントなランタイム メモリ分析は、静的および動的分析エンジンを補完するクラウドベースの高度な分析エンジンであり、回避的なマルウェアの脅威を検出して防止します。高度な脅威で使用されるこれらの回避手法には、クローキング戦略を使用したマルウェア、高度なツールを使用して作成された特注のデザイン/一時的な動作の兆候の表示、急速に広がる品質を示すマルウェアが含まれますが、これらに限定されません。クラウドベースの検出インフラストラクチャを活用することで、イントロスペクティブ分析ディテクタは、ユーザーがコンテンツ更新パッケージをダウンロードしたり、リソースを大量に消費するアプライアンスベースのアナライザを実行したりすることなく、自動的に更新および展開される幅広い検出メカニズムを操作します。クラウドベースの検出エンジンは、高度な WildFire サンプルの分析に使用されるMLベースのデータセットに基づいて継続的に監視および更新され、Palo Alto Networksの脅威研究者による追加のサポートを受けて、高度に正確な検出機能の強化のために人間の介入を提供します。

  インテリジェント ランタイム メモリ分析は、既存の WildFire分析プロファイル設定に依存しており、追加の構成は必要ありません。ただし、アクティブな高度な WildFire ライセンスが必要です。回避的および/または高度なマルウェアの品質を表示または示すサンプルは、適切な分析環境に自動的に転送されます。

高度な WildFire の概念

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

サンプル

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

どこで使用できますか?	何が必要ですか?
• CN-Series	

サンプルは、ファイアウォールとパブリック API から高度な WildFire 分析のために送信されたすべてのファイル タイプと電子メール リンクです。ファイアウォールが高度な WildFire 分析のために送信できるファイルの種類とリンクの詳細については、ファイル分析 と電子メールリンク分析を参照してください。

ファイヤーウォールの転送

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

ファイアウォールは、設定されたWildFire Analysisプロファイル設定（**Objects (**目的**)** > **Security Profiles (**セキュリティプロフィール**)** > **Advanced WildFire Analysis (**高度な**WildFire**分析**)**）に基づくWildFire分析のために、未知サンプルとアンチウイルス シグネチャに一致するブロックされたファイルを転送します。電子メールに含まれるリンク、電子メールに添付されたファイル、およびブラウザベースのファイルダウンロード、の検出に加え、ファイヤーウォールはアプリケーション内のファイル転送を検出する App-ID を活用します。ファイアウォールが検出したサンプルでは、ファイアウォールはサンプルの構造と内容を分析し、既存のシグネチャと比較します。サンプルがシグネチャと一致する場合、ファイアウォールはシグネチャに対して定義されているデフォルトのアクション（許可、アラート、またはブロック）を適用します。サンプルがアンチウイルスシグネチャと一致した場合、または高度な WildFire シグニチャと比較してもサンプルが不明なままの場合、ファイアウォールは高度な WildFire 分析のために転送します。

デフォルトでは、ファイアウォールは、未知のサンプルが検出されたセッションに関する情報も転送します。ファイアウォールが転送するセッション情報を管理するには、**Device (**デバイス**)** > **Setup (**設定**)** > **WildFire**を選択し、セッション情報設定を編集します。

セッション情報の共有

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

ファイアウォールは、未知のサンプルやブロックされたサンプルを分析のために転送するだけでなく、サンプルのネットワークセッションに関する情報も転送します。Palo Alto Networksは、セッション情報を使用して、疑わしいネットワークイベントのコンテキスト、マルウェアに関連する脆弱性の指標、影響を受けるホストとクライアント、マルウェアの配信に使用されるアプリケーションについて学びます。

セッション情報の転送はデフォルトで有効になっています。ただし、デフォルト設定を調整して、WildFireクラウド オプションの 1 つに転送するセッション情報の種類を選択できます。

- Strata Cloud Manager
- PAN-OS & Panorama

セッション情報の共有(Cloud Management)

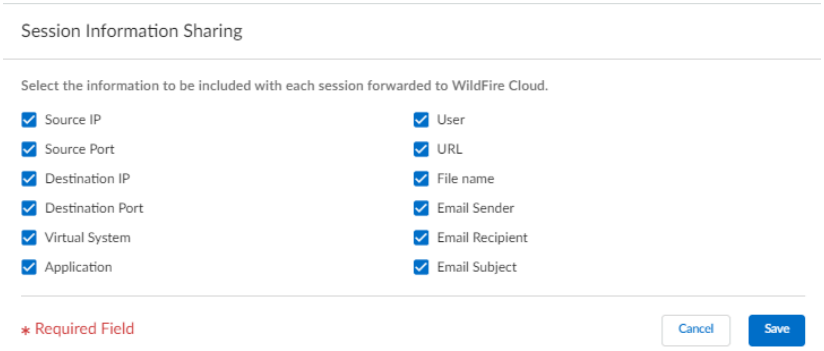
***Panorama*を使用して*Prisma Access*を管理している場合:**

[PAN-OS] タブに切り替えて、そこにあるガイダンスに従います。

***Prisma Access*クラウド管理を使用している場合は、こちらに進んでください。**

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerアプリケーションにログインします。

STEP 2 | **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Security Services (セキュリティ サービス)]** > **[WildFire and Antivirus (WildFireとアンチウイルス)]**を選択し、**[Session Information Settings (セッション情報設定)]**オプションを設定します。



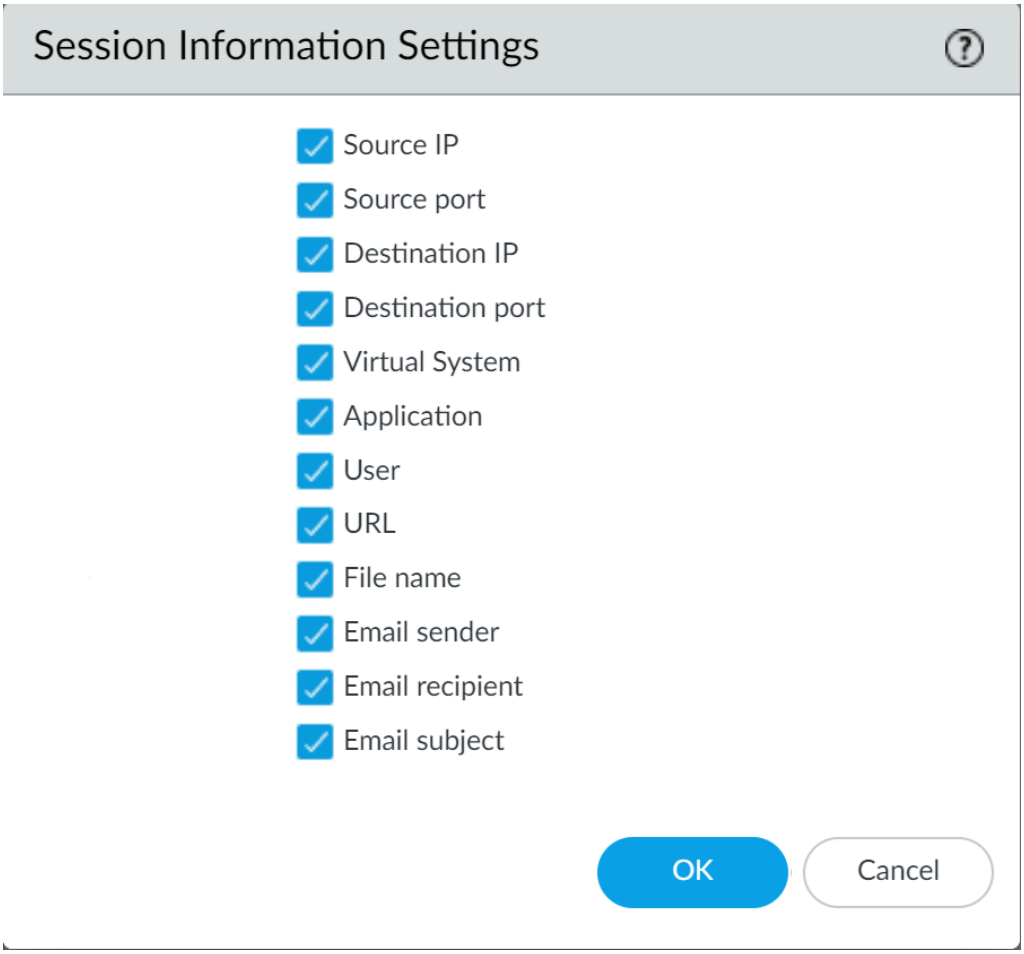
- **Source IP**（送信元 **IP**） — 未知のファイルを送信した送信元IPアドレスを転送します。
- **Source Port**（送信元ポート）— 未知のファイルを送信した送信元ポートを転送します。
- **Destination IP**（宛先**IP**）—未知のファイルの宛先IPアドレスを転送します。
- **Destination Port**（宛先ポート）—未知のファイルの宛先ポートを転送します。
- **Virtual System**（仮想システム）—未知のファイルを検出した仮想システムを転送します。
- **Application**（アプリケーション）—未知のファイルを送信したユーザーアプリケーションを転送します。
- **User**（ユーザー）—ターゲットユーザーを転送します。
- **URL**—未知のファイルに関連付けられたURLを転送します。
- **Filename**（ファイル名）—未知のファイルの名前を転送します。
- **Email sender**（電子メール送信者 ）—不明な電子メールリンクの送信者を転送します（電子メール送信者の名前はWildFireのログとレポートにも表示されます）。
- **Email recipient**（メール受信者）—未知の電子メールリンクの受信者を転送します（電子メール受信者の名前はWildFireのログとレポートにも表示されます）。
- **Email subject**（電子メールの件名）—未知の電子メールリンクの件名を転送します（電子メールの件名はWildFireのログとレポートにも表示されます）。

STEP 3 | 変更を保存します。

セッション情報の共有(PAN-OSおよびPanorama)

STEP 1 | PAN-OS Web インターフェイスにログインします。

STEP 2 | **Device (デバイス) > Setup (設定) > WildFire**を選択し、続く**Session Information Settings**（セッション情報設定）オプション



を選択またはクリアします。

- **Source IP**（送信元 **IP**） — 未知のファイルを送信した送信元IPアドレスを転送します。
- **Source Port**（送信元ポート）— 未知のファイルを送信した送信元ポートを転送します。
- **Destination IP**（宛先**IP**）—未知のファイルの宛先IPアドレスを転送します。
- **Destination Port**（宛先ポート）—未知のファイルの宛先ポートを転送します。
- **Virtual System**（仮想システム）—未知のファイルを検出した仮想システムを転送します。
- **Application**（アプリケーション）—未知のファイルを送信したユーザーアプリケーションを転送します。
- **User**（ユーザー）—ターゲットユーザーを転送します。
- **URL**—未知のファイルに関連付けられたURLを転送します。
- **Filename**（ファイル名）—未知のファイルの名前を転送します。
- **Email sender**（電子メール送信者 ）—不明な電子メールリンクの送信者を転送します（電子メール送信者の名前はWildFireのログとレポートにも表示されます）。

- **Email recipient**（メール受信者）—未知の電子メールリンクの受信者を転送します（電子メール受信者の名前はWildFireのログとレポートにも表示されます）。
- **Email subject**（電子メールの件名）—未知の電子メールリンクの件名を転送します（電子メールの件名はWildFireのログとレポートにも表示されます）。

STEP 3 | **OK** をクリックして変更内容を保存します。

分析環境

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

高度な WildFireは、オペレーティングシステムを含むさまざまな分析環境を再現して、サンプル内の悪意のある動作を特定します。サンプルの特性および特徴に応じて、複数の分析環境を使用してファイルの性質を判定することが可能です。高度な WildFireは機械学習で静的解析を使用して、既知のサンプルの変種が悪意のあるかどうかを最初に判断します。送信の最初の判定に基づいて、高度なWildFireは未知のサンプルを分析環境に送信して、動的分析から追加の情報とインジケータを抽出することにより、ファイルをより詳しく検査します。カスタムまたはオープンソースの方法を使用してファイルが難読化されている場合、Advanced WildFireクラウドは、静的分析を使用して分析する前に、動的分析環境内のメモリ内のファイルを解凍して復号化します。動的分析中、高度なWildFireはクライアントシステム内で実行中に動作するようにファイルを監視し、ブラウザのセキュリティ設定の変更、他のプロセスへのコードの挿入、オペレーティングシステムフォルダ内のファイルの変更など、さまざまな悪意のある兆候、サンプルが悪質なドメインにアクセスしようとする試みを監視します。さらに、高度なWildFireクラウド内で動的分析を行う間に生成された PCAP はディープ インスペクションの対象になり、ネットワーク アクティビティ プロファイルを作成するために使用されます。ネットワーク トラフィック プロファイルは一対多のプロファイル マッチを使用して、既知のマルウェアおよび以前は未知だったマルウェアを検出できます。

高度な WildFireは、サンプルの特性に基づいて次の方法を使用してファイルを分析できます。

- **Static Analysis**（静的分析）— - 実行前にサンプルの特性を分析して既知の脅威を検出します。
- **Machine Learning**（機械学習）—マルウェア機能セットと動的に更新される分類システムを比較することで、既知の脅威の亜種を特定します。

- **Dynamic Unpacking (**動的アンパック**)(**高度な **WildFire**グローバルクラウド専用**)**—カスタム/オープンソースの方法で暗号化されているファイルを特定およびアンパックし、静的分析を行える状態にします。
- **Dynamic Analysis**（動的分析）—- カスタムで構築された回避不能な仮想環境で、実際の効果や行動を決定するために未知の投稿を爆発させます。
- インテリジェントなランタイムメモリ分析 **(**高度な **WildFire License |** 高度な **WildFire** グローバルクラウドのみ **— NGFW** には **PAN-OS 10.0** 以降が必要**)** — 多数の回避技術を利用して最新の脅威を分析するために使用される高度な検出器を操作するクラウドベースの分析環境です。

高度なWildFireは、以下のオペレーティングシステムを複製する分析環境を実行します。

- **Microsoft Windows XP 32** ビット **(WildFire** プライベートクラウドのオプションとしてのみサポート**)**
- **Microsoft Windows 7 64** ビット
- **Microsoft Windows 7 32** ビット（**WildFire**アプライアンスのみのオプションとしてサポート）
- **Microsoft Windows 10 64** ビット **(PAN-OS 10.0** 以降を実行する高度な **WildFire**パブリッククラウドおよび **WildFire** プライベートクラウドのオプションとしてサポート**)**
- **Mac OS X (**高度な**WildFire**パブリック クラウドのみ**)**
- **Android (**高度な**WildFire**パブリック クラウドのみ**)**
- **Linux (**高度な**WildFire**パブリック クラウドのみ**)**

高度なWildFireパブリック クラウドは、複数のバージョンのソフトウェアを使用してファイルを分析し、特定のバージョンのクライアントアプリケーションを対象とするマルウェアを正確に識別します。WildFireプライベートクラウドはマルチバージョン分析をサポートしておらず、複数のバージョンにわたるアプリケーション固有のファイルを分析しません。

高度なWildFireインライン クラウド解析

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

高度なWildFireクラウドは、インライン クラウドMLベースの一連の検出エンジンを運用し、ネットワークを通過するPE (Portable Executable)検体を解析して、未知のマルウェアをリアルタイムで検出および防止します。これにより、高度なWildFireクラウド サービスは、これまでに見たことのないマルウェア(既存のWildFireシグネチャがないか、ローカルの高度なWildFireインライン クラウドML検出器を介して検出可能なもの)を検出し、クライアントへの感染をブロックできます。これには、これまで市場では見られなかった、高度なWildFireインラインMLによっ

て傍受されなかった特定の種類のマルウェアが、シグネチャの有効期限切れまたはシグネチャ データベースの容量制限により、ファイルが最近見られなかったためにそのシグネチャがファイアウォール上に存在せず、妨害されずに進行できるシナリオが含まれます。シグネチャが現在のセットの一部となっているため、新たに定義された悪意のあるファイルは、その後のファイアウォールによる遭遇でブロックされます。ただし、これは、悪意のあるファイルがWildFireクラウドによって解析された後に発生します。

高度なWildFireインライン クラウドは、リアルタイムでやり取りしてクラウド内でこれらの疑わしいファイルをマルウェアがないか解析している間、ファイルのダウンロード(または場合によってはネットワーク内への拡散)を保留することができます。WildFireで解析される他の悪意のあるコンテンツと同様に、高度なWildFireインライン クラウドで検出された脅威は脅威シグネチャを生成し、シグネチャ アップデート パッケージを通じてPalo Alto Networksから顧客に配布され、Palo Alto Networksのすべての顧客に将来的な防御を提供します。

高度なWildFireインライン クラウドは、ファイアウォール上で軽量な転送メカニズムを使用して動作し、ローカルのパフォーマンスへの影響を最小限に抑えます。また、脅威ランドスケープの最新の変化に対応するため、クラウド インラインML検出モデルがクラウド内でシームレスに追加および更新されます。コンテンツ更新や機能リリースのサポートは必要ありません。

高度なWildFireインライン クラウド解析は、WildFire分析プロファイルを通じて有効化および構成され、有効な高度なWildFireライセンスを持つPAN-OS 11.1以降が必要です。

高度な WildFire インライン ML

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

アンチウイルス プロファイルに存在する高度なWildFireインラインMLオプションを使用すると、ファイアウォール データプレーンは、PE (Portable Executable)、ELF (実行可能およびリンク形式)、MS Officeファイル、OOXML、Mach-O、およびPowerShellスクリプトとシェル スクリプトに機械学習をリアルタイムで適用できます。このアンチウイルス保護のレイヤーは、高度な WildFire ベースのシグネチャを補完し、シグネチャがまだ存在しないファイルのカバー範囲を拡大します。各インライン ML モデルは、ファイルの高確率分類を定式化するためのデコーダ フィールドとパターンを含む、ファイルの詳細を評価することにより、特定のタイプの悪意のあるファイルを動的に検出します。この保護により、現在不明なものだけでなく、Palo Alto Networks が悪性であると識別済みの特性に一致する将来的な脅威の亜種にも拡張されます。脅

威の状況における最新の変更に対応するために、インライン ML モデルがコンテンツ リリースを介して追加または更新されます。高度な WildFire インライン ML を有効にする前に、アクティブな 高度な WildFire または標準の WildFireサブスクリプションを所有している必要があります。

インライン ML ベースの保護を有効にして、URL フィルタリング設定の一部として、悪意のある URL をリアルタイムで検出します。

高度な *WildFire* インライン *ML* は、*VM-50* または *VM50L* バーチャル アプライアンスでサポートされていません。

判定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

高度な WildFire がPalo Alto Networksのホスト型 WildFire パブリック クラウドまたはローカルでホストされている高度な WildFire プライベート クラウドの 1 つで未知のサンプルを分析すると、サンプルを悪意のある、望ましくない (グレーウェアは目立たないが悪意のあるものと見なされる)、フィッシング、または良性であると判断されます。

- **Benign**（安全）—検体は安全で、悪意のあるふるまいを示していません。
- **Grayware**（グレイウェア）—セキュリティに直接的な脅威をもたらすものではありませんが、目障りな挙動をする可能性のある検体です。グレイウェアの典型的な例として、アドウェア、スパイウェア、そしてブラウザヘルパーオブジェクト（BHO）等が挙げられます。
- フィッシング - —リンクがユーザーをフィッシングサイトに誘導し、セキュリティの脅威をもたらします。フィッシング詐欺サイトは、攻撃者がユーザー情報、特にネットワークへのアクセスをロック解除する企業のパスワードを盗むことを目的として正当なWebサイトとして偽装するサイトです。WildFireアプライアンスはフィッシング判定をサポートせず、これらのタイプのリンクを悪意のあるものとして分類し続けま
- 悪意のある —サンプルがマルウェアで安全上の脅威をもたらします。マルウェアには、ウイルス、ワーム、トロイの木馬、リモート アクセス ツール（RAT）、ルートキット、ボットネットなどがあります。マルウェアと判定されたファイルに関して、シグネチャを生成、配布し、その後の感染を防止します。

それぞれの高度な WildFireクラウド (グローバル (米国) と地域) と WildFire プライベートクラウドは、他の WildFireクラウドオプションとは独立して、サンプルを分析し、WildFire 評決を生成します。WildFireプライベートクラウドの評決を除き、評決はグローバルに共有されるため、Advanced WildFireのユーザーは脅威データの世界的なデータベースにアクセスできます。

追加の分析のために、偽陽性か偽陰性のいずれかであると判断された判定を*Palo Alto Networks*の脅威チームに送信することができます。*WildFire*アプライアンスに送信されたサンプルの判定を手動で変更することもできます。

ファイル分析

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

WildFire分析プロファイルで構成されたPalo Alto Networksファイアウォールは、ファイルタイプ（電子メールリンクを含む）に基づいて高度なWildFire分析用のサンプルを転送します。加えて、ファイアウォールはエンコードまたは圧縮されたファイル（ZIP形式のファイル）を4階層までデコードし、デコードされたファイルが高度なWildFire分析プロファイルの条件に一致する場合、ファイアウォールはデコードしたファイルを分析用に転送します。

高度な WildFire 分析機能をファイアウォールで有効にして、インラインのウイルス対策保護を提供することもできます。アンチウイルス プロファイルに存在する 高度な WildFire インライン ML オプションを使用すると、ファイアウォール データプレーンは、リアルタイムで PE および ELF ファイルと PowerShell スクリプトに機械学習分析を適用できます。各インライン ML モデルは、ファイルの高確率分類を定式化するためのデコーダ フィールドとパターンを含む、ファイルの詳細を評価することにより、特定のタイプの悪意のあるファイルを動的に検出します。この保護により、現在不明なものだけでなく、Palo Alto Networks が悪性であると識別済みの特性に一致する将来的な脅威の亜種にも拡張されます。脅威の状況における最新の変更に対応するために、インライン ML モデルがコンテンツ リリースを介して追加または更新されます。詳細については 高度な WildFire インライン MLを参照してください。

高度なWildFireクラウドは、マルチステージのPE、APK、ELFマルウェアパッケージの一部としてセカンダリペイロードとして使用される特定のファイルタイプを解析することもできます。セカンダリペイロードを解析することで、高度な脅威による高度な攻撃を妨害するための追加のカバレッジが得られます。こうした高度な脅威は、追加の悪意のあるペイロードをアクティブにするコードを実行することで動作します。これには、セキュリティ対策の迂回を支援し、プライマ

リペイロードの拡散を促進するように設計されたものも含まれます。高度な WildFire は、静的および動的分析環境で処理することにより、多段階の脅威を分析します。マルチステージマルウェアによって参照されるファイルは、解析中に個別に処理されます。その結果、判定と保護は、ファイルごとに完了するとすぐに配信されます。マルチステージファイルの全体的な判定は、解析されたすべての攻撃ステージで見つかった悪意のあるコンテンツの脅威評価に基づいて決定されます。マルチステージファイルの分析中に発見された悪意のあるコンテンツは、ファイルをすぐに悪意のあるものとしてマークします。

悪意のあるコンテンツに対する安全取り扱い手順を有する組織は、API または WildFire ポータルから RAR 形式を使用して、パスワードで保護されたサンプルを手動で送信できます。高度なWildFireクラウドは、パスワード「*infected*」または「*virus*」を使用して暗号化されたサンプルを受信すると、高度なWildFire クラウドはアーカイブファイルを復号化して分析します。ファイルの判定と分析結果は、受信した形式（この場合はアーカイブ）で表示できます。

ファイアウォールは以下にリストされているすべてのファイル タイプを転送できますが、高度な WildFire 分析のサポートは、サンプルが送信される高度な WildFire クラウドによって異なる場合があります。詳細については、高度な WildFire ファイル タイプ サポートを参照してください。

WildFire Forwardingでサポートされるファイルタイプ	詳説
`apk`	Androidアプリケーションパッケージ（APK）ファイル *APK* ファイルに含まれる *DEX* ファイルは、*APK* ファイルの分析を行う一環として分析されます。
`Flash`	Web ページに組み込まれている Adobe Flashアプレットおよびフラッシュコンテンツ
`jar`	Java アプレット(JAR/クラス ファイル タイプ）。
`ms-office`	ドキュメント (DOC、DOCX、RTF)、ブック (XLS、XLSX)、PowerPoint (PPT、PPTX) プレゼンテーション、Office Open XML (OOXML) 2007 以降のドキュメントなど、Microsoft Office で使用されるファイル。インターネット クエリ (IQY) ファイルとシンボリック リンク (SLK) ファイルは、コンテンツ バージョン 8462 でサポートされています。
`pe`	Portable Executable（PE）ファイル。PEは実行ファイル、オブジェクト コード、DLL、FON（フォント）、LNKファイルなどを含みます。MSI ファイルは、コンテンツ バージョ

WildFire Forwardingでサポートされるファイルタイプ	詳細
	ン 8462 でサポートされています。サブスクリプションがなくてもPEファイルをWildFire分析に転送することはできますが、サポートされているその他のすべてのファイル タイプを分析するにはWildFireサブスクリプションが必要です。
pdf	ポータブルドキュメントフォーマット（PDF）ファイル。
MacOSX	macOSプラットフォームで使用されるさまざまなファイルタイプ。DMG、PKG、ZBundleファイルの静的解析は高度なWildFireグローバル(米国)リージョンとヨーロッパ クラウド リージョンでのみ利用可能ですが、その他のMac OS Xファイル(fatとmacho)の静的解析はすべてのリージョン クラウドでサポートされています。すべてのMacOSXファイルの動的解析は、高度なWildFireグローバル(米国)リージョンとヨーロッパ クラウド リージョンでのみサポートされています。詳細については、ファイルタイプサポートを参照してください。
email-link	SMTPおよびPOP3電子メールメッセージに含まれるHTTP / HTTPSリンク。Email Link Analysis（電子メールリンク分析）を参照してください。
アーカイブ	Roshalアーカイブ（RAR）と7-Zip（7z）アーカイブファイル。マルチボリュームアーカイブは、いくつかの小さなファイルに分割されているため、分析のためにサブミットすることはできません。 パスワード「*infected*」または「*virus*」で暗号化されたRAR ファイルのみが高度な WildFireクラウドによって復号化および分析されます。 ファイアウォールは、デコードされた後に *ZIP* アーカイブに含まれるサポートされているファイルを転送できますが、完全な *ZIP* ファイルをエンコードされた状態で転送することはできません。完全な *ZIP* ファイルを送信する場合は、ワイルドファイアポータルを使用するか、*WildFire API* を使用して *ZIP* ファイルを手動でアップロードできます。

WildFire Forwardingでサポートされるファイルタイプ	詳説
`linux`	実行可能およびリンク可能な形式（ELF）ファイル。
`/script`	様々なスクリプトファイル • Jscript (JS)、VBScript (VBS)、および PowerShell Scripts (PS1) は、コンテンツ バージョン 8101 でサポートされています。 • バッチ (BAT) ファイルは、コンテンツ バージョン 8168 でサポートされています。 • HTML アプリケーション (HTA) ファイルは、コンテンツ バージョン 8229 でサポートされています。

電子メールリンク分析

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

Palo Alto Networksファイアウォールは、SMTPおよびPOP3電子メール メッセージに含まれるHTTP/HTTPSリンクを抽出し、そのリンクを分析のためにWildFireクラウドに転送することができます。ファイアウォールは、通過する電子メールメッセージからリンクと関連付けられたセッション情報 （送信者、受信者、件名） を抽出するのみで、電子メールメッセージの受信、保存、転送、表示は行いません。

WildFireは送信されたリンクを訪問して、対応するWebページが攻撃をホストしているか、フィッシング活動を表示しているかどうかを判断します。WildFireが悪質なものやフィッシングであると判断したリンクは次のとおりです。

- WildFire Submissions（WildFireへの送信）のログエントリとしてファイヤーウォールに記録されたリンクリンクの挙動と観測されたアクティビティの詳細がWildFire Submissions（WildFireへの送信）ログエントリ毎に入手可能です。このログエントリにも電子メール ヘッダー情報（電子メールの送信者、受信者、件名）が記録されるため、メッセージ

を識別して電子メールサーバーから削除したり、電子メールが配信または開かれていた場合に脅威を軽減させたりすることができます。

- PAN-DBに追加、およびURLがマルウェアとして分類されます。

ファイアウォールは、電子メールリンクが100個たまった時点か、2分ごと（いずれか早い方）で電子メールリンクを転送します。WildFire への各バッチ アップロードは、指定されたファイアウォールの 1 分あたりのアップロード容量に対して 1 回のアップロードとしてカウントされます Firewall ファイル転送容量 (モデル別)。電子メールに含まれるリンクがURLではなくファイルのダウンロード用リンクである場合、対応したファイルタイプのWildFire分析が有効化されている場合に限り、ファイアウォールはそのファイルを転送します。

ファイアウォールが WildFire 分析のために電子メールに含まれるリンクを転送できるようにするには、高度な WildFire 分析のためのファイルの転送を参照してください。高度な URLフィルタリング ライセンスでは、悪意のあるフィッシングサイトへのユーザーアクセスをブロックすることもできます。

URL 解析

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

高度な WildFire グローバル クラウド (米国) と地域のクラウドは、URL を分析し、拡張により電子メール リンクを分析し、WildFire API を通じて標準化された評決とレポートを提供できます。PAN-DB を含む Palo Alto Networks のすべてのサービスから脅威解析の詳細を集約することで、高度な WildFire はより正確な判定を生成し、一貫した URL 解析データを提供することができます。

高度な WildFire グローバル クラウドで動作する URL アナライザは、URL フィード、相関 URL ソース (電子メール リンクなど)、NRD (新しく登録されたドメイン) リスト、PAN-DB コンテンツ、手動でアップロードされた URL を処理し、GDPR 準拠に影響を与えることなく、すべての高度な WildFireクラウドに機能の向上を提供します。URL が処理されると、判定、エビデンスのある検出理由、スクリーンショット、Web 要求に対して生成された分析データを含む URL 解析レポートを取得することができます。URL 解析中に表示される Web ページのアーティファクト（ダウンロードしたファイルとスクリーンショット）を取得して、異常なアクティビティをさらに調査することもできます。

この機能を利用するために追加の設定は必要ありませんが、分析用にEメールリンクを自動的に送信したい場合は、高度な WildFire 分析のためのファイルの転送を実行する必要があります。

追加の分析のために、偽陽性か偽陰性のいずれかであると判断された判定をPalo Alto Networksの脅威チームに送信することができます。

圧縮およびエンコードされたファイル分析

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

デフォルトでは、ファイヤーウォールは ZIP形式で圧縮されたファイルを含むエンコードまたは4階層まで圧縮されたファイルをデコードします。その後、ファイヤーウォールはデコードしたファイルを調査してポリシーを適用し、そのファイルが未知の場合、ファイヤーウォールはデコードしたファイルをWildFireに転送して分析します。ファイアウォールは高度な WildFire 分析用に完全な ZIP アーカイブ ファイルを転送できませんが、WildFire ポータルまたは WildFire API を使用してファイルを高度な WildFireパブリック クラウドに直接送信できます。

*RAR*と*7-Zip*アーカイブファイルは、ファイアウォールによってデコードされません。これらのファイルの処理はすべて、*Advanced WildFire*パブリック クラウドで行われます。

高度な WildFire のシグネチャ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

高度な WildFireは、Web トラフィック（HTTP/HTTPS）、電子メールプロトコル（SMTP、IMAP、POP）、およびFTPトラフィックからゼロデイ マルウェアを検出し、検出したマルウェアからの将来の感染を識別して防御するためのシグネチャを迅速に生成することができます。高度な WildFireは、サンプルのマルウェアペイロードに基づいてシグネチャを自動的に生成し、正確性と安全性をテストします。

それぞれの高度な WildFireクラウドはサンプルを分析し、他の高度な WildFireクラウドとは独立してマルウェアシグネチャを生成します。WildFireプライベートクラウドシグネチャを除き、高度な WildFireシグネチャはグローバルに共有されるため、世界中のユーザーは、マルウェアが最初に検出された場所に関係なく、マルウェアのカバレッジの恩恵を受けることができます。マルウェアは急速に変化するため、高度な WildFire で生成されるシグネチャでは、マルウェアの複数の亜種を対象とします。

高度な WildFireライセンスが有効なファイアウォールは、最新の高度な WildFireシグネチャが利用可能になり次第、リアルタイムで取得できます。高度な WildFireサブスクリプションがない場合、有効な脅威防止ライセンスを持つファイアウォールのアンチウイルスアップデートの一部として、24 - 48時間以内にシグニチャが使用可能になります。

ファイアウォールが新しいシグネチャをダウンロードしてインストールするとすぐに、マルウェア（またはその亜種）を含むファイルはファイアウォールによって自動的にブロックされます。マルウェアシグネチャは悪質なフィッシングリンクを検出しません。 これらのリンクを強制するには、PAN-DB URLフィルタリングライセンスが必要です。悪質なサイトやフィッシングサイトへのユーザーアクセスをブロックすることができます。

高度な WildFire の導入

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

Palo Alto Networksファイアウォールをセットアップして、未知の検体をPalo Alto Networks-で構築されている高度な WildFireグローバルクラウドおよびU.S.政府機関向けクラウド、ローカルでホストされている WildFire プライベート クラウド、またはファイアウォールが特定のサンプルを高度な WildFire パブリック クラウド オプションの 1 つに転送し、特定のサンプルを WildFire プライベート クラウドに転送できるようにします。

- WildFireパブリック クラウド
- WildFire プライベート クラウド
- WildFireハイブリッドクラウド
- WildFire:米国政府専用クラウド

WildFireパブリック クラウド

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

Palo Alto Networks ファイアウォールは、未知のファイルや電子メールリンクを高度な WildFire グローバルクラウド(米国)または Palo Alto Networks が所有および管理している高度な WildFire 地域クラウドに転送することができます。分析のためにサンプルを送信する高度な WildFireパブリック クラウドを、場所と組織のニーズに基づいて選択します。

- **Advanced WildFire Global Cloud (**高度な **WildFire** グローバルクラウド**) (**米国**)**

  高度な WildFire グローバル クラウド (米国) は、米国でホストされているパブリック クラウド環境です。

  次の URL を使用して、分析のために 高度な WildFire グローバル クラウド (米国) にファイルを送信し、高度な WildFire グローバル クラウド (米国) ポータルにアクセスするには、次のURLを使用します:wildfire.paloaltonetworks.com。

- 高度な**WildFire**ヨーロッパ クラウド

  WildFireヨーロッパクラウドは、オランダで開催される地域的なパブリッククラウド環境です。欧州連合（EU）のデータプライバシー規制を遵守するように設計されており、WildFire Europeクラウドに提出されたサンプルはEU内に留まります。

  WildFire グローバルポータルにファイルを送信して分析し、高度な WildFire ヨーロッパクラウドポータルにアクセスするには、次のURLを使用してください：eu.wildfire.paloaltonetworks.com

- **Advanced WildFire Japan Cloud**（高度な **WildFire** ジャパンクラウド）

  高度な WildFire ジャパンクラウドは、日本で開催される地域的なパブリッククラウド環境です。

  WildFire グローバルポータルにファイルを送信して分析し、高度な WildFire ジャパンクラウドポータルにアクセスするには、次のURLを使用してください：jp.wildfire.paloaltonetworks.com

- **Advanced WildFire Singapore Cloud**（高度な **WildFire** シンガポールクラウド）

  高度な WildFire シンガポールクラウドは、シンガポールで開催される地域的なパブリッククラウド環境です。

  高度な WildFire グローバルポータルにファイルを送信して分析し、高度な WildFire シンガポールクラウドポータルにアクセスするには、次のURLを使用してください：sg.wildfire.paloaltonetworks.com

- **Advanced WildFire United Kingdom Cloud (**高度な **WildFire** 英国クラウド**)**

  高度な WildFire UK クラウドは、英国で展開されている地域的なパブリッククラウド環境です。

  高度な WildFire グローバルポータルにファイルを送信して解析し、高度な WildFire 英国クラウドポータルにアクセスするには、次のURLを使用してください：uk.wildfire.paloaltonetworks.com。

- **Advanced WildFire Canada Cloud (高度な WildFire カナダクラウド)**

  WildFire カナダ クラウドは、カナダでホストされている地域のパブリック クラウド環境です。

  高度な WildFire グローバルポータルにファイルを送信して解析し、高度な WildFire カナダクラウドポータルにアクセスするには、次のURLを使用してください：ca.wildfire.paloaltonetworks.com。

- **Advanced WildFire Australia Cloud (高度な WildFire オーストラリアクラウド)**

  WildFire オーストラリア クラウドは、オーストラリアでホストされている地域のパブリック クラウド環境です。

  分析のために高度な WildFire オーストラリア クラウドにファイルを送信し、高度な WildFire オーストラリア クラウド ポータルにアクセスするには、次の URL を使用してください:au.wildfire.paloaltonetworks.com。

- **Advanced WildFire Germany Cloud (高度な WildFire ドイツクラウド)**

  高度な WildFire ドイツ クラウドは、ドイツでホストされている地域のパブリック クラウド環境です。

  次の URL を使用して、ファイルを高度な WildFire ドイツ クラウドに送信して分析し、高度な WildFire ドイツ クラウド ポータルにアクセスするには、次のURLを使用してください:de.wildfire.paloaltonetworks.com。

- **Advanced WildFire India Cloud (高度な WildFire インドクラウド)**

  高度な WildFire インドクラウドは、インドでホストされている地域のパブリック クラウド環境です。

  分析のために高度な WildFire インドクラウドにファイルを送信し、高度な WildFire インドクラウドポータルにアクセスするには、次の URL を使用します: in.wildfire.paloaltonetworks.com。

- **Advanced WildFire Switzerland Cloud (*高度な WildFire スイスクラウド)**

  高度な WildFire スイス クラウドは、スイスでホストされる地域のパブリック クラウド環境です。

  次の URL を使用して、分析のために高度な WildFire スイスクラウドにファイルを送信し、高度な WildFire スイスクラウドポータルにアクセスします。ch.wildfire.paloaltonetworks.com。

- **Advanced WildFire Poland Cloud (高度な WildFire ポーランドクラウド)**

  高度な WildFire ポーランド クラウドは、ポーランドでホストされている地域のパブリック クラウド環境です。

  次の URL を使用して、分析のために高度な WildFire ポーランド クラウドにファイルを送信し、高度な WildFire ポーランド クラウド ポータルにアクセスします。pl.wildfire.paloaltonetworks.com。

- **Advanced WildFire Indonesia Cloud (**高度な **WildFire** インドネシアクラウド**)**

  高度な WildFire インドネシアクラウドは、インドネシアでホストされている地域のパブリック クラウド環境です。

  次の URL を使用して、分析のために高度な WildFire インドネシア クラウドにファイルを送信し、高度な WildFire インドネシア クラウド ポータルにアクセスします。id.wildfire.paloaltonetworks.com。

- **Advanced WildFire Taiwan Cloud (**高度な **WildFire** 台湾クラウド**)**

  高度な WildFire 台湾クラウドは、台湾でホストされている地域のパブリッククラウド環境です。

  次の URL を使用して、分析のために高度な WildFire 台湾クラウドにファイルを送信し、高度な WildFire 台湾クラウド ポータルにアクセスします。tw.wildfire.paloaltonetworks.com。

- **Advanced WildFire France Cloud (**高度な **WildFire** フランスクラウド**)**

  高度な WildFire フランスクラウドは、フランスでホストされている地域のパブリック クラウド環境です。

  次の URL を使用して、分析のために高度な WildFire フランスクラウドにファイルを送信し、高度な WildFire フランスクラウド ポータルにアクセスします。fr.wildfire.paloaltonetworks.com。

- **Advanced WildFire Qatar Cloud (**高度な **WildFire** カタールクラウド**)**

  高度な WildFire カタールクラウドは、カタールでホストされている地域のパブリッククラウド環境です。

  次の URL を使用して、分析のために高度な WildFire カタールクラウドにファイルを送信し、高度な WildFire カタールクラウド ポータルにアクセスします。qatar.wildfire.paloaltonetworks.com。

- 高度な**WildFire**韓国クラウド

  高度なWildFire韓国クラウドは、韓国でホストされている地域的なパブリック クラウド環境です。

  次のURLを使用して、解析のために高度なWildFire韓国クラウドにファイルを送信し、高度なWildFire韓国クラウド ポータルにアクセスします: kr.wildfire.paloaltonetworks.com

- 高度な**WildFire**イスラエル クラウド

  高度なWildFireイスラエル クラウドは、イスラエルでホストされている地域的なパブリッククラウド環境です。

  次のURLを使用して、解析のために高度なWildFireイスラエル クラウドにファイルを送信し、高度なWildFireイスラエル クラウド ポータルにアクセスします: il.wildfire.paloaltonetworks.com

- 高度な**WildFire**サウジアラビア クラウド

  高度なWildFireサウジアラビア クラウドは、サウジアラビアでホストされている地域的なパブリック クラウド環境です。

  次のURLを使用して、解析のために高度なWildFireサウジアラビア クラウドにファイルを送信し、高度なWildFireサウジアラビア クラウド ポータルにアクセスします: sa.wildfire.paloaltonetworks.com

- 高度な**WildFire**スペイン クラウド

  高度なWildFireスペイン クラウドは、スペインでホストされている地域的なパブリック クラウド環境です。

  次のURLを使用して、解析のために高度なWildFireスペイン クラウドにファイルを送信し、高度なWildFireスペイン クラウド ポータルにアクセスします: es.wildfire.paloaltonetworks.com

それぞれの高度な WildFireクラウド (グローバル (米国) と地域) は、他の WildFireクラウドとは独立して、サンプルを分析し、マルウェアシグネチャと評決を生成します。高度な WildFire のシグネチャと判定はグローバルに共有されるため、世界中のWildFireユーザーは、マルウェアが最初に検出された場所に関係なく、マルウェアのカバレッジの恩恵を受けることができます。各クラウドが分析するファイルタイプの詳細については、Advanced WildFire File Type Support（高度な WildFire ファイルタイプのサポート）を参照してください。

WildFire アプライアンスを使用している場合、ファイアウォールが特定のファイルを WildFire パブリッククラウドに転送し、その他のファイルを WildFire プライベートクラウドに転送してローカル分析できるWildFire ハイブリッドクラウド のデプロイメントを有効にすることができます。また、解析を実行する前にパブリック クラウドを照会することで、既知のサンプルの評決をすばやく収集するように WildFire アプライアンスを構成することもできます。これにより、WildFireアプライアンスは、プライベートネットワークとグローバルWildFireコミュニティの両方に不明なサンプルに分析リソースを割り当てることができます。

WildFire プライベート クラウド

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な WildFire もしくは Wildfire ライセンス

Palo Alto Networksプライベートクラウドの導入環境では、Palo Alto Networksファイアウォールは、お客様の企業ネットワーク上でプライベートクラウド分析を提供しているWildFireアプライアンスへファイルを転送します。

ハイブリッド クラウド転送の詳細については、「WildFireアプライアンス管理者ガイド」を参照してください。

WildFireハイブリッドクラウド

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な WildFire もしくは Wildfire ライセンス

WildFire ハイブリッド クラウド展開のファイアウォールは、特定のサンプルをパロアルトネットワークスのホスト型 WildFire パブリック クラウドの 1 つに転送し、その他のサンプルを WildFire アプライアンスによってホストされる WildFire プライベート クラウドに転送できます。

ハイブリッド クラウド転送の詳細については、「WildFireアプライアンス管理者ガイド」を参照してください。

WildFire FedRAMP認定クラウド プラットフォーム

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。 ❑ 高度なWildFire FedRAMPアドオン

Palo Alto Networksは、WildFireグローバルクラウド、プライベートクラウド、ハイブリッドクラウドの展開オプションに加えて、安全なクラウド運用標準に準拠する必要がある組織向けに、いくつかの高セキュリティのFedRAMP認定クラウド環境へのアクセスも提供しています。FedRAMP認定クラウドは、高と中程度の影響レベルで利用でき、中程度は2つのクラウド構成で利用できます。高度なWildFire政府専用クラウドはFedRAMPの高度な認証基準に準拠しており、高度なWildFire政府専用クラウドとWildFire米国政府専用クラウドは、FedRAMPの中程度の認定基準に準拠しています。

WildFire米国政府専用クラウド*(FedRAMP*の中程度の認証基準に準拠*)*は廃止される予定です。*Palo Alto Networks*では、すべての新規顧客に対して、高度な*WildFire*クラウドの強化された機能セットとサポートを備えた高度な*WildFire*パブリック セクター クラウドの使用を推奨しています。

FedRAMPの中程度のクラウド(高度なWildFire政府専用クラウドとWildFire米国政府専用クラウド)は、Palo Alto Networksのお客様には一般にご利用いただけますが、FedRAMPの高度な認証基準に準拠している高度なWildFire政府専用クラウドは、連邦政府、国防総省、または承認された防衛産業基盤(DIB)のお客様のみがご利用いただけます。

これらのサービスは機密性が高いため、FedRAMPクラウドには他のサービスとは異なる特定のオンボーディング プロセスがあります。詳細については、特定のFedRAMPクラウド タイプを参照してください:

- 高度なWildFire政府専用クラウド
- 高度なWildFireパブリック セクター クラウド
- WildFire:米国政府専用クラウド

上記のFedRAMPクラウドは、同じデバイス上で混在させることはできません。また、高度なWildFireグローバル クラウドまたはリージョン クラウドと同時に使用することもできません。ただし、どのFedRAMPクラウドも、他のクラウドベースのセキュリティ サービス(Advanced Threat Prevention、DLPなど)と連携して使用できます。単一のデバイスに複数のFedRAMPセキュリティ レベルを組み込む必要がある場合は、個別のアカウントIDを使用する必要があります。オンボーディングが完了すると、他の高度なWildFireクラウドと同じ方法で、アンチウイルス セキュリティ プロファイルとAPIでFedRAMPクラウドURLを参照できるようになります。

高度な**WildFire**政府専用クラウド

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。 ❑ 高度なWildFire GovCloudアドオン

Palo Alto Networksは、連邦政府、国防総省、または認定防衛産業基盤(DIB)のお客様に、FedRAMP (Federal Risk and Authorization Management Program)の高認証基準に準拠した高セキュリティのマルウェア解析プラットフォームである高度なWildFire政府専用クラウドを提供しています。

高度なWildFireパブリック セクター クラウドは、商用または政府向けクラウドの地域とは別の別個のエンティティとして動作します — 電子メールアドレス、IPアドレス、パッシブDNSなど、解析のために送信された検体に存在する可能性のあるプライバシー情報は、他のWildFireクラウド インスタンスと共有されません。しかしながら、高度なWildFireパブリック クラウドによって生成された脅威データを活用することで、ファイル解析を通じて生成される保護とアンチウイルス シグネチャ同様、カバレッジ能力を最大化することが可能です。

*Palo Alto Networks*の高度な*WildFire FedRAMP*承認については、以下にアクセスしてください:FedRAMP.gov

Palo Alto NetworkのWildFire FedRAMP承認については、以下にアクセスしてください:Palo Alto Networks政府専用クラウドサービス - WildFire

高度なWildFire政府専用クラウドには、標準の商用の高度なWildFireパブリック クラウドといくつかの機能的な違いがあります。次の機能は、高度なWildFire政府専用クラウドに接続しているお客様はご利用いただけません。

- ベア メタル解析は、高度なWildFire米国政府専用クラウドの地域ではサポートされていません。
- 高度なWildFire政府専用クラウドにWildFireポータル経由でアクセスすることはできません。
- 機能を削除する権利は、サービス リクエストなしでは利用できません。

高度な**WildFire**政府専用クラウドの使用を開始する

ネットワーク内で高度なWildFire米国政府専用クラウドを使用する適切性を判断するには、社内の手順に従ってください。これには、リスク解析の実施、CSP提出パッケージの評価、認可の承認などが含まれますが、これらに限定されません。追加の運用詳細情報についてのご相談は、Palo Alto Networks営業担当 / 高度なWildFire:米国政府専用クラウド担当に連絡して下さい。

高度なWildFire米国政府専用クラウド地域へのアクセスは、FedRAMP認定サービスを運用するための適切な組織要件を満たしたときに開始されます。

オンボードプロセスを開始するには、Palo Alto Networksアカウントチームにお問い合わせください。高度なWildFireアクティベーションが完了したら、次のURLを使用して不明なファイルと電子メールリンクを解析用に転送するようにファイアウォールを再構成します: gov-cloud.wildfire.paloaltonetworks.com詳細は、「WildFire解析へのファイル転送」を参照してください。追加の支援が必要な場合は、Palo Alto Networksカスタマーサポートにお問い合わせください。

高度な**WildFire**パブリック セクター クラウド

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。 ☐ 高度なWildFire PubSecアドオン

Palo Alto Networksは、FedRAMP (Federal Risk and Authorization Management Program)の中程度の認証基準に準拠した高セキュリティのマルウェア解析プラットフォーム「高度なWildFireパブリック セクター クラウド」をお客様に提供しています。高度なWildFireパブリック セクター クラウドは、WildFire米国政府専用クラウドに置き換わります。

高度なWildFireパブリック セクター クラウドは、商用または政府向けクラウドの地域とは別の別個のエンティティとして動作します — 電子メールアドレス、IPアドレス、パッシブDNSなど、解析のために送信された検体に存在する可能性のあるプライバシー情報は、他のWildFireクラウド インスタンスと共有されません。しかしながら、高度なWildFireパブリック クラウドによって生成された脅威データを活用することで、ファイル解析を通じて生成される保護とアンチウイルス シグネチャ同様、カバレッジ能力を最大化することが可能です。

*Palo Alto Networks*の高度な*WildFire FedRAMP*承認については、以下にアクセスしてください:FedRAMP.gov

高度なWildFireパブリック セクター クラウドは、標準的な商用の高度なWildFireパブリック クラウドといくつかの機能的な違いがあります。高度なWildFireパブリック セクター クラウドに接続するお客様は、以下の機能をご利用いただけません。

- ベア メタル解析は、高度なWildFire米国政府専用クラウドの地域ではサポートされていません。
- 高度なWildFire米国パブリック セクター クラウドの地域にWildFireポータル経由でアクセスすることはできません。
- 機能を削除する権利は、サービス リクエストなしでは利用できません。

高度な**WildFire**パブリック セクター クラウドの使用を開始する

ネットワーク内で高度なWildFireパブリック セクター クラウドを使用することの適切性を判断するには、社内の手順に従ってください。これには、リスク解析の実施、CSP提出パッケージの評価、認可の承認などが含まれますが、これらに限定されません。追加の運用詳細情報についてのご相談は、Palo Alto Networks営業担当 / 高度なWildFire:米国パブリック セクター クラウド担当に連絡して下さい。

高度なWildFireパブリック セクター クラウド地域へのアクセスは、FedRAMP認定サービスを運営するための適切な組織要件を満たした時点から始まります。

オンボードプロセスを開始するには、Palo Alto Networksアカウントチームにお問い合わせください。高度なWildFireアクティベーションが完了したら、次のURLを使用して不明なファイルと電子メールリンクを解析用に転送するようにファイアウォールを再構成します: pubsec-cloud.wildfire.paloaltonetworks.com

詳細は、「WildFire解析へのファイル転送」を参照してください。追加の支援が必要な場合は、Palo Alto Networksカスタマーサポートにお問い合わせください。

WildFire:米国政府専用クラウド

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。 ❑ WildFire U.S.政府機関オンボーディング

*2024*年*7*月*15*日時点で、*Palo Alto Networks*の*WildFire*米国政府専用クラウドは高度なWildFire政府専用クラウドおよび高度なWildFireパブリック セクター クラウドに置き換えられました。これにより、強化された機能セットを備えた新しいコードベースを運用する安全性の高い高度な*WildFire*クラウド環境にアクセスできます。そのため、*Palo Alto Networks*は*WildFire*米国政府専用クラウドへの新規顧客のオンボーディングを行わなくなりました。既存のお客様は、*2024*年*11*月*30*日の廃止予定日までは、引き続き*WildFire*米国政府専用クラウドにアクセスできます。廃止日になると、既存の*URI*は高度な*WildFire*パブリック セクター クラウドにリダイレクトされます。

新しいクラウド サービスの詳細については、*Palo Alto Networks*の営業担当者に問い合わせて、その他の運用上の詳細についてご確認ください。

Palo Alto Networks WildFire U.S.（米国）政府専用クラウドは、FedRAMP（Federal Risk and Authorization Management Program連邦リスクおよび承認管理プログラム）に承認された高セキュリティのマルウェア解析プラットフォームです。このWildFireクラウド環境は、クラウド製品とサービスのセキュリティ評価、承認、および継続的な監視に標準化されたアプローチを必要とする米国連邦政府機関による使用のみを目的としています。WildFire:米国政府のクラウドは独立した別個のエンティティとして動作します—電子メールアドレス、IPアドレス、パッシブDNSなど、解析のために送信される検体内に存在するプライバシー情報は、他のWildFireクラウドインスタンスと共有されません。しかしながら、ファイル解析を通じて生成される保護とアンチウイルスシグネチャ同様、WildFireパブリッククラウドによって生成された脅威データを活用し、カバレッジ能力を最大化することが可能です。

Palo Alto NetworkのWildFire FedRAMP承認については、以下にアクセスしてください:Palo Alto Networks政府専用クラウドサービス - WildFire

WildFireパブリッククラウド（グローバルおよび地域クラウド）およびWildFire米国政府専用クラウドは、パブリッククラウドとは異なる機能を複数備えています。WildFire:米国政府専用クラウドに接続しているお客様は以下の機能は利用できません:

- ベアメタル解析は、米国では対応していません。Government cloud.

- スクリプトファイル（Bat、JS、BVS、PS1、Shellスクリプト、およびHTA）解析は、現在サポートされていません。
- WildFire:米国政府専用クラウドにWildFireポータル経由でアクセスすることはできません。
- WildFire:米国政府専用クラウドを他のクラウドベースのサービスと統合することはできません。
- 削除機能は利用できません。
- WildFire:米国政府専用クラウドは現在、高度な WildFire 分析をサポートしていません。

WildFireを開始する**:**米国政府専用クラウド

WildFire:米国政府専用クラウドに接続するには、アクセスを申請する必要があります。WildFireの使用の適性を判断するための内部手順に従ってください。リスク分析の実施、CSP 提出パッケージの評価、認可の承認など、ネットワーク内の米国政府専用クラウド。追加の運用詳細情報についてのご相談は、Palo Alto Networks営業担当 / WildFire:米国政府専用クラウド担当に連絡して下さい。

WildFire U.S.（米国）政府専用クラウドへのアクセス要求は、FedRAMP 認定サービスを運用するための適切な組織要件を満たしたときに開始されます。WildFire米国政府専用クラウドにアクセスできるエンティティ カテゴリは2つあります。米国政府請負業者および米国連邦機関(およびその他の承認された政府機関)。両方のエンティティには、WildFire米国政府専用クラウドにアクセスするための特定の要件があります。

1. **U.S.**連邦機関

   米国連邦政府機関、省庁、および局は、機関の業務内でWildFire米国政府専用クラウドの運用を許可する指定承認機関(DAA)から運用権限(ATO)を取得する必要があります。その後、アクセス権が付与されます。

   1. Palo Alto Networks連絡先(fedramp@paloaltonetworks.com)にWildFire米国政府専用クラウドを使用する意図を通知します。
   2. info@fedramp.govに要求を送信します。
   3. FedRAMPパッケージ アクセス リクエスト フォームを記入し、info@fedramp.govに送信します。

      *FedRAMP Program Management Office (PMO)*がフォームを確認し、通常、*WildFire FedRAMP*パッケージへの一時的な*30*日間のアクセスを発行します。
   4. WildFire米国政府専用クラウドのFedRAMPセキュリティ パッケージを確認します。Government cloud.WildFire米国政府専用クラウドを組織に導入するために必要な内部プロセスを完了します。
   5. ATOを発行します。
   6. WildFire米国政府専用クラウドへの恒久的なアクセスを取得するための要求をFedRAMP PMOに送信します。

2. **U.S.**政府請負業者

   米国政府請負業者で、WildFire米国政府専用クラウドを使用するまたはクラウドにアクセスする者は、次の要件を満たす必要があります。

   1. 米国市民であること。
   2. 米国連邦政府機関と、電子メールでのやり取り、文書の共有、その他の形式のインターネット通信など、インターネットを利用した情報交換を業務要件とする有効な契約(または下請契約)を締結している。
   3. 請負業者の雇用が終了すると、ユーザーはWildFire米国政府専用クラウドの使用またはアクセスを停止する必要があります。
   4. Palo Alto NetworksのEULAに含まれる機密保持条項を遵守すること。

組織が運営許可(ATO)を発行した後、または該当する場合は米国政府の請負業者がすべての使用要件を満たしている場合にのみ、WildFire米国政府専用クラウドへのアクセスをPalo Alto Networksのアカウント チームにリクエストできます。

1. 米国の実現可能性を判定するには、FedRAMP プログラム管理オフィス（FedRAMP Program Management Office (PMO)）にお問い合わせください。セキュリティニーズによる政府専用クラウド。
2. FedRAMP Marketplace指定のPalo Alto Networks連絡先にお問い合わせください。連絡先は、サービスに関する追加情報、および特定のWildFireの導入に関連するその他の操作の詳細を提供します。
3. オンボードプロセスを開始するには、Palo Alto Networksアカウントチームにお問い合わせください。アカウントチームは、お客様の詳細と展開の詳細に関する次の情報を要求します。
   - 連絡先。
   - WildFire U.S.（米国）への移行についての簡潔な説明。Government cloud.
   - Palo Alto Networks EULAで概説されている機密保持規定への組織のコンプライアンスのステートメント。
   - すべてのファイアウォールゲートウェイ（管理プレーンを含む）、およびPanoramaのすべてのインスタンスの Egress IPアドレス。
4. WildFire Program Management がWildFire 米国政府専用クラウドの使用を承認すると（通常1～3営業日）、Palo Alto Networks 開発オペレーションが適切な制御を適用します。
5. WildFire 米国政府専用クラウドへのアクセスが認められた後、以下のURLを使用して、未知のファイルと電子メールリンクを解析のために転送するようにファイアウォールを再設定します: wildfire.gov.paloaltonetworks.com詳細は、「WildFire解析へのファイル転送」を参照してください。追加の支援が必要な場合は、Palo Alto Networksカスタマーサポートにお問い合わせください。

ファイルタイプサポート

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

次の表に、WildFireクラウド環境での分析でサポートされるファイルタイプを示します。

WildFire がサポートする特定のファイルタイプの包括的なリストについては、サポートされているファイルの種類 (完全なリスト)を参照してください。

File Types Supported for Analysis（分析用にサポートされているファイルの種類）	高度な **WildFire**パブリッククラウド（全手のリージョン）	**WildFire U.S.**政府専用クラウド	高度な **WildFire**ポータル	**API (**直接アップロード、全リージョン**)**
電子メール内のリンク	✓	✓	✓	
Androidアプリケーションパッケージ（APK）ファイル	✓	✓	✓	
Adobe Flashファイル	✓	✓	✓	
Java アーカイブ（JAR）ファイル	✓	✓	✓	
Microsoft Office ファイル (SLK	✓	✓	✓	

File Types Supported for Analysis（分析用にサポートされているファイルの種類）	高度な **WildFire**パブリッククラウド（全手のリージョン）	**WildFire U.S.**政府専用クラウド	高度な **WildFire**ポータル **| API (**直接アップロード、全リージョン**)**
ファイルと IQY ファイルを含む)			
ポータブル実行可能ファイル (MSI ファイルを含む)	✓	✓	✓
ポータブルドキュメントフォーマット（PDF）ファイル	✓	✓	✓
Mac OS X*ファイル	✓	✓	✓
Linux (ELF ファイルおよびシェルスクリプト) ファイル	✓	✓	✓
アーカイブ(RAR、7-Zip、ZIP**)ファイル	✓	✓	✓
スクリプト (BAT、JS、VBS、PS1、および HTA) ファイル	✓	✘	✓
Pythonスクリプト	✓	✓	✓
Perlスクリプト	✘	✘	✓

File Types Supported for Analysis（分析用にサポートされているファイルの種類）	高度な WildFireパブリッククラウド（全手のリージョン）	WildFire U.S.政府専用クラウド	高度な WildFireポータル	API (直接アップロード、全リージョン)
アーカイブ(ZIP [直接アップロード]およびISO)ファイル	✗	✗	✓	
イメージ (JPG および PNG) ファイル	✗	✗	✓	

* DMG、PKG、ZBundleファイルの静的解析は高度なWildFireグローバル(米国)リージョンとヨーロッパ クラウド リージョンでのみ利用可能ですが、その他のMac OS Xファイル(fatとmacho)の静的解析はすべてのリージョン クラウドでサポートされています。すべてのMac OS Xファイルの動的解析は、高度なWildFireグローバル(米国)リージョンとヨーロッパ クラウド リージョンでのみサポートされています。

** ZIPファイルは、解析のために高度なWildfireクラウドに直接転送されません。代わりに、最初に firewall によってデコードされ、WildFire 分析プロファイル基準に一致するファイルは、分析のために個別に転送されます。

その他の情報をお探しですか？

- 高度な *WildFire*クラウドのそろぞれの導入の詳細については、高度な WildFire の導入を参照してください。
- *WildFire*解析でサポートされている各ファイルタイプの詳細については、File Analysis（ファイル分析）を参照してください。

サポートされているファイルの種類 (完全なリスト)

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	

次の表に、WildFire 分析でサポートされるファイル タイプを示します。[Forwarding Support (転送サポート)]列で[Yes (はい)]とマークされているファイルには、Webトラフィック(HTTP/HTTPS)および電子メール プロトコル(SMTP、IMAP、POP)でMIMEエンコードされたファイルが含まれます。

サポートされているコンテンツ タイプ	拡張例	転送サポート
7zip アーカイブ	7z	あり
Adobe Flash ファイル	swf	あり
Android APK	apk	あり
Android DEX	dex	あり
バッチ	bat	あり
bzip2アーカイブ	bz	あり
カンマ区切りの値	csv	いいえ
DLL、DLL64	dll	あり
.ELF	elf	あり
Gzipアーカイブ	gz	いいえ
HTMLアプリケーション	hta	あり
ISO	iso	いいえ
JAVAクラス	class	あり
JAVA JAR	jar	あり
JavaScript/JScript	js、jse、wsf	はい (JS のみ)

サポートされているコンテンツ タイプ	拡張例	転送サポート
JPEG (Joint Photographic Experts Group)	jpg	いいえ
リンク	elink	あり
Mach-O	macho	あり
macOS アプリ インストーラー	pkg	あり
ZIPアーカイブのmacOSアプリ バンドル	zbundle	いいえ
macOSユニバーサル バイナリ ファイル	fat	いいえ
macOS ディスク イメージ	dmg	あり
Microsoft Excel 97 - 2003 ドキュメント	xls	あり
Microsoft Excel ドキュメント	xlsx	あり
Microsoft One Noteドキュメント	1	あり
Microsoft PowerPoint 97 - 2003 ドキュメント	ppt	あり
Microsoft PowerPoint ドキュメント	pptx	あり
Microsoft シンボリック リンク ファイル	スルク	あり
Microsoft Web クエリ ファイル	iqy	あり
Microsoft Word 97 - 2003 ドキュメント	doc	あり

サポートされているコンテンツ タイプ	拡張例	転送サポート
Microsoft Word文書	docx	あり
OpenDocument スプレッドシート ドキュメント	ods	いいえ
OpenDocument テキストドキュメント	odt	いいえ
PDF	pdf	あり
PE、PE64	exe	あり
Perl スクリプト	pl	いいえ
PNG (ポータブル ネットワーク グラフィック ファイル)	png	いいえ
PowerShell	ps1	あり
Python スクリプト	py	あり
RAR アーカイブ	rar	あり
RTF	rtf	あり
シェルスクリプト	sh	あり
Tarアーカイブ	tar	いいえ
VBスクリプト	VBS、VBE	はい (VBS のみ)
Windows インストーラー パッケージ	msi	あり
Windowsリンクファイル	lnk	あり
Windows スクリプト	wsf	いいえ
ZIP アーカイブ	zip	いいえ

サポートされているコンテンツ タイプ	拡張例	転送サポート
ASP (アクティブなサーバー ページ)	アスプ	いいえ
ASPX (拡張アクティブ・サーバー・ページ)	aspx	いいえ
XML (拡張マークアップ言語)	xml	いいえ
HTML (ハイパーテキスト マークアップ言語)	html	いいえ

高度な WildFire の例

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

次のシナリオ例は、Advanced WildFire™ ライフサイクル全体を要約したものです。この例では、販売パートナーが Dropbox にアップロードした新しいソフトウェア販売ツールを Palo Alto Networks の営業担当者がダウンロードします。販売パートナーは、感染した販売ツール インストール ファイルを知らずにアップロードし、営業担当者が感染ファイルをダウンロードします。

この例では、トラフィックが SSL で暗号化されている場合でも、Palo Alto Networks ファイアウォールと高度な WildFire を併用することによってエンド ユーザーがダウンロードしたゼロデイ マルウェアを検出する方法を示します。Advanced WildFire がマルウェアを識別すると、ログがファイアウォールに送信され、ファイアウォールは管理者に警告し、管理者はマルウェアを根絶するようユーザーに連絡します。次に、Advanced WildFire がマルウェアの新しいシグネチャを生成し、その後、ファイアウォールがシグネチャを自動的にダウンロードして、将来の暴露から保護します。一部のファイル共有 Web サイトには、アップロード時にファイルをチェックするアンチウイルス機能がありますが、既知のマルウェアしか防止できません。

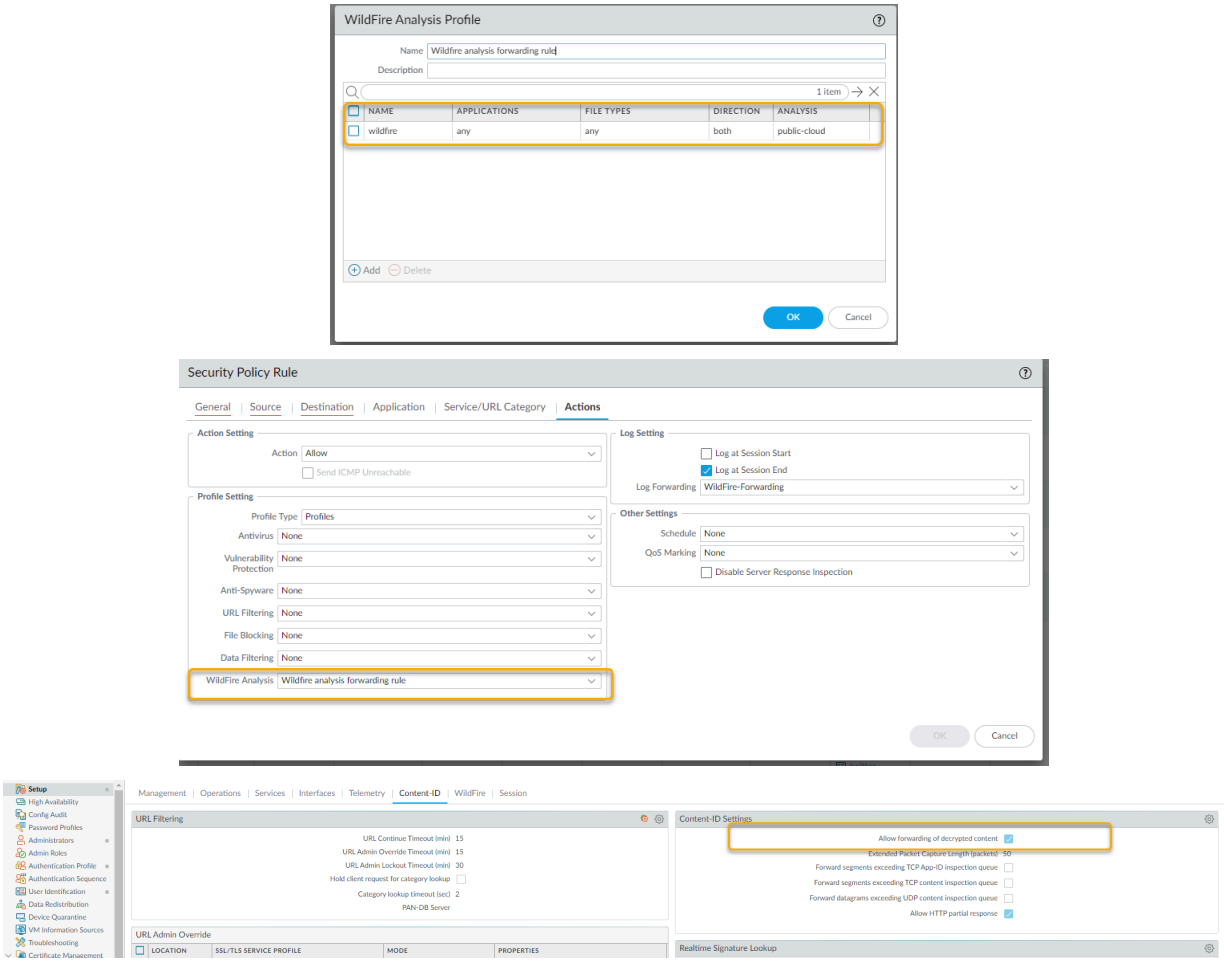
このサンプルでは、*SSL*で暗号化されたウェブサイトを例に取って作業を進めていきます。またここでは、復号化後の内容を分析用に転送するオプションを含め、ファイアウォールによる復号化が有効となっています。

STEP 1 | パートナー企業の営業担当者が sales-tool.exe という名前の販売ツール ファイルを自分の Dropbox アカウントにアップロードし、ファイルへのリンクが記載された電子メールを Palo Alto Networks の営業担当者に送信します。

STEP 2 | Palo Alto の営業担当者は、販売パートナーから電子メールを受信し、Dropbox サイトへのダウンロード リンクをクリックします。次に営業担当者は、**Download (**ダウンロード**)**をクリックしてファイルをデスクトップに保存します。

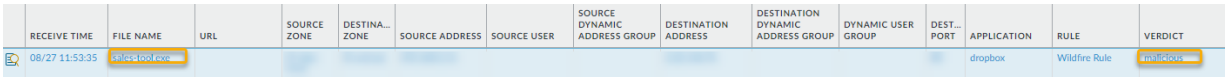
STEP 3 | Palo Alto の営業担当者を保護しているファイアウォールには、セキュリティ ポリシーにWildFire分析プロファイル ルールが適用されています。このプロファイルでは、サポートしている形式のファイルがアプリケーションによってダウンロードまたはアップロード

される際にファイルを検査します。ファイアウォールは、email-link ファイル タイプを転送するように設定することもでき、これにより、SMTP および POP3 の電子メール メッセージに含まれている HTTP/HTTPS リンクを抽出することができます。営業担当者がダウンロードをクリックするとすぐに、ファイアウォールは sales-tool.exe ファイルを Advanced WildFire に転送し、そこでファイルがゼロデイ マルウェアについて分析されます。営業担当者が SSL で暗号化される Dropbox を使用する場合でも、ファイアウォールはトラフィックを復号化するように設定されているため、すべてのトラフィックを検査することができます。以下のスクリーン ショットは、WildFire 分析プロファイル ルール、WildFire 分析プロファイル ルールが割り当てられたセキュリティ ポリシー ルール、および復号化されたコンテンツの転送が有効化された画面を示しています。

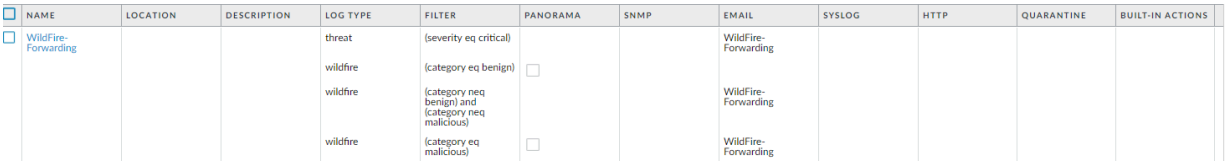


STEP 4 | この時点で、高度な WildFire はファイルを受信し、200 種類を超える悪意のある動作に関して分析を行っています。

STEP 5 | Advanced WildFire はファイル分析を完了すると、分析結果とともに Advanced WildFire ログをファイアウォールに送り返します。この例のログでは、ファイルが有害であることが示されています。



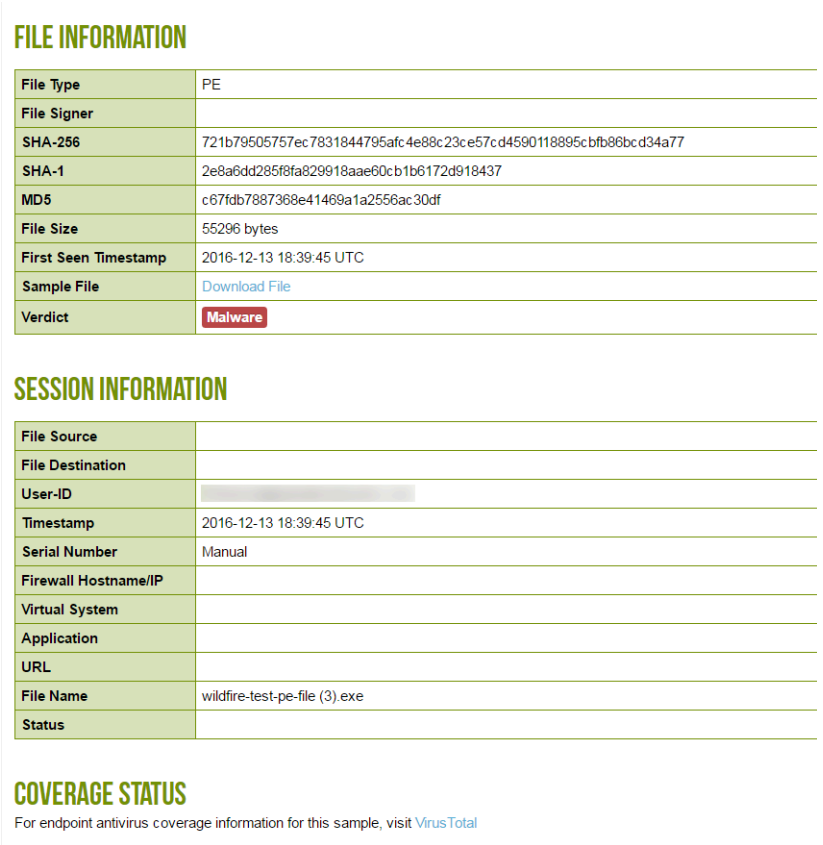
STEP 6 | ファイアウォールは、マルウェアが検出されたときにセキュリティ管理者にアラートを送信するログ転送プロファイルを使用して構成されています。



STEP 7 | セキュリティ管理者は、User-ID が設定されている場合は名前でユーザーを識別し、User-ID が有効になっていない場合は IP アドレスで識別します。この時点で、管理者は営業担当者が使用しているネットワークまたは VPN 接続を切断することができます。次に、デスクトップ サポート グループに連絡して、ユーザーと共にシステムのチェックおよびクリーニングを行います。

高度な WildFire 詳細分析レポートを使用すると、デスクトップ サポート担当者は、高度な WildFire分析レポートに詳細に記載されているファイル、プロセス、およびレジストリ情報を確認することで、ユーザー システムがマルウェアに感染しているかどうかを判断できます。

ユーザーがマルウェアを実行した場合、サポート担当者は、手動でシステムをクリーンアップするか、または初期状態にリセットすることができます。



FILE INFORMATION

File Type	PE
File Signer	
SHA-256	721b79505757ec7831844795afc4e88c23ce57cd4590118895cbfb86bcd34a77
SHA-1	2e8a6dd285f8fa829918aae60cb1b6172d918437
MD5	c67fdb7887368e41469a1a2556ac30df
File Size	55296 bytes
First Seen Timestamp	2016-12-13 18:39:45 UTC
Sample File	Download File
Verdict	Malware

SESSION INFORMATION

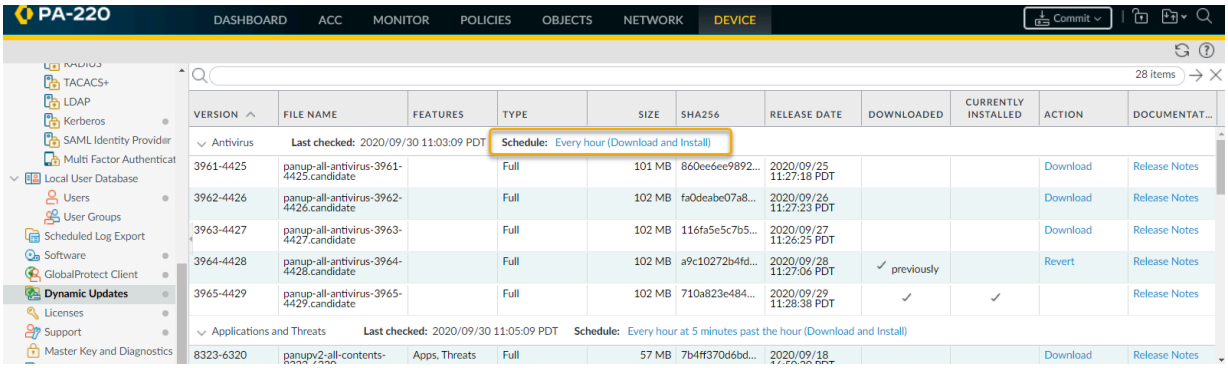
File Source	
File Destination	
User-ID	
Timestamp	2016-12-13 18:39:45 UTC
Serial Number	Manual
Firewall Hostname/IP	
Virtual System	
Application	
URL	
File Name	wildfire-test-pe-file (3).exe
Status	

COVERAGE STATUS

For endpoint antivirus coverage information for this sample, visit VirusTotal

STEP 8 | 管理者がマルウェアを識別し、ユーザーのシステムがチェックされています。今後の感染をどのように防止できますか?回答:この例では、管理者は、高度な WildFire シグネチャを 15 分ごとにダウンロードしてインストールし、ウイルス対策アップデートを 1 日に 1 回ダウンロードしてインストールするようにファイアウォールにスケジュールを設定します。営業担当者が感染ファイルをダウンロードしてから 1 時間半以内に、高度な WildFire はゼロデイ マルウェアを特定し、シグネチャを生成し、それを Palo Alto Networks が提供する高度な WildFire 更新シグネチャ データベースに追加し、ファイアウォールにダウンロードして、新しいシグネチャをインストールしました。これで、このファイアウォールと、高度な WildFire とアンチウイルス シグネチャをダウンロードするように設定されている他の

Palo Alto Networks ファイアウォールは、新しく検出されたマルウェアの感染から保護されます。次のスクリーンショットは、高度な WildFire 更新スケジュールを示しています。



これらはすべて、ほとんどのアンチウイルス ベンダーがゼロデイのマルウェアを検出するよりも、かなり早い段階で実行されます。この例では、マルウェアは非常に短時間でゼロデイとは見なされなくなっています。これは、Palo Alto Networks ではそのマルウェアをすでに検出しており、その後の感染からユーザーを保護したためです。

アドバンスド WildFireの使用を開始する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

次の手順は、ファイアウォール上で Advanced WildFire™ を開始するための簡単なワークフローを示しています。開始する前に高度な WildFire についてさらに詳しく知りたい場合は、高度な WildFire の概要 を確認し、高度な WildFire のベストプラクティスをレビューしてください。

WildFire プライベート クラウドまたはハイブリッド クラウドの使用については、WildFireアプライアンスの管理を参照してください。

Prisma Accessで高度なWildFireを使用している場合は、WildFire解析セキュリティ プロファイルを高度な WildFire 分析のためのファイルの転送に設定する前に製品についてよく理解してください。

STEP 1 | 高度な WildFire または WildFire サブスクリプションを取得します。サブスクリプションがない場合でも、PEファイルを転送してWildFire分析できます。

STEP 2 | どの高度な WildFire の導入が自分に合っているかを判断します。

- 高度な WildFireグローバルクラウド - サンプルをPalo Alto Networksがホストする高度なWildFireパブリック クラウドに転送します。
- WildFire U.S.政府専用クラウド - 検体をPalo Alto Networksがホストする WildFire U.S政府専用クラウドに転送します。Government cloud.

WildFire プライベート クラウドまたはハイブリッド クラウドを展開している場合は、*WildFire*アプライアンスの管理を参照してください。

STEP 3 | ライセンスがファイアウォール上でアクティブであることを確認します。

1. ファイアウォールにログインします。
2. **Device (デバイス)** > **Licenses (ライセンス)**の順に選択し、WildFireライセンスが有効になっていることを確認します。

   WildFireライセンスは表示されませんが、ライセンス管理の選択肢を1つ選ぶことでライセンスを有効化します。

STEP 4 | ファイアウォールをWildFireに接続し、WildFire設定を構成します。

1. **Device (**デバイス）> **Setup**（セットアップ） > **WildFire** の順に選択し、General Settings（一般設定）を編集します。
2. **WildFire**パブリック クラウド フィールドを使用して、サンプルを高度な WildFire パブリック クラウドに転送します。
3. ファイアウォールが転送するファイルのサイズ制限を定義し、WildFire のログとレポート設定を構成します。

   *PE*の***File Size***（ファイルサイズ）を*10 MB*の最大サイズ制限に設定し、他のすべてのファイルタイプの***File Size***（ファイルサイズ）をデフォルト値のままにすることが高度な WildFire のベストプラクティスです。
4. **OK**をクリックして、WildFire General Settings（一般設定）を保存します。

STEP 5 | 高度な WildFire 分析のために、ファイアウォールが復号化された SSL トラフィックを転送できるようにします。

これは高度な WildFire 推奨のベストプラクティスです。

STEP 6 | 分析のためにサンプルの提出を開始します。

1. WildFireに転送し分析するトラフィックを定義します。（**Objects (**オブジェクト**)** > **Security Profiles (**セキュリティプロファイル**)** > **WildFire Analysis (WildFire** 分析**)**を選択し、WildFire Analysis（WildFire 分析）プロファイルを変更または**Add**（追加）します）。

   ベストプラクティスとして、*WildFire Analysis* のデフォルト プロファイルを使用して、ファイアウォールが許可するトラフィックを完全にカバーできるようにします。カスタム*WildFire Analysis*（*WildFire* 分析）プロファイルを作成する場合は、***Any***（すべて）のファイルタイプを転送するようにプロファイルを設定します。これにより、ファイアウォールは、新しくサポートされているファイルタイプの転送を自動的に開始します。
2. 各プロファイル ルールについて、分析のためにサンプルを高度な WildFireクラウドに転送する 宛先 として **public-cloud** を設定します。
3. WildFire分析プロファイルをセキュリティ ポリシー ルールにアタッチします。ポリシールールに一致するトラフィックは、WildFire分析（**Policies (**ポリシー**)** > **Security (**セキュリティ**)**およびセキュリティポリシールールの **Add**（追加）または変更）のために転送されます。

STEP 7 | ファイアウォールを有効にして、最新の Advanced WildFire シグネチャを取得します。

新しい高度な WildFire シグネチャはリアルタイムで取得され、マルウェアを検出および識別します。PAN-OS 9.1 以前を使用している場合は、5分ごとに新しいシグネチャを受信することができます。

- PAN-OS 9.1 以前
  1. **Device**（デバイス） > **Dynamic Updates**（動的更新）の順に選択します:
     - **WildFire**の更新が表示されていることを確認します。
     - **Check Now**（今すぐチェック）を選択して、最新のシグネチャ更新パッケージを取得します。
  2. 最新の高度なWildFireシグネチャをダウンロードしてインストールする**Schedule**（スケジュール）を設定します。
  3. **Recurrence** フィールドを使用して、firewall が新しい更新をチェックする頻度を 毎分 に設定します。

     新しい *WildFire* 署名が *5* 分ごとに利用可能であるため、この設定により、*firewall* が可用性から *1* 分以内にこれらの署名を取得できるようになります。
  4. ファイヤーウォールが更新を取得するため、ファイヤーウォールを有効化してこれらの更新を**Download and Install**（ダウンロードしてインストール）します。
  5. **OK** をクリックします。
- PAN-OS 10.0 以降
  1. **Device**（デバイス） > **Dynamic Updates**（動的更新）の順に選択します:
  2. **WildFire** の更新が表示されていることを確認します。
  3. スケジュールを選択して更新頻度を設定し、**Recurrence**（繰り返し） フィールドを使用して、WildFire シグネチャを**Real-time**（リアルタイム）で取得するようにファイアウォールを設定します。
  4. **OK** をクリックします。

STEP 8 | 高度なWildFireが識別するマルウェアを含むStart scanning traffic for threats（脅威のトラフィックのスキャンを開始）します。

default（デフォルト）のウイルス対策プロファイルをセキュリティポリシールールに添付して、ルールがWildFireウイルス対策シグネチャ（**Policies (**ポリシー**)** > **Security (**セキュリティ**)**を選択し、ルールに対して定義された**Actions**（アクション）を追加または変更）に基づいて許可するトラフィックをスキャンします。

STEP 9 | 高度な WildFire が関連リンクを悪意のあるリンクまたはフィッシングとして識別した Web サイトへのサイト アクセスを制御します。

このオプションを使用するには、*PAN-DB URL*フィルタリングライセンスが必要です。*URL Filtering*（*URL*フィルタリング）の詳細、および*URL*カテゴリに基づいて*Web*サイトのアクセスと企業の資格情報の送信（フィッシング詐欺を防止するため）を制御する方法についてご覧ください。

URL フィルタリングの設定へ

1. Select **Objects (オブジェクト)** > **Security Profiles (セキュリティプロフィール)** > **URL Filtering (URL**フィルタリング**)**を選択し、URLフィルタリングプロファイルを**Add**（追加）または変更します。
2. **Categories**（カテゴリ）を選択し、フィッシングおよび悪意のあるURLカテゴリの**Site Access**（サイトアクセス）を定義します。
3. ユーザーがこれらのカテゴリのサイトにアクセスするのを**Block**（ブロック）するか、アクセスを許可しますが、ユーザーがこれらのカテゴリのサイトにアクセスしたときに**Alert**（警告）を生成して、そのようなイベントの可視性を確保します。
4. Credential Phishing Prevention（資格情報のフィッシング防止）を有効にすると、ユーザーは信頼できないサイトに資格情報を送信することができなくなります。
5. 新規または更新されたURLフィルタリングプロファイルを適用し、セキュリティポリシールールに添付して、許可されたトラフィックにプロファイル設定を適用します。
    1. **[Policies]** > **[**セキュリティ**]** > セキュリティポリシー ルールを **[**追加**]** または変更します。
    2. **Actions**（アクション）を選択し、Profile Settings （プロファイル設定）セクションで**Profile Type**（プロファイルタイプ）をProfiles（プロファイル）に設定します。
    3. 新しいまたは更新された**URL Filtering**（**URL** フィルタリング）プロファイルをポリシー ルールに適用します。
    4. **OK** をクリックしてセキュリティ ポリシー ルールを保存します。

STEP 10 | ファイヤーウォールがサンプルの転送に成功したことを確認します。

- 安全なファイルのロギングを有効化している場合は、**Monitor**（監視） > **WildFire Submissions**（**WildFire** への送信）の順に選択し、分析用に送信した安全なファイルのエントリをログに記録されることを確認します。(ファイアウォールが WildFireクラウドに接続されていることを確認した後で無害なファイルのログを無効にしたい場合は、デバイス > セットアップ > **WildFire]** を選択し、**[**無害なファイルのレポート**]**をクリアします)。
- ファイヤーウォールが特定のサンプルを転送したかどうかを確認できる他のオプションは、ファイヤーウォールがファイルタイプ別に転送したサンプルを見ること、およびファイヤーウォールが転送したサンプルの総数を見ることです。
- サンプル マルウェア ファイルのテスト 完全な WildFire 構成をテストします。

STEP 11 | 分析結果を調査します。

- WildFireの分析結果を確認する:
  - ファイアウォールを使用してマルウェアを監視し、サンプルのWildFire分析レポートを表示します。
  - 高度な WildFireパブリック クラウドに手動で提出したサンプルを含め、WildFireパブリッククラウドに送信されたすべてのサンプルについて、高度な WildFireポータルでレポートを表示します。。.
  - 高度な WildFire API を使用して、WildFireアプライアンスからサンプルの判定とレポートを取得します。

STEP 12 | 次のステップ：

高度な WildFire のベストプラクティスを確認して実装します。

高度な WildFire 導入のベストプラクティス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

次のトピックでは展開と構成 Palo Alto Networks が推奨するWildFire® を使用しているハードウェアまたはサービスが正しいかどうかはわかりませんが に続く名詞を少なくとも1つ見つけることをお勧めします。

- 高度な WildFire のベストプラクティス

高度な WildFire のベストプラクティス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

*Prisma Access*ユーザー - ユーザー インターフェースに関する製品固有の情報については、Prisma Accessのドキュメントを参照してください。

- ベストプラクティスに従って、レイヤ4およびレイヤ7の回避策からネットワークを保護し、信頼できるコンテンツの識別と分析を確実にします。具体的には、TCP 設定 (デバイス > セットアップ > セッション > **TCP** 設定) とコンテンツ ID ™設定 (デバイス > セットアップ コンテンツ **ID** > コンテンツ **ID** 設定 > **)** のベストプラクティスを実装していることを確認します。
- また、アクティブな脅威防御サブスクリプションがあることを確認してください。高度な WildFire®と脅威防止により、包括的な脅威の検出と防止が可能になります。
- Palo Alto Networks によって生成された最新の製品アップデートと脅威の保護を受けるために、コンテンツのアップデートを日常的にDownload and install content updates（ダウンロードしてインストールしてください）。更新プログラム パッケージに含まれる内容の詳細については、コンテンツ更新プログラムとソフトウェア更新プログラムのインストール手順を参照してください。
- PAN-OS 10.0 以降を実行している場合は、 高度な WildFire シグネチャをリアルタイムで取得するようにファイアウォールを構成します。これにより、高度な WildFireパブリック クラウドが生成できるようになるとすぐに、新しく発見されたマルウェア シグネチャにアクセスできるようになり、悪意のあるアクティビティにさらされる時間を最小限に抑えて攻撃の成功を防ぎます。
- SSL トラフィックを復号化するようにファイアウォールを構成した場合は、ファイアウォールを Forward Decrypted SSL Traffic for WildFire Analysisに有効にします。このオプションを有効にできるのはスーパーユーザーのみです。
- デフォルトの WildFire分析プロファイルを使用して、ファイアウォールが分析のために転送するトラフィックを定義します (「オブジェクト > セキュリティ プロファイル > **WildFire** 分析」)。デフォルトのWildFire分析プロファイルにより、セキュリティポリシーが許可するすべてのトラフィックが完全にカバーされます。ファイルがアップロードされたかダウンロー

ドされたかにかかわらず、すべてのアプリケーションでサポートされているすべてのファイルタイプが高度なWildFire分析のために転送されるように指定しています。

カスタムのWildFire Analysisプロファイルを作成する場合は、プロファイルを設定を**any**（すべて）のファイルタイプを転送にすることをお勧めします。これにより、分析がサポートされるようになると、ファイアウォールはファイル タイプの転送を自動的に開始できるようになります。

WildFire分析プロファイルをファイアウォール トラフィックに適用する方法の詳細については、次の手順を参照してください。 高度な WildFire 分析のためのファイルの転送。

トラフィックがリセットまたはドロップ アクションを引き起こす高度な *WildFire* シグネチャを生成する場合、ウイルス対策プロファイルの *WildFire* アクション設定がトラフィックに影響を与える可能性があります。高度な*WildFire*は独自に作成されたプログラムを悪意のあるプログラムと判断し、それらに対するシグネチャを生成する可能性があるため、カスタムビルドプログラムをデプロイするソフトウェア配布アプリケーションなどの内部トラフィックを除外して、ベストプラクティスに安全に移行することができます。内部の独自に作成されたプログラムが *WildFire* シグネチャを引き起こすかどうかを調べるには、***Monitor***（モニター） > ***Logs***（ログ） > ***Advanced WildFire Submissions***（高度な***WildFire*** への送信）をチェックします。

- ファイアウォールを高度な WildFire 分析のためのファイルの転送に設定している間、サポートされているすべてのファイル タイプのファイル サイズ制限 を確認してください。すべてのファイルタイプの**Size Limit**（サイズ制限）をデフォルトの制限値のままにしておきます。（**Device (**デバイス**)** > **Setup (**セットアップ**)** > **WildFire**を選択し、一般設定を編集してファイルタイプに基づいてファイルサイズの制限を調整します。ヘルプ情報を表示して、各ファイルタイプのデフォルトのサイズ制限を見つけることができます)。

  WildFire転送のデフォルトのファイルサイズ制限について

  ファイアウォールのデフォルトのファイルサイズ制限は、大部分の市場に出回っているマルウェア（デフォルトのサイズ制限よりも小さい）に含めるように設計されており、悪意のある可能性は低く、WildFire転送容量に影響を与える可能性の低い大規模なファイルは除外されます。ファイアウォールには、高度な WildFire 分析用にファイルを転送するために予約された特定の容量があるため、多数の大きなファイルを転送すると、ファイアウォールが一部のファイルの転送をスキップする可能性があります。この状態は、ファイアウォールを高速で通過するファイルタイプの最大ファイルサイズ制限が設定されている場合に発生します。この場合、悪意のある可能性のあるファイルは高度な WildFire 分析のために転送されない可能性があります。デフォルトのサイズ制限を超えてPE以外のファイルのサイズ制限を増やしたい場合は、この条件を考慮してください。

  以下のグラフは、Palo Alto Networksの脅威研究チームが観測したマルウェアのファイルサイズの分布を表しています。ファイアウォールのデフォルトファイルサイズの設定を最大ファ

イルサイズの設定に増やすことで、各ファイルタイプのマルウェアキャッチレートを比較的小さくすることができます。

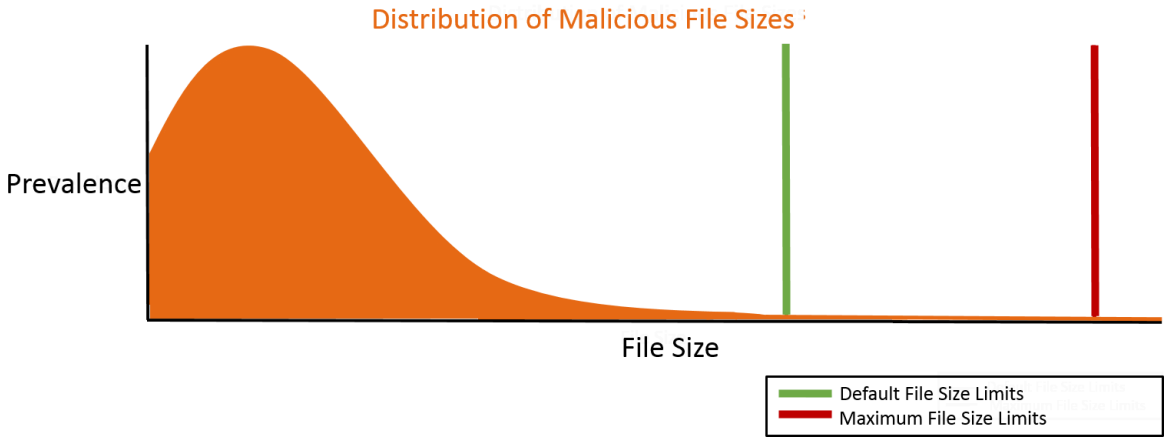


図 **1 :** 致命的な大きな悪意のあるファイルをキャッチする推奨ファイルサイズの制限

稀にみる大規模な悪意のあるファイルを特に心配している場合は、ファイルサイズの制限をデフォルトの設定を超えて増やすことをお勧めします。このような場合、次の設定を使用して、まれな非常に大きな悪質なファイルをキャッチすることをお勧めします。

（**Device (**デバイス**)** > **Setup (**セットアップ**)** > **WildFire**を選択し、一般設定を編集してファイルタイプに基づいて各ファイルの**Size Limit**（サイズ制限） を調整します:

ファイルタイプ	**PAN-OS 9.0** 以降ファイル転送最大サイズ推奨	**PAN-OS 8.1** ファイル転送最大サイズ推奨
pe	16MB	10MB
apk	10MB	10MB
pdf	3,072KB	1,000KB
ms-office	16,384KB	2,000KB
jar	5MB	5MB
Flash	5MB	5MB
MacOSX	10MB	1MB
アーカイブ	50MB	10MB
linux	50MB	10MB
/script	20KB	20KB

高度な WildFire 分析の構成

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

次のトピックでは、ネットワークデプロイメントでAdvanced WildFire™分析を有効にする方法について説明します。Palo Alto Networksファイアウォールは、未知のファイルを自動的に高度なWildFireパブリック クラウド もしくはWildFireプライベート クラウドへ転送するように設定したり、高度なWildFireポータルから手動で分析対象のファイルを送信したりすることができます。分析のために提出されたサンプルは、良性、グレイウェア、悪意のある、フィッシングの判定を受け、各サンプルについて詳細な分析レポートが生成されます。

- 高度な WildFire 分析のためのファイルの転送
- 高度な WildFire 分析のための復号化された SSL トラフィックの転送
- 高度な WildFire インライン ML を有効にする
- 高度なWildFireインライン クラウド解析を有効にする
- リアルタイムシグネチャ検索のホールド モードを有効にする
- WildFireへの送信を確認する
- WildFireポータルへファイルを手動でアップロードする
- モデルによるファイアウォールファイル転送能力

高度な WildFire 分析のためのファイルの転送

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

Palo Alto Networksファイアウォールを設定して、解析のために不明なファイルまたは電子メールリンクと、既存のアンチウィルスシグネチャと一致してブロックされたファイルを転送するようにします。**WildFire**分析プロファイルを使用して、高度な WildFireパブリック クラウドオプションのいずれかに転送するファイルを定義し、そのプロファイルをセキュリティルールにアタッチしてゼロデイマルウェアの検査をトリガーします。

使用中のアプリケーション、検出されたファイルタイプ、電子メールメッセージに含まれるリンク、または検体の送信方向（アップロード、ダウンロード、またはその両方）に基づいて、解析のために転送されるトラフィックを指定します。たとえば、ファイアウォールをセットアップして、 ユーザーがWebブラウズセッション中にダウンロードしようとするPortable Executables(ポータブル実行可能ファイル-PE）またはファイルを転送できます。未知の検体に加えて、ファイアウォールは既存のアンチウイルスシグネチャと一致するブロックされたファイルを転送します。これにより Palo Alto Networks は、シグネチャが防止に成功したものの、これまで確認されていないマルウェア亜種に基づく脅威インテリジェンスの貴重な情報源を得ることができます。

WildFireアプライアンスを使用してWildFireプライベートクラウドをホストしている場合は、ローカル解析用に機密ファイルを引き続きWildFireプライベートクラウドに転送するようにファイアウォールを構成することにより、WildFire解析リソースを WildFireハイブリッド クラウドに拡張できます。そして、機密性の低いファイルの種類やサポートされていないファイルの種類をWildFireパブリッククラウドに転送します。WildFireアプライアンスの使用と設定の詳細については、WildFire アプライアンスの管理を参照してください。

開始する前に：

- ファイル解析のサポートは、高度なWildFireクラウド リージョン間で多少の違いが生じる可能性があります。詳細については、ファイルタイプサポートを参照してください。

- ファイルを転送するように構成しているファイアウォールと高度な WildFire クラウドの間にファイアウォールが存在する場合は、中央のファイアウォールで次のポートが許可されていることを確認してください。

ポート	使用率
443	登録、PCAPダウンロード、サンプルダウンロード、レポート検索、ファイル送信、PDFレポートダウンロード
10443	ダイナミック更新

- Strata Cloud Manager
- PAN-OS & Panorama

高度なWildFire解析のためのファイルの転送(Cloud Management)

Panoramaを使用して***Prisma Access***を管理している場合**:**

[PAN-OS] タブに切り替えて、そこにあるガイダンスに従います。

Prisma Accessクラウド管理を使用している場合は、こちらに進んでください。

STEP 1 | サンプルの転送先となる高度な WildFireクラウドを指定します。

[Manage (管理)] > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Security Services (セキュリティ サービス)]** > **[WildFire and Antivirus (WildFireとアンチウイルス)]** > **[General Settings (一般設定)]**を選択し、WildFireクラウド展開(パブリック、政府、プライベート、またはハイブリッド)に基づいて一般設定を編集します。

*The WildFire U.S.Government Cloud (U.S.*政府専用クラウド*)* は連邦機関専用のオプションの解析環境です。

分析のためにサンプルを転送するクラウド環境の**WildFire**クラウド URL を追加します。

高度な **WildFire**パブリック クラウドオプション**:**

1. **WildFire**パブリック クラウド URL を入力します:
   - 米国: **`wildfire.paloaltonetworks.com`**
   - ヨーロッパ: **`eu.wildfire.paloaltonetworks.com`**
   - 日本: **`jp.wildfire.paloaltonetworks.com`**
   - シンガポール: **`sg.wildfire.paloaltonetworks.com`**
   - 英国: **`uk.wildfire.paloaltonetworks.com`**
   - カナダ: **`ca.wildfire.paloaltonetworks.com`**

- オーストラリア: **au.wildfire.paloaltonetworks.com**
- ドイツ:**de.wildfire.paloaltonetworks.com**
- インド: **in.wildfire.paloaltonetworks.com**
- スイス: **ch.wildfire.paloaltonetworks.com**
- ポーランド: **pl.wildfire.paloaltonetworks.com**
- インドネシア: **id.wildfire.paloaltonetworks.com**
- 台湾: **tw.wildfire.paloaltonetworks.com**
- フランス: **fr.wildfire.paloaltonetworks.com**
- カタール: **qatar.wildfire.paloaltonetworks.com**
- 韓国: **kr.wildfire.paloaltonetworks.com**
- イスラエル: **il.wildfire.paloaltonetworks.com**
- サウジアラビア: **sa.wildfire.paloaltonetworks.com**
- スペイン: **es.wildfire.paloaltonetworks.com**

2. **WildFire Private Cloud**（**WildFire**プライベートクラウド）フィールドがクリアされていることを確認してください。

WildFire FedRAMPクラウドのオプション**:**

1. **WildFire FedRAMP**クラウドのURLを入力します。
   - 米国政府専用クラウド: **wildfire.gov.paloaltonetworks.com**
   - 高度なWildFire政府専用クラウド: gov-cloud.wildfire.paloaltonetworks.com
   - 高度なWildFireパブリック セクター クラウド: pubsec-cloud.wildfire.paloaltonetworks.com
2. **WildFire Private Cloud**（**WildFire**プライベートクラウド）フィールドがクリアされていることを確認してください。

STEP 2 | **[Allow Forwarding of Decrypted Content (**復号化されたコンテンツの転送を許可する**)]**を選択して、高度なWildFire解析のために復号化されたSSLトラフィックを転送するようにPrisma Accessを有効にします。復号化れたトラフィックは、セキュリティ ポリシー ルールに対して評価されます。セキュリティ ルールにアタッチされている WildFire分析プロファイルと一致する場合、復号化されたトラフィックは、再暗号化される前に分析のために転送されます。

復号化された *SSL* トラフィックを分析のために転送することは、高度な *WildFire* のベストプラクティスです。

STEP 3 | Prisma Accessが解析のために転送する検体のサイズ制限を定義します。

これは、ファイル転送値をデフォルト設定に設定することが高度な WildFire のベストプラクティスです。

STEP 4 | 送信ログの設定を構成します。

1. **Report Benign Files**（安全なファイルのレポート）を選択して、安全であると判定を受けるファイルのロギングを許可します。
2. **Report Grayware Files**（レポートのグレイウェア ファイル）を選択して、グレイウェアであると判定を受けるファイルのロギングを許可します。

STEP 5 | 完了したら、変更を保存します。

STEP 6 | 分析のために転送するトラフィックを定義します。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Security Services (セキュリティ サービス)]** > **[WildFire and Antivirus (WildFireとアンチウイルス)]**を選択し、**[Add Profile (プロファイルを追加)]**を選択します。プロファイルのName（名前）とDescription（説明）を入力します。
2. 解析用に転送されるトラフィックを定義するためにルールを追加し、そのルールに名前を付けます（例：local-PDF-analysis）。
3. 不明なトラフィックと一致させ、以下の解析ベース用に検体を転送するために、プロファイルのルールを定義します。
   - トラフィックの方向:ファイルの送信方向(アップロード、ダウンロード、またはアップロードとダウンロード)に基づいて分析のためにファイルを転送します。例えば、アップロードとダウンロードを選択すると、送信方向に関係なく、すべての不明なPDFを分析用に転送することができます。
   - アプリケーション—使用中のアプリケーションを基準にした解析用にファイルを転送します。
   - ファイルの種類—電子メール内に含まれるリンクを含む、ファイルの種類を基準にした解析用にファイルを転送します。例えば、解析用ファイアウォールで検出された不明なPDFを転送するには、**PDF**を選択します。
   - Analysis（分析）で転送するトラフィックの宛先を選択します。
     - ルールと照合されるすべてのトラフィックを WildFireパブリック クラウドに転送して分析する場合は、**Public Cloud (パブリッククラウド)**を選択します。
     - ルールと照合されるすべてのトラフィックを WildFireアプライアンスに転送して分析する場合は、private-cloud を選択します。
     - 完了したら、WildFire 分析転送ルールを保存します。
4. WildFire およびアンチウイルス セキュリティ プロファイルを保存します。

STEP 7 | WildFire およびアンチウイルス セキュリティ プロファイルを有効にします。

セキュリティ ポリシー ルールによって許可されるトラフィックは、添付のWildFire分析プロファイルに対して評価されます。Prisma Accessは、WildFire解析用のプロファイルに一致するトラフィックを転送します。

STEP 8 | 構成の変更をプッシュします。

STEP 9 | （任意） 高度な WildFire インライン ML を有効にする

STEP 10 | 次の操作を選択します...

- WildFire 送信 を確認して、ファイアウォールが分析用のファイルを正常に転送していることを確認します。
- WildFireアクティビティを監視して、マルウェアについて報告されたアラートと詳細を評価します。

高度なWildFire解析のためのファイルの転送(PAN-OSおよびPanorama)

STEP 1 | (PA-7000シリーズ ファイアウォールのみ)PA-7000 シリーズ ファイアウォールで解析用のサンプルを転送できるようにするには、まず をログ カード インターフェース として NPC のデータ ポートを設定する必要があります。LFC(ログ転送カード)を装備したPA-7000シリーズアプライアンスを使用している場合は、LFC で使用されるポートをに設定する必要があります。設定すると、サンプルを転送する際に、ログ カード ポートまたは LFC インターフェースが管理ポートよりも優先されます。

STEP 2 | サンプルの転送先となる高度な WildFire の導入を指定します。

デバイス > セットアップ > **WildFire**を選択して、ご利用のWildFire cloud deployment （パブリック、政府、プライベートまたはハイブリッド）に基づき一般設定を編集します。

*The WildFire U.S.Government Cloud (U.S.*政府専用クラウド*)* は連邦機関専用のオプションの解析環境です。

高度な **WildFire**パブリック クラウド**:**

1. **WildFire**パブリック クラウド URL を入力します:
   - 米国: **wildfire.paloaltonetworks.com**
   - ヨーロッパ: **eu.wildfire.paloaltonetworks.com**
   - 日本: **jp.wildfire.paloaltonetworks.com**
   - シンガポール: **sg.wildfire.paloaltonetworks.com**
   - 英国: **uk.wildfire.paloaltonetworks.com**
   - カナダ: **ca.wildfire.paloaltonetworks.com**
   - オーストラリア: **au.wildfire.paloaltonetworks.com**
   - ドイツ:**de.wildfire.paloaltonetworks.com**
   - インド: **in.wildfire.paloaltonetworks.com**
   - スイス: **ch.wildfire.paloaltonetworks.com**
   - ポーランド: **pl.wildfire.paloaltonetworks.com**
   - インドネシア: **id.wildfire.paloaltonetworks.com**
   - 台湾: **tw.wildfire.paloaltonetworks.com**
   - フランス: **fr.wildfire.paloaltonetworks.com**
   - カタール: **qatar.wildfire.paloaltonetworks.com**
   - 韓国: **kr.wildfire.paloaltonetworks.com**
   - イスラエル: **il.wildfire.paloaltonetworks.com**
   - サウジアラビア: **sa.wildfire.paloaltonetworks.com**
   - スペイン: **es.wildfire.paloaltonetworks.com**
2. **WildFire Private Cloud**（**WildFire**プライベートクラウド）フィールドがクリアされていることを確認してください。

WildFire FedRAMPクラウドのオプション**:**

1. **WildFire FedRAMP**クラウドのURLを入力します。
   - 米国政府専用クラウド: **wildfire.gov.paloaltonetworks.com**
   - 高度なWildFire政府専用クラウド: gov-cloud.wildfire.paloaltonetworks.com

- 高度なWildFireパブリック セクター クラウド: pubsec-cloud.wildfire.paloaltonetworks.com

2. **WildFire Private Cloud**（**WildFire**プライベートクラウド）フィールドがクリアされていることを確認してください。

STEP 3 | ファイアウォールが転送するファイルのサイズ制限を定義し、ログとレポートの設定を構成します。

一般設定 (デバイス > セットアップ > **WildFire**) の編集を続けます。

- ファイアウォールから転送されるファイルの ファイル サイズ制限 を確認します。

  PE の ファイル サイズ を最大サイズ制限の *10 MB* に設定し、他のすべての ファイル タイプについては <ファイル サイズ> をデフォルト値に設定したままにすることは、高度な WildFire のベストプラクティスです。

- **Report Benign Files**（安全なファイルのレポート）を選択して、安全であると判定を受けるファイルのロギングを許可します。
- **Report Grayware Files**（レポートのグレイウェア ファイル）を選択して、グレイウェアであると判定を受けるファイルのロギングを許可します。
- セッション情報設定を編集して、WildFire分析レポートに記録するセッション情報を定義します。デフォルトでは、すべてのセッション情報がWildFire分析レポートに表示されます。チェックボックスをオフにして対応するフィールドをWildFire分析レポートから削除し、 **OK** をクリックして設定を保存します。

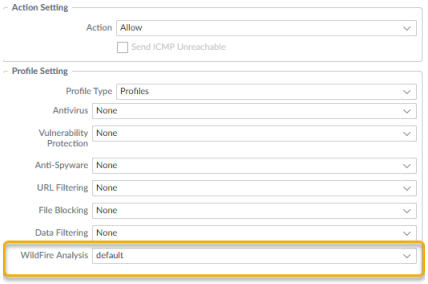
STEP 4 | 分析のために転送するトラフィックを定義します。

1. **Objects**（オブジェクト） > **Security Profiles**（セキュリティプロファイル） > **WildFire Analysis**（**WildFire**分析）を選択して、新しいWWildFire分析プロファイルを追加するとともに、そのプロファイルに説明用の名称を記入します。
2. 解析用に転送されるトラフィックを定義するためにプロファイルのルールを追加し、そのルールに名前を付けます（例：local-PDF-analysis）。
3. 不明なトラフィックと一致させ、以下の解析ベース用に検体を転送するために、プロファイルのルールを定義します。
   - アプリケーション—使用中のアプリケーションを基準にした解析用にファイルを転送します。
   - ファイルの種類—電子メール内に含まれるリンクを含む、ファイルの種類を基準にした解析用にファイルを転送します。例えば、解析用ファイアウォールで検出された不明なPDFを転送するには、**PDF**を選択します。
   - 方向—ファイルの送信方向（アップロード、ダウンロード、またはその両方）に基づいて解析のためにファイルを転送します。例えば、送信方向に関係なく、すべての不明なPDFを解析のために転送するには、両方を選択します。
4. **OK**をクリックすると、WildFire分析プロファイルを保存します。

STEP 5 | WildFire 分析プロファイルをセキュリティ ポリシー ルールにアタッチします。

セキュリティ ポリシー ルールによって許可されるトラフィックは、添付のWildFire分析プロファイルに対して評価されます。ファイアウォールは、WildFire分析用プロファイルに一致するトラフィックを転送します。

1. **[Policies]** > > **[**セキュリティ**]** の順に選択して、セキュリティ ポリシー ルールを **[**追加**]** または変更します。
2. セキュリティ ポリシー内の **[**アクション**]** タブをクリックします。
3. Profile Settings（プロファイル設定）セクションで、**Profiles**（プロファイル）を**Profile Type**（プロファイルの種類）として選択し、**WildFire Analysis**（**WildFire**分析）プロファイルを選択して、ポリシールールを添付します



STEP 6 | 高度な WildFire 分析のために、ファイアウォールが復号化された SSL トラフィックも転送できるようにしてください。

これは 推奨されるベストプラクティスです。

STEP 7 | （任意） 高度な WildFire インライン ML を有効にする

STEP 8 | （任意） リアルタイムシグネチャ検索のホールド モードを有効にする

STEP 9 | 高度な WildFire のベストプラクティスを確認して実装します。

STEP 10 | 「コミット」 をクリックして、更新された設定を適用します。

STEP 11 | (オプション)デバイス証明書をインストールして、 ファイアウォールがPalo Alto Networksのクラウド サービスと通信するために使用する証明書の最新バージョンに更新します。

STEP 12 | (オプション)コンテンツ クラウドのFQDN設定の構成。

STEP 13 | 次の操作を選択します...

- WildFire 送信 を確認して、ファイアウォールが分析用のファイルを正常に転送していることを確認します。
- WildFireアクティビティを監視して、マルウェアについて報告されたアラートと詳細を評価します。

WildFireポータルへファイルを手動でアップロードする

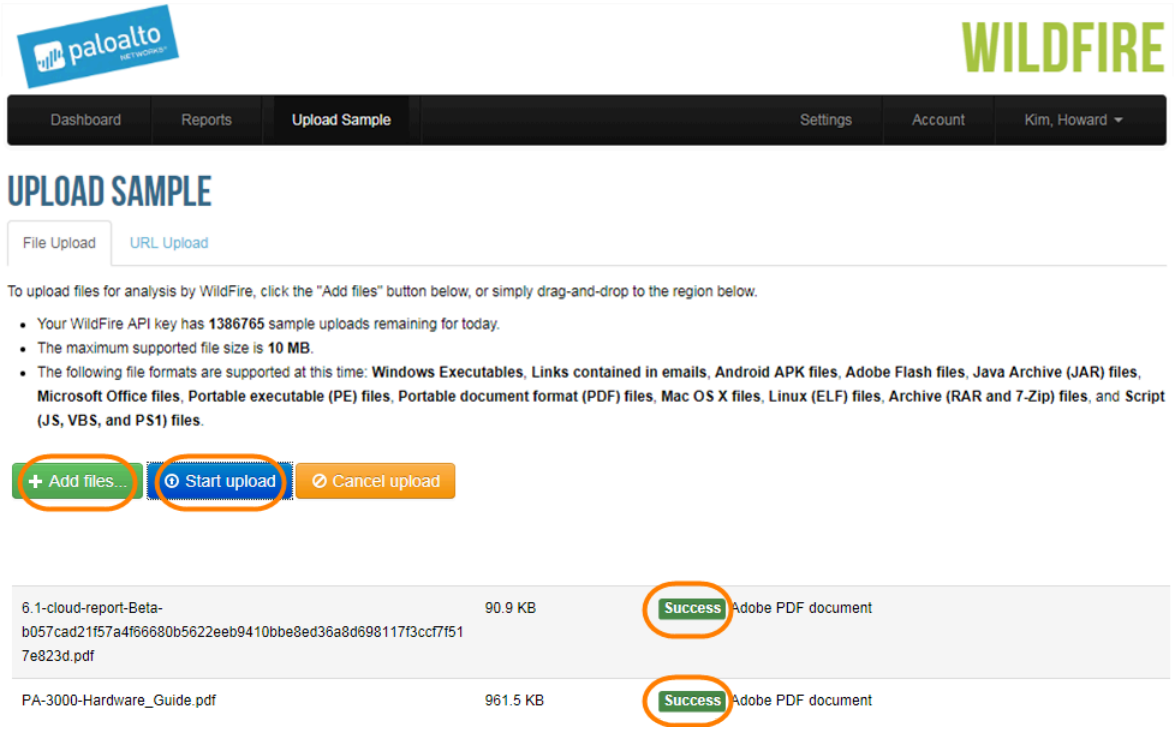
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

サポートアカウントを持っているPalo Alto NetworksのユーザーはPalo Alto Networks WildFire portal（WildFireポータル）を利用して、5つまでのサンプルを手動送信して分析することが可能です。高度な WildFire または WildFire サブスクリプションをお持ちの場合は、1 日あたり 1000 サンプルのアップロード制限の一部として、サンプルをポータルに手動で送信できます。ただし、1 日あたり 1000 サンプルの制限には、WildFire API の送信も含まれることに注意してください。

STEP 1 | WildFireポータルへ、ファイルやURLを手動でアップロードして分析します。

1. WildFire portal（WildFire ポータル）にログインします。
2. メニューバーの **Upload Sample**（サンプルをアップロード）ボタンをクリックします。
   - 分析のためにファイルを提出するには、**File Upload**（ファイルのアップロード）を選択し、分析のために提出するファイルを**Open**（開き）ます。**Start**（開始）をクリックして、単一ファイルの分析を開始するか、 **Start Upload**（アップロード開始）をクリックして分析のために追加したファイルをすべて送信します。

- 分析のためにURLを送信するには、**URL Upload**（**URL**アップロード）をクリックし、URLを入力して、分析のために**Submit**（送信）します。



3. **Uploaded File Information**（アップロード ファイル情報）ポップアップを閉じます。

STEP 2 | 判定を見て、ファイルの分析結果を確認します。

Advanced WildFire がサンプルを分析するまで、少なくとも 5 分間お待ちください。

手動アップロードは特定のファイアウォールに関連付けられていないため、手動アップロードはレポートのセッション情報を表示しません。

1. WildFire Portal（WildFireポータル）ダッシュボードに戻ります。
2. 前回の1時間セッションで、送信元列で**Manual**（手動）を選択して最新の手動送信されたサンプルの分析情報を見ます。
3. アップロード済みのファイルまたはURLを見つけ、受領時間の左にある詳細アイコンをクリックします。

高度な WildFire 分析のための復号化された SSL トラフィックの転送

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

高度な WildFire 分析のために、ファイアウォールが復号化された SSL トラフィックを転送できるようにします。ファイアウォールが復号化するトラフィックは、セキュリティ ポリシー ルールに照らして評価されます。セキュリティ ルールに添付された WildFire分析プロファイルと一致する場合、復号化されたトラフィックは、ファイアウォールが再暗号化する前に分析のために転送されます。スーパーユーザーだけがこのオプションを有効にすることができます。

分析のために復号化された *SSL* トラフィックを転送することは、高度な WildFire のベストプラクティスです。

複数の仮想システムが有効になっていないファイアウォールの場合：

1. まだ有効にしていない場合は、ファイアウォールで 復号化と高度な WildFire 分析のためのファイルの転送を実行できるようにします。 。
2. **Device (** デバイス**)** > **Setup (**設定**)** > **Content-ID**の順に選択します。
3. Content-ID設定を編集し、**Allow Forwarding of Decrypted Content**（復号化されたコンテンツの転送を許可） を有効にします。
4. **OK**をクリックして変更を保存します。

仮想システムが設定されたファイアウォールの場合：

1. まだ 復号化を有効にしていない場合は、復号化と高度な WildFire 分析のためのファイルの転送を有効にします。
2. この場合は、**Device (**デバイス**)** > **Virtual Systems (**仮想システム**)**の順に選択し、変更する仮想システムをクリックして、**Allow Forwarding of Decrypted Content**（復号化されたコンテンツの転送を許可）のボックスにチェックを入れます。

Prisma Accessの場合、これは**WildFire**およびアンチウイルスのセキュリティ プロファイル設定の一部として構成されます。詳細については、Prisma Accessの高度な WildFire 分析のためのファイルの転送を参照してください。

高度なWildFireインライン クラウド解析を有効にする

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

Palo Alto Networksの高度なWildFireは、ネットワークを通過するPE (Portable Executable)ファイルをインライン解析し、高度なマルウェアをリアルタイムで検出および防止する一連のクラウドベースのML検出エンジンを運用しています。WildFireが検出する他の悪意のあるコンテンツと同様に、高度なWildFireインライン クラウド解析が検出した脅威はシグネチャを生成し、アップデート パッケージを通じて顧客に拡散されるため、Palo Alto Networksのすべての顧客に将来的な防御策を提供します。

クラウドベースのエンジンにより、これまでに見たことのないマルウェア(Palo Alto Networksのゼロデイマルウェアなど、これまでに報告されたことがないマルウェアやPalo Alto Networksでは検出されなかったマルウェア)の検出を可能にし、環境への侵入をブロックします。高度なWildFireインライン クラウド解析は、ファイアウォールで軽量転送メカニズムを使用して、パフォーマンスへの影響を最小限に抑えます。クラウドベースのMLモデルはシームレスに更新されるため、コンテンツ更新や機能リリースのサポートを必要とせず、常に変化する脅威のランドスケープに対処できます。

高度なWildFireインライン クラウド解析は、WildFire分析プロファイルを通じて有効化および構成され、有効な高度なWildFireライセンスを持つPAN-OS 11.1以降が必要です。

STEP 1 | 高度なWildFireクラウド解析サービスへの認証に使用される更新されたファイアウォール デバイス証明書をインストールします。インラインクラウド解析が有効なすべてのファイアウォールについて繰り返します。

ファイアウォールに現在のバージョンのデバイス証明書をすでにインストールしている場合は、この手順は必要ありません。

STEP 2 | PAN-OS Web インターフェイスにログインします。

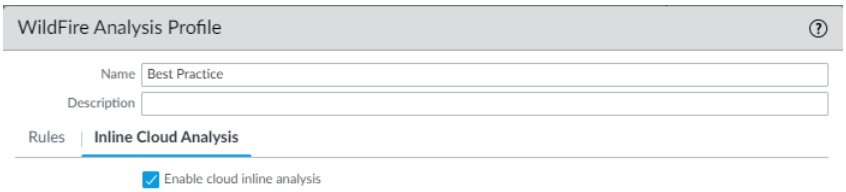
STEP 3 | 高度なWildFireインライン クラウド解析を有効にするには、有効な高度なWildFireサブスクリプションが必要です。詳細については、以下を参照してください:ライセンス、登録、およびアクティベーション。

現在アクティブなライセンスがあるサブスクリプションを確認するには、**[Device (デバイス)] > [Licenses (ライセンス)]**を選択し、適切なライセンスが使用可能で有効期限が切れていないことを確認します。

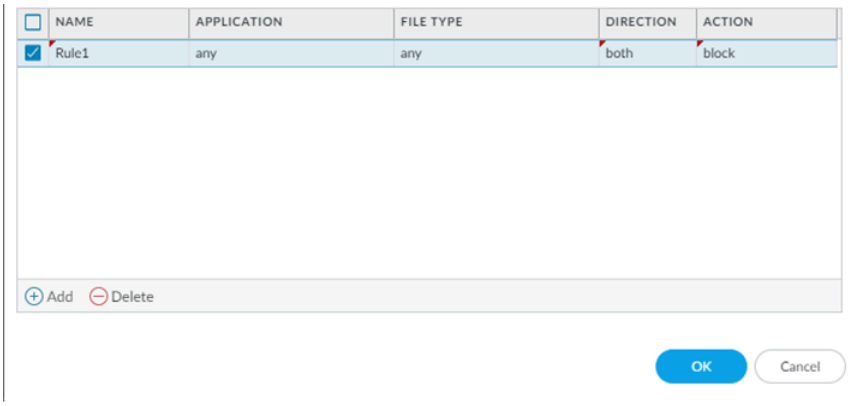
現在の*WildFire*ライセンスの有効期限が切れ、高度な*WildFire*ライセンスをインストールする場合は、高度な*WildFire*ライセンスをインストールする前にまず*NGFW*から*WildFire*ライセンスを削除する必要があります。

STEP 4 | 高度なWildFireインライン クラウド解析を有効にするには、WildFire解析セキュリティ プロファイルを更新または新規作成します。

1. 既存の**WildFire**分析プロファイルを選択するか、新しいプロファイルを追加します(**[Objects (オブジェクト)]** > **[Security Profiles (セキュリティプロファイル)]** > **[WildFire Analysis (WildFire解析)]**)。
2. WildFire分析プロファイルを選択し、**[Inline Cloud Analysis (インライン クラウド解析)]**と**[Enable cloud inline analysis (クラウドインライン解析を有効にする)]**に移動します。



3. 高度なWildFireインライン クラウド解析が高度なマルウェアを検出したときに実行するアクションを定義するルールを指定します。



- Name (名前): プロファイルに追加するルールの分かりやすい名前を入力します(最大31文字)。
- Application (アプリケーション):インライン クラウドMLアクションを定義するルールが適用されるアプリケーション トラフィックを追加します。
- File Type (ファイル タイプ): ルールに定義された解析先で分析するファイル タイプを選択します。

  現時点では、*PE (Portable Executable)*のみがサポートされています。

- Direction (方向): 送信の方向に応じてトラフィックにルールを適用します。ルールはダウンロード トラフィックに適用できます。
- Action (アクション): 高度なWildFireインライン クラウド解析を使用して脅威が検出されたときに実行するアクションを設定します。アプリケーション トラフィックを宛先

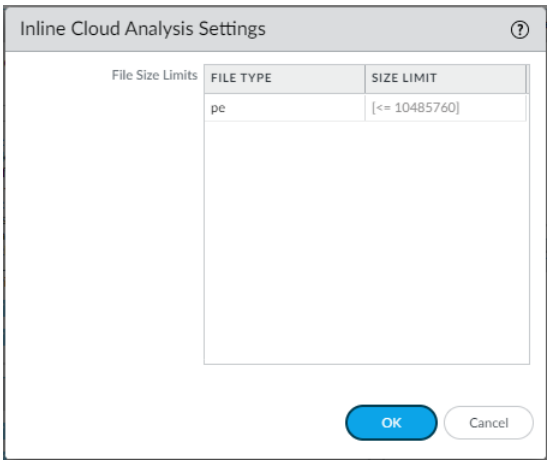
まで継続することを許可することも、送信元または送信元-宛先のどちらかからのトラフィックをブロックすることもできます。

*Palo Alto Networks*では、最適なセキュリティを確保するために、ブロックするようにアクションを設定することをお勧めします。

4. **[OK]**をクリックして、WildFire分析プロファイル設定ダイアログを終了します。

STEP 5 | 高度なWildFireインライン クラウド解析を使用して、解析のために転送できる最大ファイル サイズを確認します。

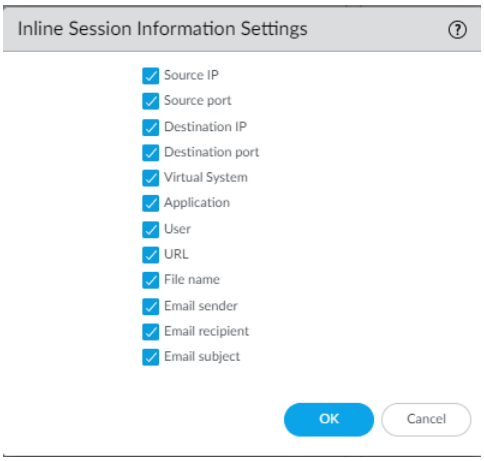
高度な*WildFire*インライン クラウド解析は、迅速な*WildFire*判定を提供します。ただし、悪意のある検体の完全なレポートは、検体が完全に動的解析を受けた後にのみ利用可能であり、これには最大*30*分かかります。



1. **[Device (デバイス)]** > **[Setup (セットアップ)]** > **[WildFire]** > **[Inline Cloud Analysis Settings (インライン クラウド分析設定)]**を選択し、ファイル サイズの制限を確認します。
2. **OK** をクリックして変更を確定します。

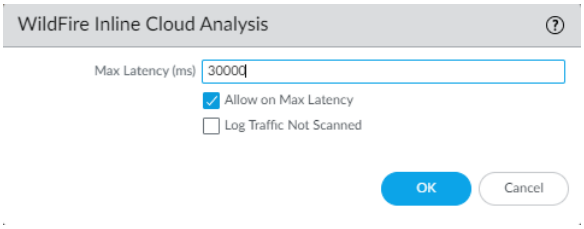
STEP 6 | 特定の検体についてファイアウォールが転送するネットワーク セッション情報を指定します。Palo Alto Networksは、セッション情報を使用して、疑わしいネットワークイベントのコンテキスト、マルウェアに関連する脆弱性の指標、影響を受けるホストとクライアント、

マルウェアの配信に使用されるアプリケーションについて学びます。これらのオプションはデフォルトで有効になっています。



1. **[Device (デバイス)]** > **[Setup (セットアップ)]** > **[WildFire]** > **[Inline Session Information Settings (インライン セッション情報設定)]**を選択し、必要に応じてオプションをオンまたはオフにします。
   - **Source IP**（送信元 **IP**） — 未知のファイルを送信した送信元IPアドレスを転送します。
   - **Source Port**（送信元ポート）— 未知のファイルを送信した送信元ポートを転送します。
   - **Destination IP**（宛先**IP**）—未知のファイルの宛先IPアドレスを転送します。
   - **Destination Port**（宛先ポート）—未知のファイルの宛先ポートを転送します。
   - **Virtual System**（仮想システム）—未知のファイルを検出した仮想システムを転送します。
   - **Application**（アプリケーション）—未知のファイルを送信したユーザーアプリケーションを転送します。
   - **User**（ユーザー）—ターゲットユーザーを転送します。
   - **URL**—未知のファイルに関連付けられたURLを転送します。
   - **Filename**（ファイル名）—未知のファイルの名前を転送します。
   - **Email sender**（電子メール送信者 ）—不明な電子メールリンクの送信者を転送します（電子メール送信者の名前はWildFireのログとレポートにも表示されます）。
   - **Email recipient**（メール受信者）—未知の電子メールリンクの受信者を転送します（電子メール受信者の名前はWildFireのログとレポートにも表示されます）。
   - **Email subject**（電子メールの件名）—未知の電子メールリンクの件名を転送します（電子メールの件名はWildFireのログとレポートにも表示されます）。
2. **OK** をクリックして変更を確定します。

STEP 7 | タイムアウト遅延と、要求が最大遅延を超えた場合に実行するアクションを設定します。



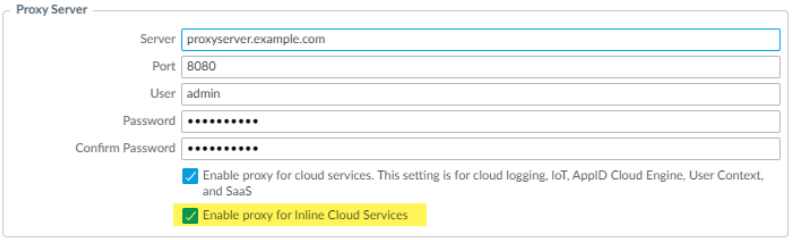
1. 高度なWildFireインライン クラウド解析リクエストで遅延制限に達したときに実行するアクションを指定します。
   - Max Latency (ms) (最大遅延時間(ミリ秒)): 高度なWildFireインライン クラウド解析が結果を返すまでの最大許容処理時間を秒単位で指定します。
   - Allow on Max Latency (最大遅延時に許可): 最大遅延に達したときに、ファイアウォールが許可のアクションを実行できるようにします。このオプションの選択を解除すると、ファイアウォール アクションがブロックに設定されます。
   - Log Traffic Not Scanned (スキャンされていないトラフィックをログに記録): ファイアウォールが、高度なマルウェアの存在を示すが、高度なWildFireクラウドによって処理されていない高度なWildFireインライン クラウド解析要求をログに記録できるようにします。
2. **OK** をクリックして変更を確定します。

STEP 8 | (ファイアウォールが明示的なプロキシ サーバーを使用してデプロイされている場合に必要)設定されたすべてのインライン クラウド解析機能によって生成される要求を促進するサーバーへのアクセスに使用するプロキシ サーバーを構成します。単一のプロキシ サーバーを指定することができ、構成済みのすべてのインライン クラウドおよびロギング サービスを含む、すべてのPalo Alto Networksの更新サービスに適用されます。

1. (PAN-OS 11.2.3以降）PAN-OSを介してプロキシ サーバーを構成します。
   1. **[Device (デバイス)]** > **[Setup (セットアップ)]** > **[Services (サービス)]**の順に選択し、**[Services (サービス)]**の詳細を編集します。
   2. **[Proxy Server (プロキシ サーバー)]**設定を指定し、**[Enable proxy for Inline Cloud Services (インライン クラウド サービスのプロキシを有効にする)]**を選択しま

す。**[Server (サーバー)]**フィールドにIPアドレスまたはFQDNのいずれかを指定できます。

プロキシ サーバーのパスワードには、6文字以上を含める必要があります。



3. **OK** をクリックします。

2. (PAN-OS 11.1.5以降)ファイアウォールCLIを使用してプロキシ サーバーを構成します。
   1. ファイアウォール CLI にアクセスします。
   2. 次のCLIコマンドを使用して、基本プロキシ サーバーの設定を行います。

```
set deviceconfig system secure-proxy-server <FQDN_or_IP>
 set deviceconfig system secure-proxy-port <1-65535>
 set deviceconfig system secure-proxy-user <value> set
 deviceconfig system secure-proxy-password <value>
```

   プロキシ サーバーのパスワードには、6文字以上を含める必要があります。

   3. 次のCLIコマンドを使用して、プロキシ サーバーがインライン クラウド サービス サーバーに要求を送信できるようにします。

```
debug dataplane mica set inline-cloud-proxy enable
```

   4. 次のCLIコマンドを使用して、インライン クラウド サービスのプロキシ サポートの現在の動作ステータスを表示します。

```
debug dataplane mica show inline-cloud-proxy
```

   以下に例を示します。

```
debug dataplane mica show inline-cloud-proxy Proxy for
 Advanced Services is Disabled
```

STEP 9 | (推奨)悪意のあるアクティビティが検出されたため、ファイアウォールが元のセッションを終了した後、クライアントがファイルの一部をフェッチし、その後新しいセッションを開始して残りのファイルをフェッチできないようにファイアウォールを構成します。

これは、Webブラウザが[HTTP Range (HTTPの範囲)]オプションを実装している場合に発生します。**[Allow HTTP partial response (HTTP部分レスポンスを許可する)]**を有効にすると最大限の可用性が得られますが、サイバー攻撃が成功するリスクも高くなります。Palo Alto Networksでは、セキュリティを最大限に高めるために**[Allow HTTP partial response (HTTP部分レスポンスを許可する)]**を無効にすることを推奨しています。

[Allow HTTP partial response (HTTP部分レスポンスを許可する)]はグローバル設定で、*RANGE*ヘッダーを使用する*HTTP*ベースのデータ転送に影響し、特定のアプリケーションでサービス異常が発生する可能性があります。***[Allow HTTP partial response (HTTP部分レスポンスを許可する)]***を無効にした後、ビジネス クリティカルなアプリケーションの動作を検証します。

1. **[Device (デバイス)]** > **[Setup (セットアップ)]** > **[Content-ID (コンテンツID)]** > **[Content-ID Settings (コンテンツID設定)]**を選択します。
2. **[Allow HTTP partial response (HTTP部分レスポンスを許可する)]**を選択解除し、**[OK]**をクリックします。

STEP 10 | 変更を **Commit (コミット)** します。

STEP 11 | (オプション)コンテンツ クラウドのFQDN設定の構成。

高度な WildFire インライン ML を有効にする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

ファイアウォールのデータプレーン上で機械学習（ML）ベースの分析を使用して、悪意のあるポータブル実行可能ファイルやPowerShellスクリプトの変種がネットワークに侵入するのをリアルタイムで防ぐことができます。お使いのセキュリティプラットフォーム上で WildFire® クラウド解析技術を利用することにより、高度なWildFire インライン ML は、ファイルの高確率分類を定式化するためのデコーダ フィールドとパターンを含むファイルの詳細を評価することにより、特定のタイプの悪意のあるファイルを動的に検出します。この保護により、現在不明であるだけでなく、Palo Alto Networks が悪性であると識別した特性に一致する脅威の将来の亜種にも拡張されます。高度な WildFire インライン ML は、既存のアンチウイルスプロファイル保護設定を補完します。さらに、ファイルハッシュの例外を指定して、発生するあらゆる誤検知を除外することができ、これにより、特定のセキュリティニーズをサポートするために、より詳細なルールをプロファイルに作成することができます。

高度なWildFireインラインMLを有効にするには、アクティブな高度なWildFireまたはWildFireサブスクリプションが必要です。また、アンチウイルス(またはPrisma Access用のWildFireおよびアンチウイルス)セキュリティ プロファイルを作成(または変更)してサービスを構成および有効にし、そのアンチウイルス プロファイルをセキュリティ ポリシー ルールにアタッチします。

高度な *WildFire Inline ML* は現在、*VM-50* または *VM50L* バーチャル アプライアンスではサポートされていません。

- Strata Cloud Manager
- PAN-OS & Panorama

高度なWildFireインラインMLを有効にする(PAN-OSおよびPanorama))

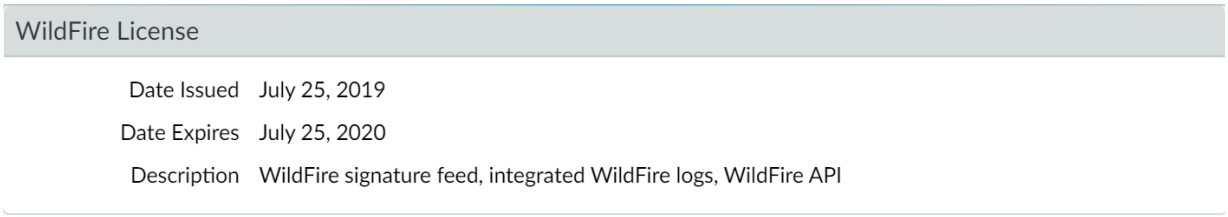
WildFire インライン ML 設定を有効にするには、インライン ML 設定で設定されたアンチウイルス プロファイルをセキュリティ ポリシー ルールに添付します。

高度なWildFireインラインMLをバイパスするには、**[Action Setting (アクション設定)]**をモデルごとに無効(全プロトコル)に設定するか、部分ハッシュを使用してWildFireインラインMLファイル例外を作成する必要があります。WildFireインラインML脅威IDに基づくシグネチャ例外でアンチウイルス プロファイルを構成しないでください。設定すると、ファイアウォールはネットワークからIPアドレスへのすべてのトラフィックをブロックします。

WildFire インライン *ML* は現在、*VM-50* または *VM50L* バーチャル アプライアンスでサポートされていません。

STEP 1 | WildFire インライン ML を利用するには、Windows 実行可能ファイルを分析するためのアクティブな WildFireサブスクリプションがなければなりません。

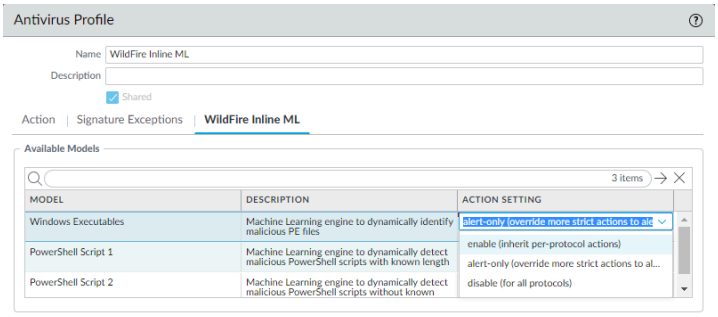
WildFireサブスクリプションがあることを確認します。現在ライセンスを持っているサブスクリプションを確認するには、**Device**（デバイス）> **Licenses(ライセンス)** を選択し、適切なライセンスが表示され、有効期限が切れていないことを確認します。



STEP 2 | リアルタイム WildFire インライン ML モデルを使用するには、アンチウイルス セキュリティ プロファイルを新規作成するか、既存のものを更新します。

1. 既存の **Antivirus Profile (アンチウイルス プロファイル)** を選択するか、アンチウイルス プロファイルを新規作成し (**Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > Antivirus (アンチウイルス)**を選択し、新規プロファイルを**Add (追加)** します。
2. アンチウイルス プロファイルを設定します。
3. **WildFire Inline ML (WildFire インライン ML)** タブを選択し、各 WildFire インライン ML モデルの **Action Setting (アクション設定)** を適用します。この操作は、モデルベースごとの各プロトコル用に設定された WildFire インライン ML アクション設定を施行します。次の分類エンジンが使用可能です。
   - Windows実行可能ファイル
   - PowerShell スクリプト 1
   - PowerShell スクリプト 2
   - Executable Linked Format (PAN-OS コンテンツ リリース 8367 以降のインストールで利用可能)
   - MSOffice (PAN-OS コンテンツ リリース 8434 以降のインストールで利用可能)
   - Shell Scripts (PAN-OS コンテンツリリース 8543 以降のインストールで利用可能)

- OOXML (PAN-OS 11.1.3以降およびPAN-OSコンテンツ リリース8825以降のインストールで利用可能)
- Mach-O (PAN-OS 11.1.3以降およびPAN-OSコンテンツ リリース8885-8930以降のインストールで利用可能)



以下のアクション設定が可能です。

- 有効にする(プロトコルごとのアクションを継承する) —WildFire は、**Action** (アクション) タブのデコーダ セクションの WildFire インライン ML アクション列内の選択内容に従ってトラフィックを検査します。
- アラートのみ (より厳密なアクションをアラートにオーバーライドします)—WildFire は、**Action** (アクション) タブのデコーダセクションの WildFire インライン ML アクション列内の選択内容に従ってトラフィックを検査し、アラート (ドロップ、クライアントのリセット、サーバーのリセット、両方のリセット) アラートよりも高い重大度のアクションを上書きします。これにより、アラートを生成して脅威ログに保存しながら、トラフィックを通過させることができます。
- 無効化(すべてのプロトコル用) —WildFire は、ポリシー アクションなしでトラフィックを通過させます。

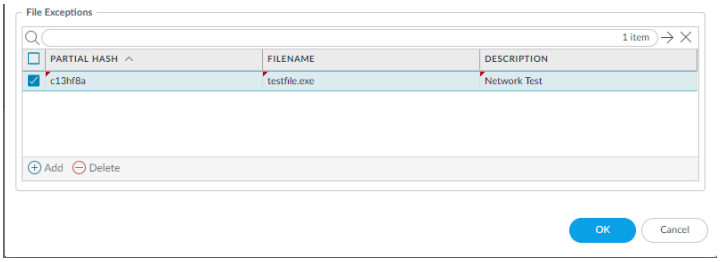
4. **OK** をクリックして、アンチウイルス プロファイル設定ウィンドウを終了し、新しい設定を **Commit** (コミット) します。

STEP 3 | (オプション) 誤検知が発生した場合は、アンチウイルス セキュリティ プロファイルにファイル例外を追加します。これは通常、分析のために WildFire にファイルを転送していない

ユーザーに対して行われます。ファイルの例外の詳細を例外リストに直接追加するか、脅威ログからファイルを指定することができます。

WildFire のインライン *ML* を使用して分析されたファイルタイプを転送するように *WildFire* 分析セキュリティ プロファイルが設定されている場合、誤検知は受信時に自動的に修正されます。*WildFire*分析によって良性に分類されたファイルに対する*ml*-ウイルスアラートが引き続き表示される場合は、*Palo Alto Networks*のサポートにお問い合わせください。

- ファイルの例外を例外リストに直接追加します。
  1. 「**Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Antivirus(アンチウイルス)**」を選択します。
  2. 特定のファイルを除外したい アンチウイルス プロファイルを選択してから、 **WildFire Inline ML (WildFire** インライン **ML)** を選択します。
  3. 施行から除外するファイルのハッシュ、ファイル名、および説明を追加します。



  4. **OK** をクリックしてアンチウイルス プロファイルを保存し、更新を **Commit (コミット)** します。
- 脅威ログ エントリからファイル例外を追加します。
  1. **Monitor (モニター) > Logs (ログ) > Threat (脅威)** を選択し、**ml-virus** 脅威タイプのログをフィルタリングします。ファイル例外を作成するファイルの脅威ログを選択します。
  2. **Detailed Log View (詳細ログ ビュー)** に移動し、**Details (詳細)** ペインにスクロールダウンしてから、**Create Exception (例外を作成)** を選択します。

  3. ファイル例外を追加するには、**Description (説明)** を追加して **OK** をクリックします。
  4. 新しいファイル例外は、**Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Antivirus(アンチウイルス) > WildFire Inline ML(WildFire** インライン **ML)** の **File Exceptions (ファイル例外)** リストにあります。

STEP 4 | (オプション) ご利用のファイアウォールの、インライン ML クラウド サービスへの接続ステータスを確認します。

接続ステータスを表示するには、ファイアウォール上で次のCLIコマンドを実行します。

```
show mlav cloud-status
```

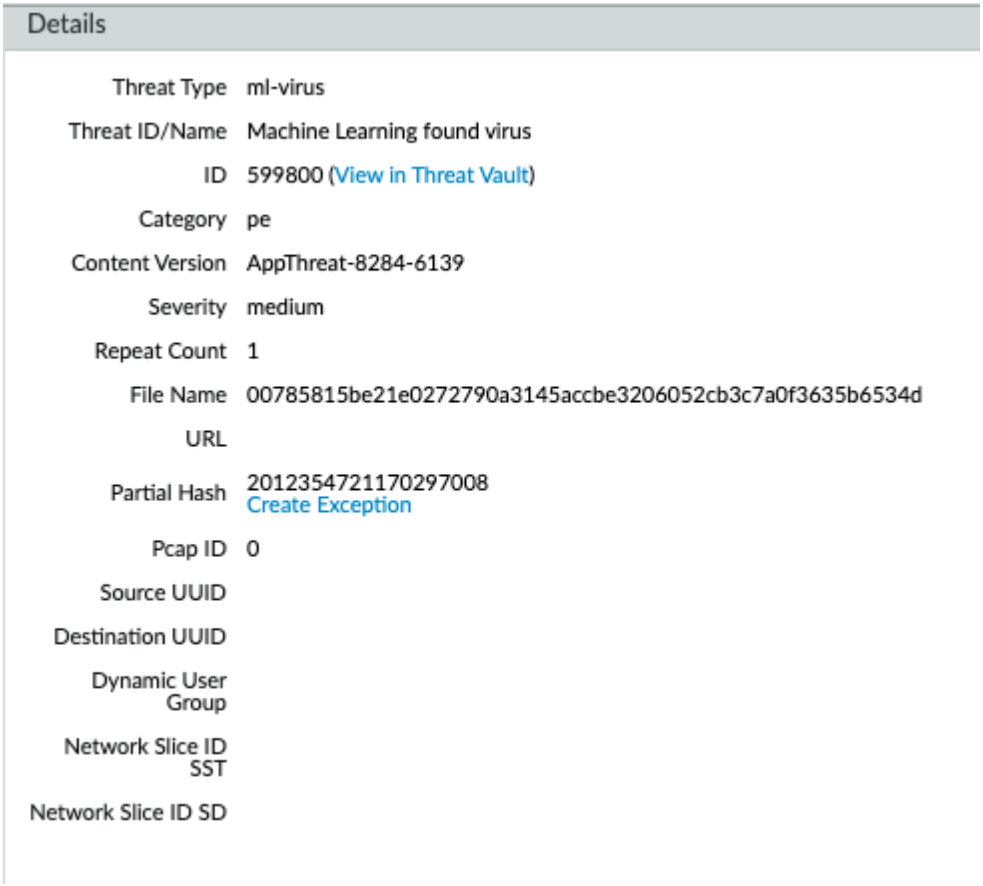
以下に例を示します。

```
show mlav cloud-status MLAV cloud Current cloud server:
 ml.service.paloaltonetworks.com Cloud connection: connected
```

インライン ML クラウド サービスに接続できない場合は、以下のドメインがブロックされていないことを確認してください: ml.service.paloaltonetworks.com.

STEP 5 | (オプション)コンテンツ クラウドのFQDN設定の構成。

WildFire インライン ML を使用して検出されたファイルに関する情報を見るには、脅威ログを確認します (**Monitor (モニター) > Logs (ログ) > Threat (脅威)** を選択し、リストからログ タイプを選択します)。WildFire インライン ML を使用して分析されたファイルには、脅威の種類 **ml-virus** というラベルが付けられます:



高度なWildFireインラインMLを有効にする(Cloud Management)

***Panorama*を使用して*Prisma Access*を管理している場合:**

[PAN-OS] タブに切り替えて、そこにあるガイダンスに従います。

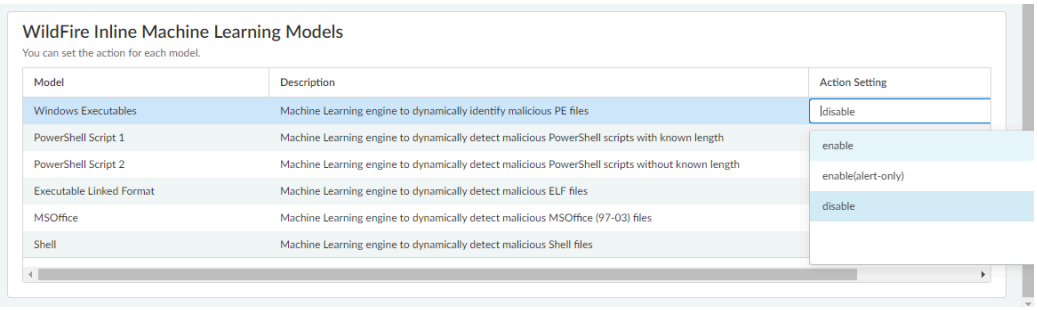
***Prisma Access*クラウド管理を使用している場合は、こちらに進んでください。**

STEP 1 | WildFireインラインMLを利用するには、Prisma Accessサブスクリプションの一部としてアクティブなWildFireサブスクリプションが必要です。

有効で期限切れになっていない WildFireサブスクリプションがあることを確認してください。

STEP 2 | リアルタイム WildFire インライン ML モデルを使用するには、**WildFire** とアンチウイルス セキュリティ プロファイルを新規作成するか、既存のものを更新します。

1. 既存の**WildFire**およびアンチウイルス セキュリティ プロファイルを選択するか、新しいセキュリティ プロファイルを作成します(**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Security Services (セキュリティ サービス)]** > **[WildFire and Antivirus (WildFireとアンチウイルス)]**を選択して、**[Add Profile (プロファイルを追加)]**を選択します。
2. 分析のためにサンプルを転送するように WildFire およびアンチウイルス プロファイル を設定します。
3. **WildFire** インライン機械学習モデル を選択し、各 WildFire インライン ML モデルに アクション設定を適用します。この操作は、モデルベースごとの各プロトコル用に設定された WildFire インライン ML アクション設定を施行します。



次の分類エンジンが使用可能です。

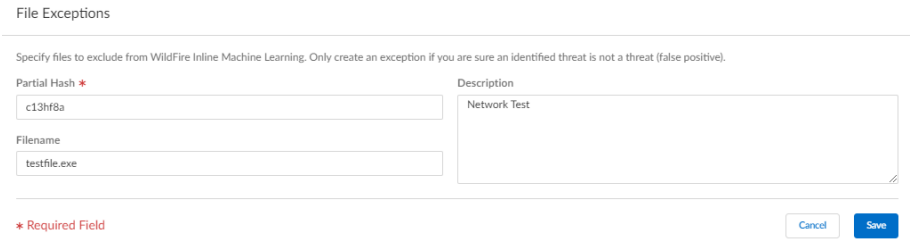
- Windows実行可能ファイル
- PowerShell スクリプト 1
- PowerShell スクリプト 2
- 実行可能リンク形式
- MSオフィス
- シェルスクリプト

- 有効にする—WildFire は、**Action (アクション)** タブのデコーダ セクションの WildFire インライン ML アクション列内の選択内容に従ってトラフィックを検査します。
- 有効にする **(アラートのみ)**—WildFire は、**Action (アクション)** タブのデコーダセクションの WildFire インライン ML アクション列内の選択内容に従ってトラフィックを検査し、アラート (ドロップ、クライアントのリセット、サーバーのリセット、両方のリセット) アラートよりも高い重大度のアクションをオーバーライドします。これにより、アラートを生成して脅威ログに保存しながら、トラフィックを通過させることができます。
- 無効化 —WildFire は、ポリシー アクションなしでトラフィックを通過させます。

STEP 3 | (オプション) 誤検知が発生した場合は、 WildFireとアンチウイルス セキュリティ プロファイルにファイル例外を追加します。これは通常、分析のために WildFire にファイルを転送していないユーザーに対して行われます。ファイルの例外の詳細を例外リストに直接追加するか、脅威ログからファイルを指定することができます。

WildFire のインライン *ML* を使用して分析されたファイルタイプを転送するように *WildFire* 分析セキュリティ プロファイルが設定されている場合、誤検知は受信時に自動的に修正されます。*WildFire*分析によって良性に分類されたファイルに対する*ml*-ウイルスアラートが引き続き表示される場合は、*Palo Alto Networks*のサポートにお問い合わせください。

- ファイルの例外を例外リストに直接追加します。
  1. **[詳細設定]** を選択し、**[ファイル例外]** ペインで **[例外を追加]** を選択します 。
  2. 施行から除外するファイルのハッシュ、ファイル名、および説明を追加します。



  3. 完了したら、ファイルの例外を保存します。

STEP 4 | WildFire および アンチウイルスのプロファイル設定を保存し、 構成の変更をプッシュします。

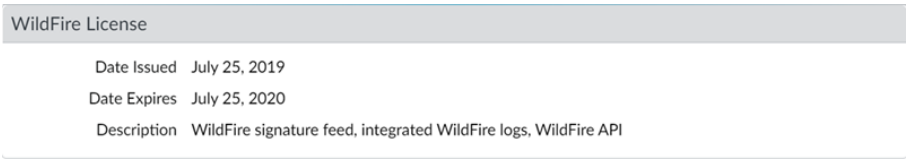
リアルタイムシグネチャ検索のホールド モードを有効にする

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

リアルタイム シグネチャ クラウドがシグネチャ検索を実行している間、検索の転送を保留するようにNGFWを構成できます。検索が完了すると、特定の WildFire 判定に対する組織のセキュリティ ポリシーに基づいて、ファイルが要求元のクライアントにリリース (またはブロック) され、既知のマルウェアの最初の転送が防止されます。アンチウイルス プロファイルごとにホールド モードを構成し、シグネチャ検索タイムアウトと関連アクションのグローバル設定を適用できます。

この機能は、PAN-OS 11.0.2以降を実行しているアクティブなWildFireまたは高度なWildFireライセンスを持つすべてのユーザーが利用できます。

STEP 1 | WildFire リアルタイムシグネチャルックアップのホールド モードを有効にするには、WildFire または高度な WildFireサブスクリプション サービス ライセンスが必要です。ファイアウォールで ライセンスをまだアクティブ化 していない場合は、必ずアクティブ化してください。現在アクティブなライセンスを持っているサブスクリプションを確認するには、 **Device**（デバイス）> **Licenses(**ライセンス**)**を選択し、適切なライセンスが表示され、有効期限が切れていないことを確認します。以下の例は、標準の WildFire ライセンスの説明を示しています。



STEP 2 | ファイアウォールがWildFireシグネチャをリアルタイムで取得するためのスケジュールを設定します。

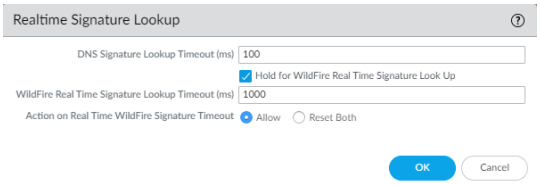
ファイアウォールがリアルタイム シグネチャを使用するように構成されている場合でも、補足シグネチャ パッケージは定期的にインストールされます。これにより、接続の問題が発生

した場合に最新のシグネチャ ソースが提供され、シグネチャがローカルで利用できる場合は速度上の利点も得られます。

1. **[Device (デバイス)]** > **[Dynamic Updates (動的更新)]**を選択します。
2. WildFire更新のスケジュールを選択します。
3. リアルタイム更新の繰り返し(ファイアウォールがパロアルトネットワークスの更新サーバで新しいシグネチャをチェックする頻度)を設定します。
4. **[OK]**をクリックしてWildFire更新スケジュールを保存し、変更をコミットします。

STEP 3 | タイムアウト設定とリクエストがタイムアウトを超えた場合のアクションを構成します。

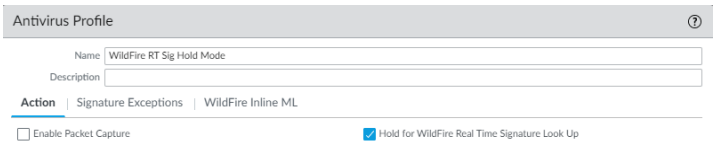
WildFire リアルタイム シグネチャ検索の保留モードをアンチウイルス プロファイルごとに有効にする前に、保留モードをグローバルに有効にする必要があります。



1. **Device Setup (デバイスセットアップ)** > **ContentID (コンテントID)** > **Realtime Signature Lookup (リアルタイムシグネチャ検索)**を選択します
2. **WildFire**のリアルタイムシグネチャ検索を有効化します。
3. **WildFire** リアルタイムシグネチャ検索 タイムアウト **(ミリ秒)** を ミリ秒単位で指定します (デフォルト値は 1000)。

   Palo Alto Networks では、テスト中にタイムアウトが繰り返されない限り、デフォルト値の *1000* ミリ秒を使用することを推奨しています。
4. リアルタイム **WildFire** シグネチャ タイムアウト時のアクションを指定します。デフォルト値は **[Allow (許可)]**ですが、Palo Alto Networksでは、ホールド モードが有効な場合はこれを **[Reset- Both]** に設定することをお勧めします。オプションには次のものが含まれます。
   - Allow (許可) - NGFWは、ホールド タイムアウトしきい値に達したときにパケットの通過を許可します。
   - Reset Both (両方をリセット) - ホールド タイムアウトしきい値に達すると、NGFWはクライアント側とサーバー側の両方で接続をリセットします。
5. 完了したら、「**OK**」 を選択します。

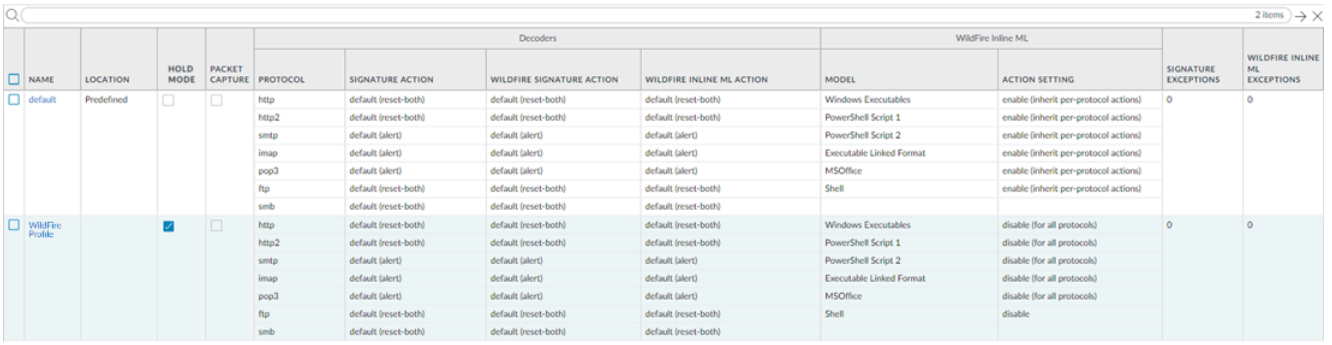
STEP 4 | 新しいアンチウイルス セキュリティ プロファイルを更新または作成して、WildFire リアルタイム シグネチャ検索のホールド モードを有効にします。



1. 既存のアンチウイルスセキュリティ プロファイルを選択するか、新しいセキュリティ プロファイル を追加します (**[オブジェクト]** > **[セキュリティ プロファイル]** > **[ウイルス対策]**)。
2. アンチウイルス セキュリティ プロファイルを選択し、**[アクション]**に進みます。
3. **[WildFire** リアルタイムシグネチャの検索**]** で **[保留]**を選択します。
4. WildFireリアルタイム シグネチャ検索のホールド モードを有効にするすべてのアクティブなアンチウイルス プロファイルに対して手順4.1～4.3を繰り返します。

STEP 5 | 変更を **Commit (**コミット**)** します。

STEP 6 | (オプション) ウイルス対策の概要表示ページで、アンチウイルス セキュリティ プロファイル設定の概要 (ホールド モードの有効化など) を表示できます。



	NAME	LOCATION	HOLD MODE	PACKET CAPTURE	Decoders				WildFire Inline ML		SIGNATURE EXCEPTIONS	WILDFIRE INLINE ML EXCEPTIONS
					PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	MODEL	ACTION SETTING		
☐	default	Predefined	☐	☐	http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	enable (inherit per-protocol actions)	0	0
					http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	enable (inherit per-protocol actions)		
					smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	enable (inherit per-protocol actions)		
					imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	enable (inherit per-protocol actions)		
					pop3	default (alert)	default (alert)	default (alert)	MSOffice	enable (inherit per-protocol actions)		
					ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	enable (inherit per-protocol actions)		
					smb	default (reset-both)	default (reset-both)	default (reset-both)				
☐	WildFire Profile		☑	☐	http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	disable (for all protocols)	0	0
					http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	disable (for all protocols)		
					smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	disable (for all protocols)		
					imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	disable (for all protocols)		
					pop3	default (alert)	default (alert)	default (alert)	MSOffice	disable (for all protocols)		
					ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	disable		
					smb	default (reset-both)	default (reset-both)	default (reset-both)				

コンテンツ クラウドのFQDN設定の構成

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

高度なWildFireサービス リクエストを処理するためにNGFWが使用するクラウド コンテンツの完全修飾ドメイン名(FQDN)を指定できます。既定の FQDN は hawkeye.services-edge.paloaltonetworks.com に接続し、最も近い cloud サービス サーバーに解決されます。自動サーバー選択をオーバーライドするには、データの常駐性とパフォーマンスの要件に最も適した地域の cloud コンテンツサーバーを指定します。クラウド コンテンツのFQDNはグローバルに使用されるリソースであり、この接続に依存する他のサービスがトラフィック ペイロードを送信する方法に影響することに注意してください。

場合によっては、クラウド コンテンツの*FQDN*が、特定の地域の特定の*Palo Alto Networks*製品の機能を完全にサポートしていないことがあります。クラウド コンテンツの*FQDN*を変更する前に、製品が完全にサポートされていることを確認してください。

使用するサービスに応じて、クラウド コンテンツのFQDNは、トラフィック ペイロードを含む解析サービス リクエストを容易にし、選択したリージョンのサーバーにデータを送信します。お住まいの地域外にあるコンテンツ クラウドのFQDNを指定した場合(たとえば、EUリージョンにいるが、APACリージョンのFQDNを指定した場合)、所属する組織のプライバシーおよび法的規制に違反する可能性があります。Palo Alto Networks製品でクラウド コンテンツのFQDNがどのように使用されるかについては、特定の製品ドキュメントを参照してください。

サービス接続の問題が発生している場合は、構成したクラウド コンテンツの*FQDN*がブロックされていないことを確認します。

STEP 1 | PAN-OS Web インターフェイスにログインします。

STEP 2 | **[Device (デバイス)] > [Setup (セットアップ)] > [Content-ID (コンテンツID)] > [Content Cloud Settings (コンテンツ クラウド設定)]**を選択し、必要に応じてFQDNを変更します。

- デフォルト: **hawkeye.services-edge.paloaltonetworks.com**
- 米国中部(米国アイオワ州): **us.hawkeye.services-edge.paloaltonetworks.com**
- ヨーロッパ(ドイツ、フランクフルト): **eu.hawkeye.services-edge.paloaltonetworks.com**
- アジア太平洋(シンガポール): **apac.hawkeye.services-edge.paloaltonetworks.com**
- インド(ムンバイ): **in.hawkeye.services-edge.paloaltonetworks.com**
- 英国(イギリス、ロンドン）: **uk.hawkeye.services-edge.paloaltonetworks.com**
- フランス(フランス、パリ）: **fr.hawkeye.services-edge.paloaltonetworks.com**
- 日本(東京）: **jp.hawkeye.services-edge.paloaltonetworks.com**
- オーストラリア(オーストラリア、シドニー）: **au.hawkeye.services-edge.paloaltonetworks.com**
- カナダ(カナダ、モントリオール）: **ca.hawkeye.services-edge.paloaltonetworks.com**
- スイス: **ch.hawkeye.services-edge.paloaltonetworks.com**
- オランダ: **nl.hawkeye.services-edge.paloaltonetworks.com**
- インドネシア: **id.hawkeye.services-edge.paloaltonetworks.com**
- カタール: **qa.hawkeye.services-edge.paloaltonetworks.com**
- 台湾: **tw.hawkeye.services-edge.paloaltonetworks.com**
- ポーランド: **pl.hawkeye.services-edge.paloaltonetworks.com**
- 韓国(韓国、ソウル): **kr.hawkeye.services-edge.paloaltonetworks.com**
- サウジアラビア: **sa.hawkeye.services-edge.paloaltonetworks.com**
- イタリア: **it.hawkeye.services-edge.paloaltonetworks.com**

STEP 3 | **OK** をクリックします。

サンプル送信の検証

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

マルウェア テスト サンプルを使用して展開をテストし、ファイアウォールが WildFire 分析用にファイルを正しく転送していることも確認します。

- サンプル マルウェア ファイルのテスト
- ファイルの転送を確認する

サンプル マルウェア ファイルのテスト

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な WildFire もしくは Wildfire ライセンス

Palo Alto Networksは、高度な WildFire設定のテストに使用できるサンプル マルウェア ファイルを提供しています。次の手順を実行してマルウェア サンプル ファイルをダウンロードし、そのファイルが高度な WildFire 分析用に転送されていることを確認し、分析結果を表示します。

STEP 1 | マルウェアのテストファイルのいずれかをダウンロードしてください。PE、APK、MacOSX、ELFの中から選択できます。

暗号化された*WildFire*サンプルマルウェアファイルをダウンロードする前に、***Device***（デバイス）> ***Certificate Management***（証明書の管理）> ***SSL Decryption Exclusion***（***SSL***復号化例外）ページの復号化リストの例外から**.wildfire.paloaltonetworks.com*エントリを一時的に無効にする必要があります。無効にしないと、正しくダウンロードされません。検証テストの実施後に、必ず該当の*SSL*復号化例外ページで **.wildfire.paloaltonetworks.com* エントリを再度有効にしてください。

- ファイアウォールで SSL 復号化を有効にしている場合は、次のいずれかの URL を使用します：
  - PE—https://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK—https://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX—https://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF—wildfire.paloaltonetworks.com/publicapi/test/elf
- ファイアウォールで SSL 復号化を有効にしていない場合は、代わりに次のいずれかの URL を使用します：
  - PE—http://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK—http://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX—http://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF—wildfire.paloaltonetworks.com/publicapi/test/elf

テストファイルの名前は wildfire-test-*file_type*-file.exe で、それぞれのテストファイルは固有の SHA-256 ハッシュ値を持っています。

マルウェア テスト ファイルを取得するため*WildFire API*も使用できます。詳細は、WildFire API Referenceを参照してください。

STEP 2 | ファイアウォールのウェブインターフェイス上で、**Monitor (監視)** > **WildFire Submissions (WildFire**への送信**)** の順に選択し、WildFireにファイルが転送されたことを確認してください。

ファイルの分析結果が**WildFire Submissions**（**WildFire**への送信）ページに表示されるまで、少なくとも5分お待ちください。テストファイルの判定結果は必ずマルウェアと表示されます。

ファイルの転送を確認する

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な WildFire もしくは Wildfire ライセンス

ファイアウォールが高度な WildFire 分析のためのファイルの転送に設定されたら、次のオプションを使用してファイアウォールとWildFireパブリックまたはプライベートクラウド間の接続を確認し、ファイル転送を監視します。

ファイアウォールが分析用のサンプルを転送しているかどうかを確認する方法はいくつかあり、*CLI*コマンドを使う場合もあります。*CLI*コマンドの使い方と詳細についてはPAN-OS CLI Quick Start Guide（PAN-OS CLI クイックスタートガイド）を参照してください。

分析のためにファイアウォールから転送されたファイルの総数を含め、Advanced WildFireパブリッククラウドおよび/またはWildFireプライベートクラウドへのファイアウォール接続のステータスを確認します。

`show wildfire status`（**`WildFire`**ステータス表示）コマンドを実行して以下の作業を行います。

- ファイアウォールが接続されている高度な WildFire パブリッククラウド、または WildFire プライベートクラウドのステータスを確認します。ステータスが`Idle`（アイドリング）になっている場合、高度なWildFireクラウド（パブリックまたはプライベート）は分析用ファイルを受信できる状態にあります。
- 設定されたファイルサイズ上限を確認します（**Device (**デバイス**)** > **Setup (**セットアップ**)** > **WildFire** の順に選択）。
- 分析のためにファイアウォールによって転送されたファイルの総数など、ファイル転送を監視します。ファイアウォールがWildFireハイブリッド クラウドの導入環境内に設置され

ている場合、WildFireパブリック クラウドとWildFireプライベート クラウドに転送されたファイル数も表示されます。

以下はWildFireプライベートクラウド導入環境下における`show wildfire status`（`WildFire`ステータス表示）コマンドの出力例です。

```
admin@VM-FW> show wildfire status

Connection info:
  Signature verification:            enable
  Server selection:                  enable
  File cache:                        enable
WildFire Public Cloud:
  Server address:                    wildfire.paloaltonetworks.com
  Status:                            Disabled due to configuration
  Best server:
  Device registered:                 no
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
WildFire Private Cloud:
  Server address:                    X.X.X.X
  Status:                            Idle
  Best server:                       X.X.X.X:XXXXX
  Device registered:                 yes
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
File size limit info:
  pe                                  9 MB
  apk                                 49 MB
  pdf                                 1000 KB
  ms-office                           9500 KB
  jar                                 9 MB
  flash                               10 MB
  MacOSX                              1 MB
Forwarding info:
  file idle time out (second):       90
  total concurrent files:            0
  Public Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
  Private Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
```

高度な WildFire パブリッククラウドまたは WildFire プライベートクラウドのみの転送情報を表示するには、次のコマンドを使用します。

- **`show wildfire status channel public`**
- **`show wildfire status channel private`**

電子メールリンクを含め、転送されたサンプルをファイル形式でソートして閲覧する。

このオプションを使用すると、良質およびグレイウェアサンプルのロギングが有効になっていても、ファイアウォールに***WildFire Submissions***（***WildFire*** 送信）のエントリとして悪質またはフィッシングの判定を受け取った電子メールリンクのみが記録されるため、分析の電子メールリンクが転送されていることを確認できます。*WildFire*への送信エントリには、安全な電子メールリンクのログが非常に多く記録されるからです。

`show wildfire statistics` コマンドを使用して、高度な WildFire パブリッククラウドまたは WildFire プライベートクラウドに転送されるファイルタイプを確認します。

- このコマンドは、動作中のファイアウォールの出力を表示し、ファイアウォールが分析のために転送する各ファイルタイプのカウンタを表示します。カウント数が0の場合、ファイアウォールはそのファイルタイプを転送していません。
- 以下のカウンタ表示が0ではないことを確認し、電子メールリンクがWildFireに転送されていることを確かめてください。
- `FWD_CNT_APPENDED_BATCH` —高度な WildFire パブリッククラウドまたは WildFire プライベートクラウドへのアップロードを待っているバッチに追加された電子メールリンクの数を示します。
- `FWD_CNT_LOCAL_FILE` — 高度な WildFireパブリッククラウドまたはWildFireプライベートクラウドにアップロードされたメールリンクの総数を示します。

特定のサンプルがファイアウォールから転送されていることを確認し、そのサンプルのステータスを確認します。

このオプションは以下のようなトラブルシューティングを行う際に役立ちます。

- まだ判定を受けていないサンプルがファイアウォールによって正しく転送されたことを確認します。**WildFire Submissions** がファイアウォールに記録されるのは、分析が完了し、

サンプルが判定を受けた場合のみであるため、このオプションを使用して、現在分析中のサンプルをファイアウォールが転送したことを確認します。

- セキュリティー ポリシーにより許可され、WildFire分析プロファイルにと照合され、分析に転送された特定のファイルまたは電子メールリンクのステータス履歴を追跡することができます。
- Hybrid Cloud（ハイブリッドクラウド）デプロイメントのファイアウォールが、適切なファイルタイプとメールリンクをWildFireパブリッククラウドまたは高度な WildFireプライベート クラウドのいずれかに転送していることを確認します。

ファイアウォールで次の CLI コマンドを実行して、ファイアウォールが分析用に転送したサンプルを表示します。

- CLIコマンド**debug wildfire upload-log**を使用して、ファイアウォールによって転送されたすべてのサンプルを表示します
- CLI コマンド **debug wildfire upload-log channel public** を使用して、高度なWildFireパブリック クラウドに転送されたサンプルのみを表示します。
- ファイアウォールがWildFireプライベートクラウドへ転送したサンプルのみを参照する場合はCLIコマンド**debug wildfire upload-log channel private**[デバッグWildFireアップロードログチャンネルプライベート]を実行します。

次の例は、高度な WildFireパブリッククラウド環境のファイアウォール上で実行した上記の 3 つのコマンドの出力を示しています。

```
user@firewall> debug wildfire upload-log
+ channel   WildFire channel (Public/Private)
  |         Pipe through a command
  <Enter>   Finish input

user@firewall> debug wildfire upload-log channel private

Private Cloud upload logs:


user@firewall> debug wildfire upload-log channel public

Public Cloud upload logs:

    log: 0, filename: support-login.swf
    processed 353590 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 169651, transaction_id: 261
    file_len:  91536, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 1238, app_id: 872
    from XX.XX.XX.XX/XXXX to XX.XXX.XXX.XXX/XXX
    SHA256: 6b2f1a23407ab2db9a17ccdf686bacc6dad7d2489c65ba90dbdf02508b3d4efd

    log: 1, filename: G2M_D_because_12.03.2014_300x250.swf
    processed 611505 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 259049, transaction_id: 260
    file_len:  39206, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 20583, app_id: 872
    from XX.XX.XX.XX/XXXXX to XXX.XX.XXX.XXX/XX
    SHA256: cd52d1b7a7521a14237c1531edb109627fee084806a300d907b57322b1efd6e7
```

モニターサンプルは分析用に正常に送信されました。

ファイアウォールのウェブインターフェースから、**Monitor (**監視**)** > **Logs (**ログ**)** > **WildFire Submissions (WildFire**への送信**)**の順に選択します。ファイアウォールによって Advanced

WildFire パブリッククラウドまたは WildFire プライベートクラウドに分析のために転送されたすべてのファイルは、WildFire Submissions ページに記録されます。

- 判定でサンプルを確認してください:

  デフォルトでは、malicious判定またはphishing判定を受けたサンプルのみが **WildFire Submission** エントリとして表示されます。benignおよび/またはgraywareサンプルのロギングを有効にするには、**Device** > **Setup** > **WildFire** > **Report Benign Files/ Report Grayware Files**.

  firewall がファイルを転送していることを確認するための簡単なトラブルシューティング手順として、*benign*ファイルのロギングを有効にします。***WildFire***送信 ログを調べて、ファイルが分析のために送信され、*WildFire* の判定 *(*この場合は*benign*判定*)* を受けていることを確認します。

- サンプルの分析場所を確認します。

  WildFireクラウド 列には、ファイルの転送先の場所と分析された場所が表示されます。これは、ハイブリットクラウド を展開する場合に便利です。

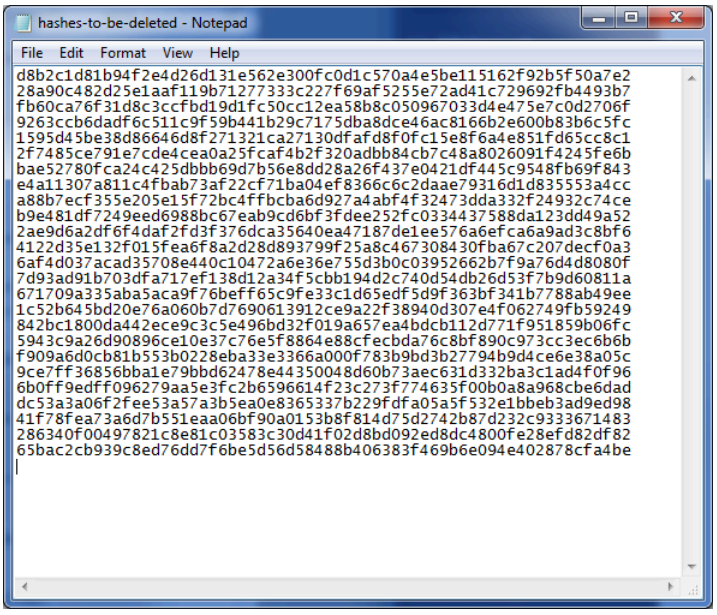
削除リクエストのサンプル

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

分析のために高度な WildFire クラウドに送信された固有のサンプルは、ユーザーの裁量で削除できます。これにより、GDPR を遵守しなければならないユーザーなどのデータ保護ポリシーの対象となるユーザーが、組織のデータ保存ポリシーに基づいてサンプルを永久に破棄できます。サンプル データには、セッション/アップロード日およびサンプル ファイル自体が含まれています。

STEP 1 | 削除するサンプルの SHA256 あるいは MD5 ハッシュのリストを持つテキストファイルを作成します。ファイル内のハッシュは 1 行ずつに分けます。また、最大 100 件のサンプルを含められます。

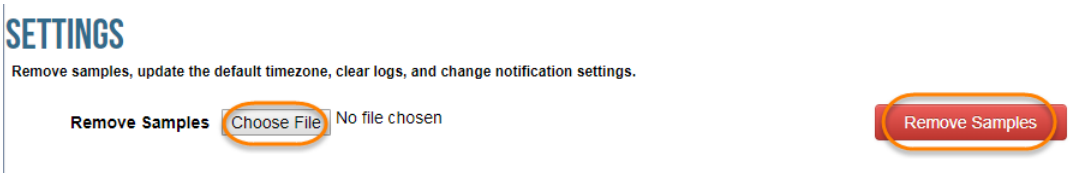
削除できるのは、ユーザーの環境に固有のファイルだけです。他のパブリックあるいはプライベートなフィードで当該ファイルを利用できることが分かった場合、対象のアカウントのセッションおよびアップロード日だけが削除されます。



STEP 2 | Palo Alto Networks サポート資格情報または WildFire アカウントを使用して、WildFire ポータルにログインします。

STEP 3 | メニューバーの**Settings**（設定）を選択します。

STEP 4 | **Choose File (**ファイルの選択**)**をクリックし、ステップ 1 で作成したハッシュ リストのテキストファイルを選択してから**Remove Samples (**サンプルを削除**)**します。ファイルが正常にアップロードされたら通知を受け取ります。



STEP 5 | サンプルが WildFire クラウドから削除されたら、リクエストの詳細が記載された確認用メールを受信します。これには、削除をリクエストしたサンプルのリスト、および各サンプルの削除ステータスが含まれています。このプロセスは最大 7 日間かかる場合があります。

```
Dear WildFire customer,
your request for removal of samples from WildFire cloud has been completed. In total 1 samples were removed from WildFire,
the following table shows removal status for each individual sample hash

+------------------------------------------------------------------+--------+-------------------+
| Hash                                                             | Status |      Information  |
+------------------------------------------------------------------+--------+-------------------+
|6d2ef9f79b5b81429cb1ffeebd6b2919a9a84ec0cc0e5023cbf45a68967c6e1c | Deleted ||                  |
+------------------------------------------------------------------+--------+-------------------+
```

存在しないサンプル、あるいはユーザーの環境に固有なものではないサンプルに対しては、それぞれ***Not found (***見つかりません**)**および***Rejected (***拒否**)**のステータスが返されます。

Firewall ファイル転送容量 (モデル別)

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series	❑ 高度な Wildfire ライセンス

ファイル転送容量は、各 Palo Alto Networks ファイアウォール モデルが分析のために高度な WildFire クラウドにファイルを送信できる 1 分あたりの最大レートです。ファイアウォールが1分毎の上限に達した場合、残りのサンプルはキューに追加されます。

次の表の [予約済みドライブ領域] は、ファイルのキューイング用に予約されているファイアウォール上のドライブ領域の量を表します。ファイアウォールのドライブスペースが上限に達した場合、キューに空きができるまで、ファイアウォールは WildFireに向けた新しいファイルの転送をキャンセルします。

ファイアウォールが *Advanced WildFire* クラウドにファイルを転送できる速度は、ファイアウォールからのアップロード リンクの帯域幅にも依存します。

プラットフォーム	1 分あたりの最大ファイル数	予約済みドライブ領域
VM-50	5	100MB
VM-100	10	100MB
VM-200	15日	200MB
VM-300	25	200MB
VM-500	30	250MB
VM-700	40	250MB
PA-220	20	100MB
PA-400	20	100MB
PA-820	75	300MB
PA-850	75	300MB
PA-1400 シリーズ	20	100MB

プラットフォーム	1 分あたりの最大ファイル数	予約済みドライブ領域
PA-3220	100	200MB
PA-3250/3260	100	500MB
PA-3400シリーズ	100	500MB
PA-5200 シリーズ	250	1500MB
PA-5400シリーズ	250	1500MB
PA-7000シリーズ	300	1GB

アクティビティの監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

WildFire portal（WildFireポータル）を使用してWildFireに提出されたサンプルと各サンプルの分析結果を表示することができます。また、サンプルを送信したファイアウォールにアクセスすることもできます（複数を集中管理する場合はPanorama） ファイアウォール）、またはusing the WildFire API（WildFire APIを使用）します。

WildFireがサンプルを分析し、悪意のある、フィッシング、グレーウェア、または良性の判定を行った後、詳細な分析レポートがサンプル用に生成されます。サンプルを送信したファイアウォールから閲覧できるWildFire分析レポートには、サンプルが検出された際のセッションに関する詳細情報も含まれています。新たにマルウェアと判定されたサンプルについては、関連が疑われる既存のWildFireシグネチャ情報や、サンプルがマルウェアであることを示すファイル特性、挙動、アクティビティに関する情報もWildFire分析レポートに記載されています。

また、高度なWildFireがPalo Alto Networksの他のアプリケーションやセキュリティ サービスとどのように統合され、脅威から組織を保護するかを確認できるほか、Strata Cloud Managerコマンド センターを通じて、デプロイメント環境の運用の全体的な健全性を大まかに把握できます。コマンド センターはNetSecのホームページとして機能し、ネットワークの健全性、セキュリティ、および効率性の包括的なサマリーを、複数のデータ ファセットを備えたインタラクティブなビジュアル ダッシュボードで提供します。これにより、一目で簡単に評価できます。

製品プラットフォームに応じて、解析情報などの形でネットワーク アクティビティのコンテキストを含む、高度なWildFireマルウェア検出の統計情報と使用傾向を提供する高レベルのダッシュボードにアクセスできます。

Palo Alto Networksは、高度なWildFireアクティビティを監視するためのいくつかの方法を提供しています。

- Strata Cloud Managerコマンド センター
- 高度なWildFireダッシュボード
- WildFireログとレポートについて

- WildFire 送信ログ設定の構成
- WildFireポータルを使用したマルウェアの監視
- WildFire分析レポート－詳細
- マルウェア検出時のアラートを設定する

WildFireログとレポートについて

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

ファイアウォール上で、WildFireポータルを使用して、Strata Cloud Manager、またはWildFire APIを使用してアクティビティの監視できます。

WildFireは分析する各サンプルを安全、マルウェア、フィッシング、グレイウェアに分類し、そのサンプルの詳細と挙動を記載したWildFire分析レポートを生成します。WildFire分析レポートは、WildFire APIを使用してサンプルを送信したファイアウォールと、そのサンプルを分析したWildFireクラウド（パブリックもしくはプライベート）から確認することができます。

- ファイアウォール上- WildFire解析のためにファイアウォールによって送信されたすべての検体は、WildFire送信エントリとして記録されます。WildFire SubmissionsログのAction［挙動］列には、ファイルがファイアウォールによって許可されたかブロックされたかが示されます。それぞれのWildFireへの送信エントリにつき、詳細ログビューを展開し、そのサンプルのWildFire分析レポートを閲覧したり、レポートをPDF形式でダウンロードしたりすることができます。
- WildFireポータル上で - 各サンプルのWildFire分析レポートを含めたWildFireアクティビティを監視することができます。また、レポートをPDF形式でダウンロードすることもできます。WildFireプライベートクラウドの導入環境では、ポータルへ手動でアップロードされたサンプル、およびクラウドインテリジェンスが有効化されたWildFire アプライアンスから送信されたサンプルの詳細をWildFireポータルから閲覧することができます。

  *WildFire*分析レポートをポータル上で見るオプションは、クラウドインテリジェンス 機能が有効化された*WildFire* アプライアンス のみに対応しています。

- Strata Cloud Manager上 — Prisma AccessによってWildFire解析用に提出されたすべての検体は、WildFireログとして記録され、Strata Cloud Managerログ ビューアで確認できます。トラフィックの詳細、コンテキスト、その他の関連詳細、検体がネットワーク内でどのように進行したかに関する情報などを表示できます。
- WildFire APIでは：WildFire アプライアンスまたはWildFireパブリッククラウドからのWildFire分析レポートを取得します。

高度なWildFire分析レポート—詳細

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

ファイアウォール、WildFireポータル、WildFire APIの高度な WildFire分析レポートにアクセスできます。

高度な WildFire分析レポートには、詳細なサンプル情報のほか、対象ユーザーに関する情報、電子メールヘッダー情報 (有効な場合)、ファイルを配信したアプリケーション、およびファイルのコマンドと制御のアクティビティに関連するすべての URL が表示されます。高度なWildFireレポートには、ファイルを転送したファイアウォールで設定されたセッション情報と、ファイルに対して観測された動作に基づいて、次の表に示す情報の一部またはすべてが含まれています。

*WildFire*ポータルに手動でアップロードされたファイル、または*WildFire API*を使用してアップロードされたファイルの*Advanced WildFire*レポートを表示すると、トラフィックがファイアウォールを通過しなかったため、レポートにセッション情報は表示されません。たとえば、レポートには攻撃者/送信元や被害者/宛先は表示されません。

レポートの見出し	詳説

File Information（ファイル情報）	• **File Type**（ファイル形式）：Flash、PE、PDF、APK、JAR/Class、または MS Office。このフィールドの名前は HTTP/HTTPS 電子メール リンク レポートの URL で、分析された URL が表示されます。
	• **File Signer**（ファイルの署名者）：認証を目的にファイルに署名したエンティティです。
	• **Hash Value**（ハッシュ値）：ファイル ハッシュは、ファイルを一意に識別して、どのような方法によってもファイルが変更されていないことを保証するフィンガープリントによく似ています。以下に、分析されるファイルごとに WildFire によって生成されるハッシュ バージョンの一覧を示します。
	  • **SHA-1**：ファイルの SHA-1 値が表示されます。
	  • **SHA-256**：ファイルの SHA-256 値が表示されます。

レポートの見出し	詳説
	• **MD5**：ファイルの MD5 情報が表示されます。 • **File Size**（ファイルサイズ）—WildFire で分析されたファイルのサイズ（バイト単位）です。 • **First Seen Timestamp**（初回閲覧時のタイムスタンプ）—WildFire システムで以前分析されたことがある場合、これは最初に検出されたときの日時です。 • **Verdict**（判定）—分析の判定が表示されます。 • **Sample File**（サンプル ファイル）—サンプル ファイルをローカル システムにダウンロードするには、**Download File**（ファイルのダウンロード） リンクをクリックします。ダウンロードできるのはマルウェア判定のファイルのみで、安全判定のファイルはダウンロードできません。
Coverage Status（カバー範囲ステータス）	**Virus Total**（全ウイルス） リンクをクリックして、他のベンダーによってすでに特定されているサンプルに対するエンドポイントのアンチウィルスの対応範囲の情報を表示します。一覧表示されているベンダーのいずれによってもファイルが検出されなかった場合は、「file not found」と表示されます。 さらに、レポートがファイアウォールでレンダリングされると、脅威から保護するために Palo Alto Networks で現在提供されているシグネチャおよび URL フィルタリングの処理対象に関する最新情報もこの画面に表示されます。この情報は動的に取得されるため、PDF レポートには表示されません。 アクティブなシグネチャについて、以下の対応範囲情報が表示されます。 • **Coverage Type**（カバータイプ）：Palo Alto Networks が提供する保護のタイプ（ウィルス、DNS、WildFire、またはマルウェアの URL）。 • **Signature ID**（シグネチャ**ID**）：Palo Alto Networks が提供する各シグネチャに割り当てられる一意の ID 番号。 • **Detail**（詳細）：ウィルスの一般名。

レポートの見出し	詳説
	• **Date Released**（リリース日）：マルウェアに対する保護を提供する対応範囲を Palo Alto Networks がリリースした日付。 • **Content Version**（コンテンツバージョン）：マルウェアに対する保護を提供するコンテンツ リリースのバージョン番号。
Session information [セッション情報**]**	サンプルを転送したファイアウォールを通過したときのトラフィックに基づいたセッション情報が含まれています。WildFire がレポートに含めるセッション情報を定義するには、**Device (**デバイス**)** > **Setup (**セットアップ**)** > **WildFire** > **Session Information Settings (**セッション情報送信項目設定**)**の順に選択します。 以下のオプションを使用できます。 • ソースIP • 送信元ポート • 宛先IP • 宛先ポート • 仮想システム（マルチ vsys がファイアウォールで設定されている場合） • アプリケーション • ユーザー（User-ID がファイアウォールで設定されている場合） • URL • FileName（ファイル名） • 電子メール送信者 • 電子メール受信者 • 電子メール件名 デフォルトでは、ファイアウォールがサンプルを許可またはブロックしたかどうかを示すステータスフィールドがセッション情報に含まれます。
Dynamic Analysis	リスクが低く、WildFireがファイルの安全性を容易に判断できる場合は、動的解析を行わずに静的解析のみを実行します。

レポートの見出し	詳説
	動的解析が実行されると、このセクションには、検体が実行された各環境の解析結果を示すタブが含まれます。たとえば、［仮想マシン4］タブには、Windows 7、Adobe Reader 11、Flash 11、Office 2010が動作している分析環境が表示されます。 *WildFire*アプライアンスでは、分析のために仮想マシンが *1* つだけ使用されます。管理者は、ローカル環境に最適な分析環境属性に基づいてその仮想マシンを選択します。たとえば、大半のユーザーが *32* ビットの *Windows 7* を使用している場合は、その仮想マシンを選択します。
Behavior Summary	各Virtual Machine [仮想マシン] タブには、特定の環境でのサンプル ファイルの動作がまとめられています。たとえば、サンプルによりファイルの作成または変更、プロセスの開始、新しいプロセスの生成、レジストリの変更、またはブラウザ ヘルパー オブジェクトのインストールが行われたかどうかなどが含まれます。 Severity [重大度] 列には、各動作の重大度が表示されます。重大度のゲージには、重大度が低い場合には棒が 1 本表示され、重大度レベルが高くなるにつれて棒の数が増えます。この情報は、動的分析と静的分析のセクションにも追加されます。 BEHAVIORAL SUMMARY This sample was found to be **malware** on this virtual machine. Behavior Description Severity Indicator Behavior / Severity Created a file in the Windows folder The Windows folder contains the core components of the Windows operating system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection. Deleted itself Malware often deletes itself after installation to avoid detection. Legitimate applications do not delete themselves directly. 以下に、分析されるさまざまな動作の説明を示します。 • **Network Activity (**ネットワーク アクティビティ**)**：サンプルによって実行されたネットワーク アクティビティ（ネットワーク上の他のホストへのアクセスや phone-home アクティビティなど）が表示されます。パケット キャプチャをダウンロードするためのリンクが提供されます。

レポートの見出し	詳説
	• **Host Activity (by process) (**ホストアクティビティ（プロセス別）**)**：設定、変更、または削除されたレジストリ キーなどの、ホストで実行されたアクティビティの一覧が表示されます。 • **Process Activity (**プロセス アクティビティ**)**：親プロセスを開始したファイル、プロセス名、およびプロセスで実行されたアクションが表示されます。 • **File (**ファイル**)**：子プロセスを開始したファイル、プロセス名、およびプロセスで実行されたアクションが表示されます。 • **Mutex**：サンプル ファイルがほかのプログラム スレッドを生成する場合、ミューテックス名および親プロセスがこのフィールドに記録されます。 • **Activity Timeline (**アクティビティ タイムライン**)**：サンプルの記録されたアクティビティすべてのプレイ バイ プレイ リストを表示します。これは、分析中に発生したイベントのシーケンスを理解するのに役立ちます。 アクティビティ タイムラインの情報は、*WildFire* レポートの *PDF* エクスポートでのみ確認できます。
Submit Malware [マルウェア送信**]**	サンプルを手動で Palo Alto Networks 送信する場合に、このオプションを使用します。WildFire クラウドは、サンプルの再分析を行い、そのサンプルを有害と判定するとシグネチャを生成します。これは、シグネチャ生成とクラウド インテリジェンスを有効にしていない WildFireアプライアンスの場合に役立ち、アプライアンスから WildFire クラウドにマルウェアを転送するために使用されます。
不正確な判定を報告	判定結果について誤検出または検出漏れが疑われる場合は、このリンクをクリックしてサンプルを Palo Alto Networks の脅威対策チームに送信してください。脅威対策チームは、サンプルの追加分析を行い、再分類すべきか判断します。マルウェア サンプルが安全であると判定されると、そのファイルのシグネチャは次のアンチウイルス シグネチャの更新で無効にされます。また、安全なファイルが有害であると判定されると、新しいシグ

レポートの見出し	詳説
	ネチャが生成されます。調査が完了すると、実行されたアクションについて記載された電子メールが送信されます。

WildFire 送信ログ設定の構成

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

WildFire送信ログは、自動的に生成されるタイムスタンプ付きのファイルであり、Palo Alto Networks ネットワークセキュリティプラットフォームがWildFire分析プロファイル設定（[オブジェクト] > [セキュリティ プロファイル] > [WildFire分析]）に基づいて分析する際に、WildFireクラウドにサンプル（ファイルと電子メールリンク）を転送したイベントを追跡する監査証跡を提供します。WildFire送信ログ エントリは、サンプルの静的分析および動的分析が完了した WildFire クラウドに転送されたサンプルごとに生成されます。WildFire送信ログ エントリには、サンプルに対して実行されたアクション (許可またはブロック)、WildFire 分析によって決定された送信されたサンプルに対する WildFire 判定、サンプルの重大度レベル、およびその他の詳細が含まれます。

デフォルトでは、WildFire送信ログは無害なサンプルと悪意のあるサンプルに対して作成されます。一方、グレイウェアと良性のサンプルはログを生成しません。WildFire送信ログ設定を変更して、電子メール リンクに含まれる追加のセッション情報だけでなく、グレイウェアおよび良性のサンプルも含めることができます。

Wildfire Submissions （**WildFire**送信）ログでは、以下のオプションを設定することができます。

- 安全あるいはグレイウェアと判定されたサンプルのロギングを有効にする
- WildFireログおよびレポートに電子メールのヘッダー情報を追加する

安全あるいはグレイウェアと判定されたサンプルのロギングを有効にする

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

安全あるいはグレイウェアと判定されたサンプルのロギングは初期設定では無効になっています。安全あるいはグレイウェアと判定されたメール内リンクはロギング対象外です。

STEP 1 | **Device (デバイス) > Setup (設定) > WildFire**を選択し、**General Settings**（一般的な設定）を編集します。

STEP 2 | **Report Benign Files**（安全なファイルを報告）及び**Report Grayware Files**（グレイウェアファイルを報告）の両方またはいずれかを選択し、**OK**をクリックして設定を保存します。

WildFireログおよびレポートに電子メールのヘッダー情報を追加する

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

以下の方法で電子メールのヘッダー情報（メール送信者、受信者、件名）をWildFireログやレポートに追加することができます。

サンプルと共にセッション情報がWildFireクラウドへ送信され、これらをもとにWildFire分析レポートが作成されます。ファイアウォールもWildFireクラウドも、実際の電子メールのコンテンツを受信、保存、または表示しません。

電子メールの添付ファイルやリンクにおいて検出された脅威を素早く見つけ出して修正したり、悪意のあるコンテンツにアクセスまたはダウンロードしてしまった人を特定したりする際にセッション情報が役立ちます。

STEP 1 | **Device**（デバイス） > **Setup**（セットアップ） > **WildFire**を選択します。

STEP 2 | （セッション情報送信項目設定） セクションを編集し、オプション（**Email sender**（電子メール送信者） 、**Email recipient**（電子メール受信者）、および **Email subject**（電子メール件名））を 1 つ以上有効にします。

STEP 3 | **OK** をクリックして保存します。

マルウェア検出時のアラートを設定する

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス

WildFireが悪意のあるサンプルまたはフィッシングサンプルを特定したときに警告を送信するように、Palo Alto Networksファイアウォールを設定できます。安全なファイルやグレイウェアファイルが検出された場合のアラートも設定できますが、安全あるいはグレイウェアの電子メールリンクについては設定することができません。この例は電子メール アラートの設定方法を示していますが、ログ転送を設定し、アラートがSyslogメッセージ、SNMP トラップ、またはPanoramaアラートとして送信されるよう設定することもできます。

STEP 1 | 電子メールサーバーのプロファイルを設定します。

1. **[Device]** > **[**サーバー プロファイル**]** > **Email**（Eメール） の順に選択します。
2. **Add (**追加**)**をクリックし、プロファイルの **Name (**名前**)**を入力します（WildFire-Email-Profile など）。
3. （任意）**Location (**場所**)**ドロップダウンから、このプロファイルの適用先となる仮想システムを選択します。
4. **Add (**追加**)**をクリックして新しい電子メール サーバー エントリを追加し、Simple Mail Transport Protocol（SMTP）サーバーに接続して電子メールを送信するために必要な情報を入力します（プロファイルには電子メール サーバーを 4 つまで追加できます）。
   - **Server (**サーバー**)**：電子メール サーバーを識別する名前（1 ～ 31 文字）。このフィールドは単なるラベルであり、既存の SMTP サーバーのホスト名である必要はありません。
   - **Display Name (**表示名**)**：電子メールの [差出人] フィールドに表示される名前。
   - **From (**送信者**)**：通知メールの送信元の電子メール アドレス。
   - **To (**宛先**)**：通知メールの送信先の電子メール アドレス。
   - **Additional Recipient(s) (**追加の受信者**)**：第 2 受信者に通知を送信するための電子メール アドレスを入力します。
   - **Gateway (**ゲートウェイ**)** - 電子メールの送信に使用する SMTP ゲートウェイの IP アドレスまたはホスト名。
5. **OK** をクリックしてサーバー プロファイルを保存します。
6. **Commit (**コミット**)**をクリックして設定中の項目に対する変更を保存します。

STEP 2 | 電子メール サーバー プロファイルをテストします。

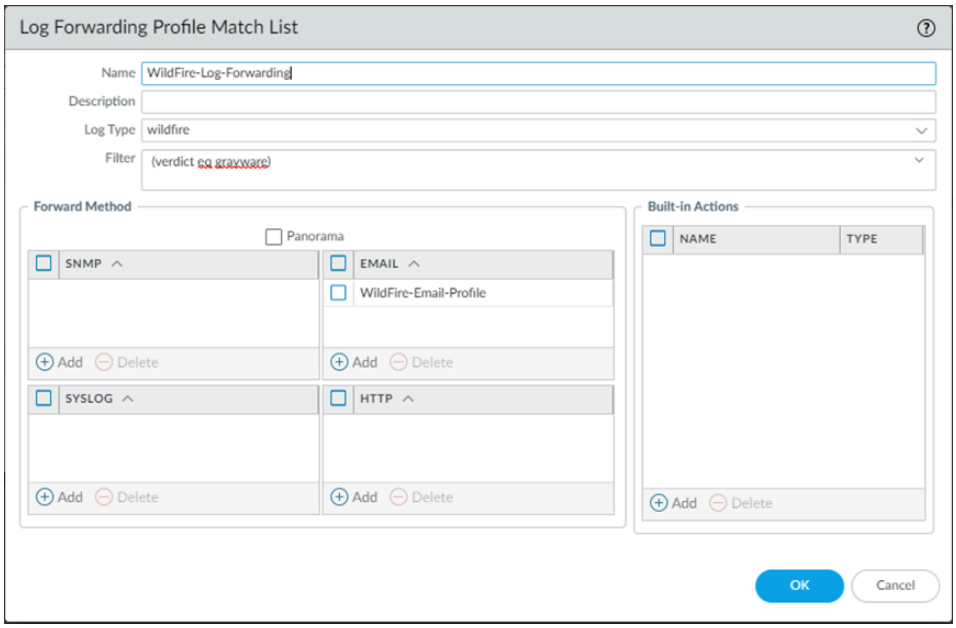
1. **[Monitor]** > **[PDF** レポート**]** > **[**電子メール スケジューラ**]** を選択します。
2. **Add**（追加）をクリックして、**Email Profile**（電子メールプロファイル） のドロップダウンリストから新しい電子メールプロファイルを選択します。
3. **Send test email**（テストメールの送信）ボタンをクリックすると、電子メールプロファイルで定義されている受信者にテスト電子メールが送信されます。

STEP 3 | ログ転送プロファイルを設定して、WildFire ログを、Panorama、電子メール アカウント、SNMP、Syslog サーバーおよび HTTP 要求に転送できるようにします。

この例では、サンプルに悪意があると認められたときのために電子メールのログを設定します。テストの際、安全なものとグレイウェアのログ転送を有効化し、多くのアクティビティが生成されるようにすることもできます。

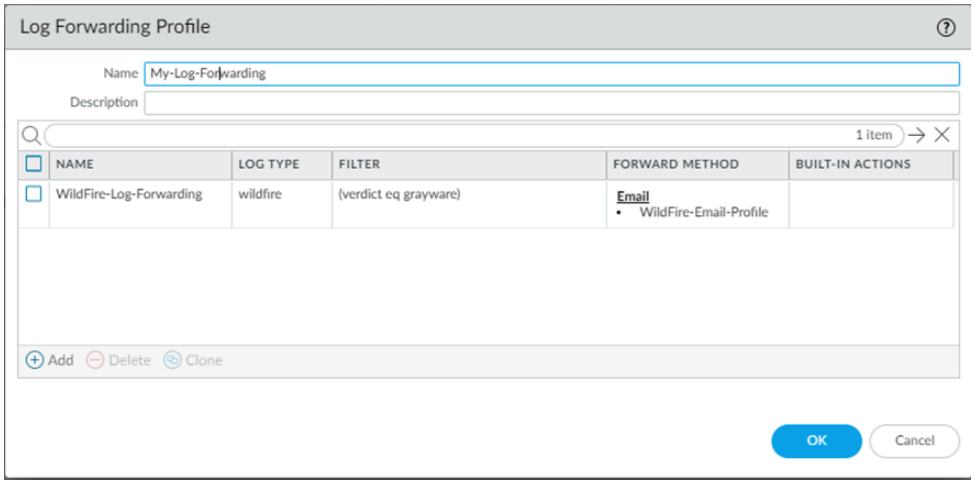
ファイアウォールは、ブロックされたファイルの*WildFire*ログを電子メールアカウントに転送しません。

1. **[Objects]** > **[**ログ転送**]**の順に選択します。
2. プロファイルを**Add**（追加）して名前を付けます（例：WildFire-Log-Forwarding）。オプションで、ログ転送プロファイルの**Description**（説明） を追加できます。
3. **Add**（追加） して転送方式を設定します。



1. **Log Fowarding Profile Match List**（ログ転送プロファイルの一致リスト）の名前を指定します。
2. **WildFire** ログタイプを選択します：
3. **(verdict eq malicious)** クエリを使用してログをフィルタリングします。
4. **Forward Method**（転送方式）オプションで、手順1（このケースでは、WildFire-Email-Profile）で作成した電子メールプロファイルを選択し、一致リストの更新を保存するために **OK** をクリックします。

4. 再度 **OK** をクリックしてログ転送プロファイルの更新を保存します。



STEP 4 | WildFireの転送に使用するセキュリティーポリシーにログ転送プロファイルを（WildFire分析プロファイル添付した状態で）追加します。

WildFire 分析プロファイルは、高度な WildFire 分析のためにファイアウォールが転送するトラフィックを定義します。WildFire 分析プロファイルを設定してセキュリティ ポリシー ルールに添付するには、高度な WildFire 分析のためのファイルの転送を参照してください。

1. **[Policies]** > **[**セキュリティ**]** の順に選択して、WildFire 転送で使用するポリシーをクリックします。
2. **Actions (**アクション**)**タブの**Log Setting (**ログ設定**)**セクションで、自分で設定した**Log Forwarding (**ログ転送**)**プロファイルを選択してください。
3. **OK** をクリックして変更を保存し、設定を **Commit (**適用**)**します。

WildFire のログと分析レポートを表示する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

WildFire ログには、分析のために WildFireクラウドにアップロードされたサンプル (ファイルと電子メールリンク) に関する情報が含まれています。これには、アプリケーションの種類や攻撃者のIPアドレスなど、ログに記録されたイベントに関連するプロパティ、アクティビティ、動作などのアーティファクトのほか、サンプルをマルウェア、フィッシング、グレイウェア、または良性に分類するなどの高レベルの分析結果や詳細なサンプル情報など、Wildfire固有の特性が含まれます。WildFire送信ログを確認することで、ネットワーク内のユーザーが疑わしいファイルをダウンロードしたかどうかもわかります。WildFire分析レポートには、詳細なサンプル情報のほか、対象ユーザーに関する情報、電子メールヘッダー情報 (有効な場合)、ファイルを配信したアプリケーション、およびファイルのコマンドと制御のアクティビティに関連するすべての URL が表示されます。これにより、ファイルが有害かどうか、レジストリ キーを変更したかどうか、ファイルの読み取り/書き込みを行ったかどうか、新しいファイルを作成したかどうか、ネットワーク接続チャネルを開いたのかどうか、アプリケーションのクラッシュを引き起こしたかどうか、プロセスを生成したかどうか、ファイルをダウンロードしたかどうか、他の有害な動作が示されているかどうかがわかります。

WildFireログはNGFWファイアウォールではWildFire送信ログとして表示されますが、クラウド管理プラットフォームでは、関連するログをStrata Logging Serviceにアップロードするようにログ転送を設定する必要があります。その後、WildFireログは脅威ログ(WildFireタイプ)として表示されます。

- Strata Cloud Manager
- PAN-OS & Panorama

WildFireのログと解析レポートを表示する(PAN-OSおよびPanorama)

WildFireの分析用に送信されるサンプルは、ファイアウォールの Web インターフェイス上で、**WildFire Submissions** （**WildFire**への送信） ログのエントリとして表示されます。それぞ

れのWildFireエントリから、サンプルのログ詳細やWildFire分析レポートを表示する詳細ログビューを開くことが出来ます。

Mozilla Firefox ユーザー*:WildFire* 分析レポートは、*Firefox v54* 以前のリリースでのみ正しく表示されます。レポートの表示で問題が発生した場合は、*Google Chrome* などの別のウェブブラウザの使用を検討してください。または、*PDF* バージョンをダウンロードして開くか、*WildFire* ポータルからレポートを表示することもできます。

STEP 1 | 「高度な WildFire 分析のためのファイルの転送」を行います。

STEP 2 | Configure WildFire Submissions Log Settings（WildFire提出ログの設定を設定する）。

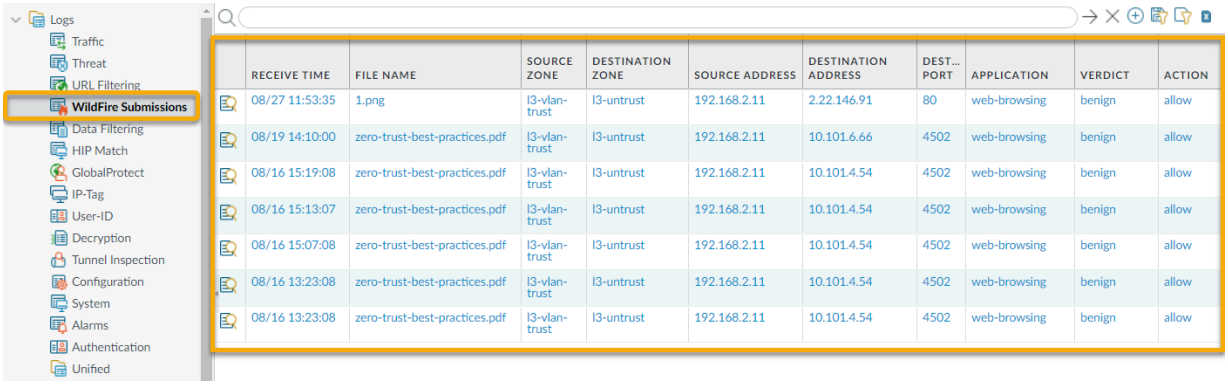
STEP 3 | ファイアウォールがWildFireパブリック、プライベート、もしくはハイブリッドクラウドに送信したサンプルを閲覧する場合は、 **Monitor (モニター) > Logs (ログ) > WildFire Submissions (WildFireへの送信)**を選択します。サンプルのWildFire分析が完了すると、サンプルを送信したファイアウォールへ結果が送り返され、WildFireへの送信ログから閲覧できるようになります。送信ログには次の情報のような、任意のサンプルについての詳細情報が含まれています：

- 判定の列にはサンプルが安全なファイル、グレイウェア、マルウェアのいずれにあたるかが表示されます。
- Action（アクション）列はファイアウォールが、サンプルを許可またはブロックしているかどうかを示します。

- Severity (重大度) 列は、対象のサンプルが組織に及ぼす脅威の大きさを critical (重要)、high (高)、medium (中)、low (低)、informational (通知) という値を使って示します。

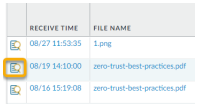
  次の重大度レベルの値は、判定およびアクションの値を組み合わせて決定されます。

  - 低—アクションが許可に設定されたグレイウェアのサンプルです。
  - 高—アクションが許可に設定された悪意のあるサンプルです。
  - 通知：
    - アクションが許可に設定された安全なサンプルです。
    - アクションがブロックに設定されたいずれかの判定を持つサンプルです。

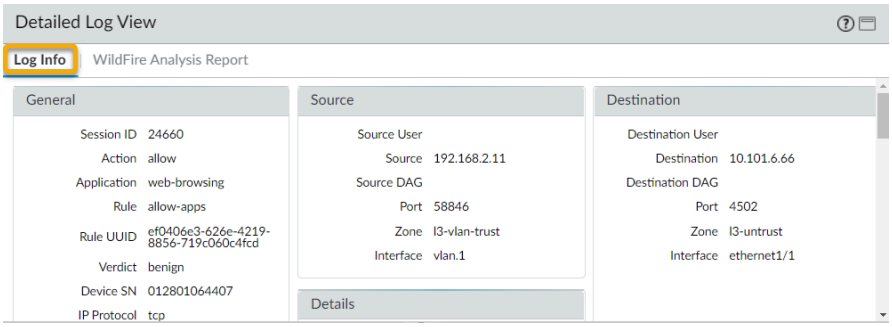


RECEIVE TIME	FILE NAME	SOURCE ZONE	DESTINATION ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	DEST... PORT	APPLICATION	VERDICT	ACTION
08/27 11:53:35	1.png	l3-vlan-trust	l3-untrust	192.168.2.11	2.22.146.91	80	web-browsing	benign	allow
08/19 14:10:00	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.6.66	4502	web-browsing	benign	allow
08/16 15:19:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 15:13:07	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 15:07:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 13:23:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 13:23:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow

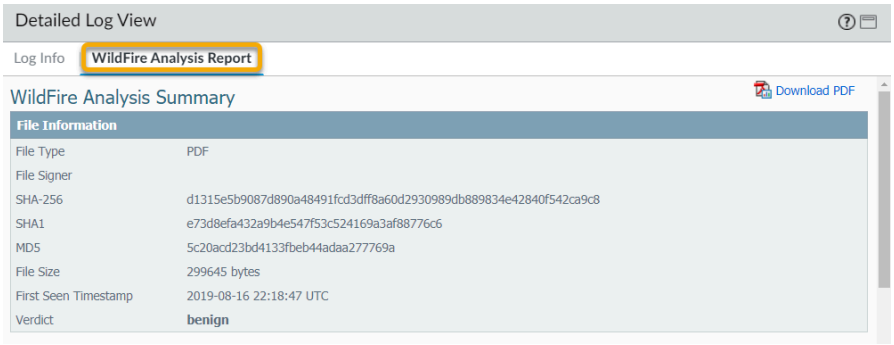
STEP 4 | 各エントリの詳細ログビューを開く際はLog Details （ログ詳細） のアイコンを選択してください。



詳細ログビューには、エントリ内のログ情報とWildFire分析レポートが表示されます。ファイアウォールのパケットキャプチャ（PCAP）が有効化されている場合、サンプルのPCAPもここに表示されます。



全てのサンプルに対し、WildFire分析レポートからファイルとセッションの詳細を表示させることができます。マルウェアのサンプルの場合はWildFire分析レポートの内容が拡張され、そのファイルに悪意があると判断される原因となった性質や挙動について詳細情報が表示されています。



STEP 5 | （オプション）WildFire分析レポートの**Download PDF**（**PDF**をダウンロード）を行います。

WildFireのログと解析レポートを表示する(Cloud Management)

Panoramaを使用して***Prisma Access***を管理している場合は、以下のプロセスに従って*Prisma Access*のコンテンツにアクセスするか、***[PAN-OS]***タブに切り替えてガイダンスに従うことができます。

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerアプリケーションにログインします。

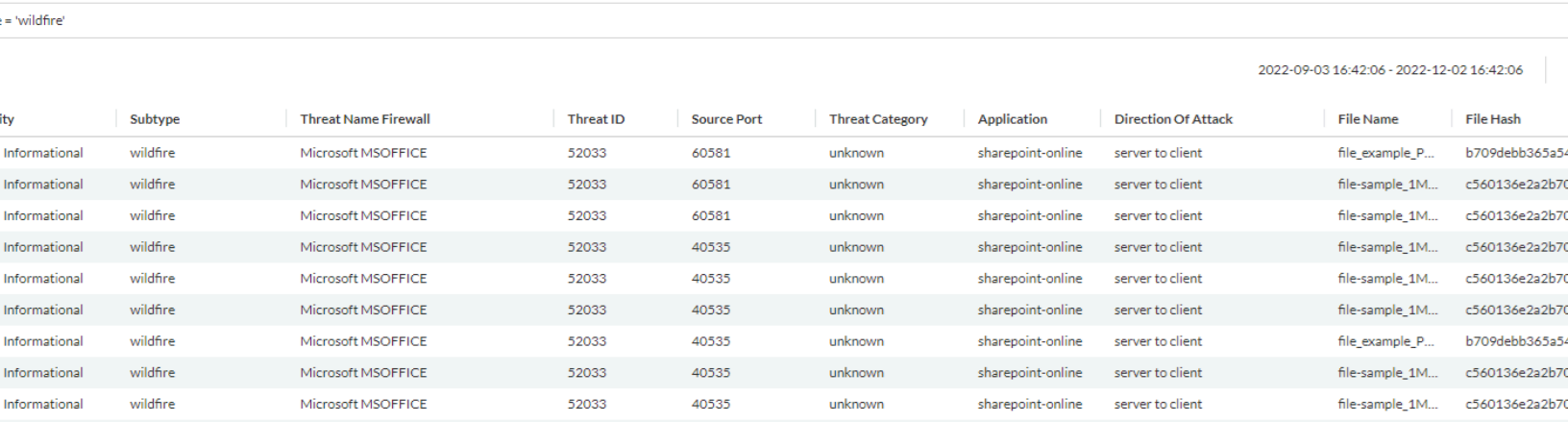
> Activity の使用方法の詳細については、「Log Viewer (ログ ビューアー)」を参照してください。

STEP 2 | 脅威ログをフィルタリングして、Prisma Accessに提出されたWildFire検体の送信を表示します。

1. **[Incidents and Alerts (インシデントとアラート)]** > **[Log Viewer (ログ ビューアー)]**を選択します。
2. 検索するログの種類を **Threat(脅威)**に変更します。
3. クエリ ビルダーを使用して WildFire サンプル送信を示すために使用される WildFire サブタイプを使用して検索フィルターを作成します。たとえば、`sub_type.value = 'wildfire'` を使用して WildFire ログを表示できます。必要に応じて、追加のクエ

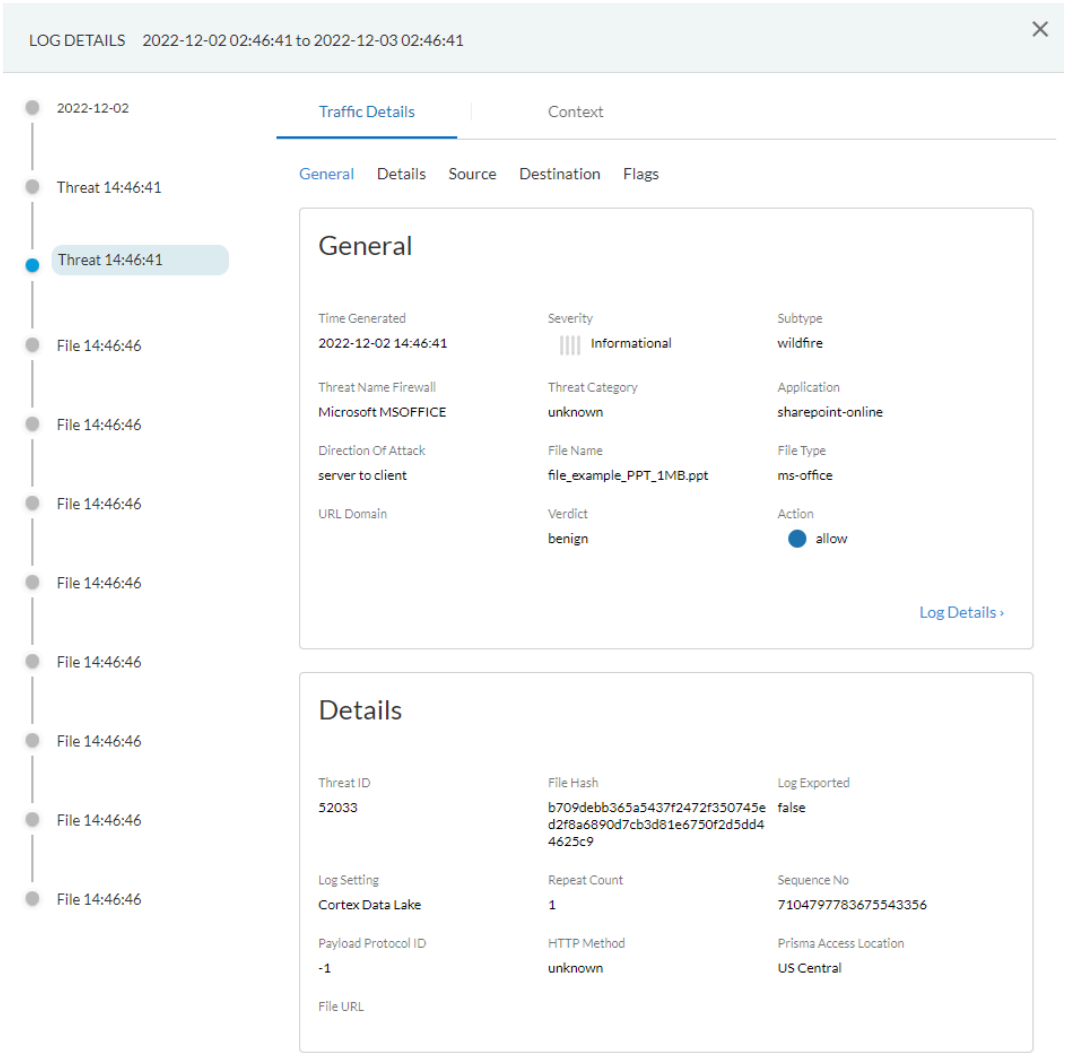
リ パラメータ (重大度レベルやアクションなど) や日付範囲など、検索条件を調整します。

*WildFire*分析レポートを表示するには、*WildFire* ポータルにログインし、ハッシュ値またはファイル名を使用してレポート ファイルを取得する必要があります。詳細については、「WildFire ポータル上でレポートを確認する」を参照してください。



ity	Subtype	Threat Name Firewall	Threat ID	Source Port	Threat Category	Application	Direction Of Attack	File Name	File Hash
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a54
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a54
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70

4. フィルターの組み立てが完了したら、クエリを実行します。
5. 結果からログ エントリを選択すると、ログの詳細が表示されます。
6. 脅威ログの サブタイプは、サンプルに関するその他の情報とともに **[全般]** ペインに表示されます。脅威に関するその他の関連詳細は、対応するウィンドウに表示されます。



WildFireポータルを使用したマルウェアの監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

Palo Alto NetworksのWildFireポータルを開き、Palo Alto Networksのサポート認証情報またはWildFireアカウントを使用してログインします。ポータルにダッシュボードが表示され、特定の WildFire サブスクリプションまたはサポート アカウントに関連付けられているすべてのファイアウォールのサマリー レポート情報の一覧が表示されます。ポータルには、リストされているデバイスごとに、検出されたマルウェアサンプルの数、分析された安全なファイルの数、これから分析される保留中のファイルの数についての統計情報が表示されます。WildFireポータルアカウント上には、ポータルへ手動で送信されたサンプルと共に、ネットワーク上でWildFireパブリッククラウドに接続されたファイアウォールから送信されたサンプルすべてに関するデータが表示されます。さらに、を有効にして、ワイルドファイア アプライアンスでマルウェアを署名の生成と配布のために WildFire パブリック クラウド に転送する場合、それらのマルウェア サンプルのレポートにもポータルからアクセスできます。

WildFireポータルを用いてWildFireアクティビティを監視する方法については以下のセクションをご覧ください。

- WildFireポータル設定のカスタマイズ
- WildFireポータルのユーザーアカウントの追加
- WildFire ポータル上でレポートを確認する

WildFireポータル設定のカスタマイズ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

どこで使用できますか?	何が必要ですか?
• VM-Series • CN-Series	

このセクションでは、カスタマイズできるWildFireクラウドアカウントの設定（アカウントに接続された各ファイアウォールのタイムゾーンや電子メール通知など）について説明します。また、クラウドに保存されたファイアウォールのログを削除することもできます。

STEP 1 | ポータルの設定にアクセスします。

1. WildFireポータルにログインします。
2. メニューバーの**Settings**（設定）を選択します。

STEP 2 | WildFireクラウドアカウントのタイムゾーンを設定します。

Set Time Zone（タイムゾーン設定）のプルダウンリストからタイムゾーンを選択し、**Update Time Zone**（タイムゾーンを更新） をクリックし、変更を保存します。

*WildFire*分析レポートに表示されるタイムスタンプは、*WildFire*クラウドアカウントで設定されたタイムゾーンに基づいています。

STEP 3 | （オプション）特定のファイアウォールのクラウド上でホストされているWildFireログを削除します

1. **Delete WildFire Reports**（**WildFire**のレポート削除）のドロップダウンを開き、シリアルナンバーからファイアウォールを指定して**Delete Reports**（レポート削除）をクリックすれば、WildFireポータルに保存されたログを削除することができます。このアクションでは、ファイアウォールに保存されたログは削除されません。
2. **OK** をクリックして、削除を続行します。

STEP 4 | （オプション）WildFire分析の判定に基づいて電子メール通知を設定します。

*WildFire*ポータルは、ファイアウォールが*WildFire*分析のために転送したブロックファイルのアラートを送信しません。

1. アラート設定のセクションで、**Malware, Phishing**（マルウェア、フィッシング）、**Grayware**（グレイウェア）、**Benign**（安全）から、電子メール通知を希望するタイプにチェックを入れます。
   - WildFireクラウドにアップロードされた全ての判定結果の通知を希望する場合は**All**（全て）の列の判定チェックボックスを選択してください。
   - WildFireポータルを経由してWildFireパブリッククラウドに手動でアップロードされた判定結果の通知を希望する場合は**Manual**（手動）の列の判定チェックボックスを選択してください。
   - 特定のファイアウォールから送信された判定結果の通知を希望する場合は、それぞれのファイアウォールのシリアルナンバーの判定チェックボックスを選択してください。
2. サポートアカウントに登録済みの電子メールアドレスへ判定内容の電子メール通知を行う場合は、**Update Notification**（通知内容を更新）を選択してください。

WildFireポータルのユーザーアカウントの追加

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

WildFireクラウドアカウントは、スーパー ユーザー（Palo Alto Networks デバイスの登録所有者）によって作成されます。WildFireクラウドアカウントを使用すると、他のユーザーがWildFireクラウドにログインしたり、スーパー ユーザーまたは登録所有者によって明示的に許可されたデバイスのデータを表示したりできます。WildFireのユーザーは既存のPalo Alto Networksアカウントとの連携が可能で、Palo Alto Networksサポートアカウントを保有していない場合はWildFireパブリッククラウドと特定のファイアウォールデータへのアクセスが可能になります。

STEP 1 | WildFireポータルへアクセスできるユーザーを追加したいアカウントを選択します。

WildFireポータルのユーザーは、そのサポートアカウントに関連する全てのファイアウォールの情報を参照することができます。

1. Palo Alto Networks サポートポータルにログインします。
2. **Manage Account**（アカウント管理）から、**Users and Accounts**（ユーザーおよびアカウント）をクリックします。
3. 既存のアカウントまたはサブアカウントを選択します。

STEP 2 | WildFire ユーザーを追加します。

1. **Add WildFire User**（**WildFire** ユーザーを追加）ボタンをクリックします。
2. 追加したいユーザーの電子メール アドレスを入力します。

ユーザーを追加する際の唯一の制限は、無料の*Web*ベース電子メールアカウント（*Gmail*、*Hotmail*、*Yahoo* など）の電子メールアドレスは使用できないことです。サポートされていないドメインの電子メール アドレスが入力されると、警告のポップアップが表示されます。

STEP 3 | ファイアウォールを新しいユーザー アカウントに割り当てて、WildFireクラウドにアクセスします。

アクセス権を付与したいファイアウォールのシリアルナンバーを選択し、任意でアカウントの詳細を入力します。

既存のサポート アカウントのユーザーは、WildFire のレポート表示で現在使用できるファイアウォールのリストが記載された電子メールを受信します。サポート アカウントを作成していないユーザーの場合、ポータルでは、ポータルへのアクセス方法と新しいパスワードの設定方法を記載した電子メールを送信します。

これで新規ユーザーは、WildFireクラウドにアクセスし、アクセス権が付与されているファイアウォールの WildFireレポートを表示できます。また、ユーザーはこれらのデバイスの自動電子メール アラートを設定し、分析されたファイルのアラートを受信することもできます。受信するレポート（有害なファイルのレポートや安全なファイルのレポート）を選択できます。

WildFire ポータル上でレポートを確認する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ 高度な Wildfire ライセンス *Prisma Access*の場合、これは通常*Prisma Access*ライセンスに含まれています。

どこで使用できますか?	何が必要ですか?
• VM-Series • CN-Series	

WildFireポータルには、ファイアウォールから送信されたサンプル、手動でアップロードしたサンプル、WildFire APIを通じてアップロードされたサンプルに関するレポートが表示されます。WildFireクラウドが分析した最新のレポートを表示する場合は**Reports**（レポート） を選択します。レポートエントリには、登録されたそれぞれのサンプルについて、サンプルがクラウドに届いた日時、ファイルを送信したファイアウォールのシリアルナンバー、ファイル名あるいはURL、そしてWildFireの判定結果（安全、グレイウェア、マルウェア、フィッシング）が表示されています。

ファイル名やサンプルのハッシュ値からレポートを探す場合は検索機能を使用してください。特定の**Source**（ソース）（手動で送信されたもの、あるいは特定のファイアウォールから送信されたもののみを表示）、あるいは特定のWildFire**Verdict**（判定） （全て、安全、マルウェア、グレイウェア、フィッシング、保留中）から絞り込みを行うことが出来ます。

ポータルから各レポートを表示にするには、レポート名の左にある **Reports**（レポート）アイコンをクリックします。詳細なレポートを保存するには、レポートページの右上にある **Download as PDF**（**PDF** としてダウンロード） ボタンをクリックします。WildFire分析レポートの詳細については、WildFire Analysis Reports—Close Up（WildFire分析レポート - クローズアップ）を参照してください。

以下に、特定のファイアウォールによって送信されるサンプルファイルの一覧を示します。