paloalto
TECHDOCS

高度なURLフィルタリングの管理

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 21, 2023

Table of Contents

URLフィルタリングの基本

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URLフィルタリングテクノロジーは、ユーザーのアクセスとインターネット上のコンテンツとの対話をきめ細かく制御することで、Webベースの脅威からユーザーを保護します。URLカテゴリ、ユーザー、グループに基づいてサイトへのアクセスを制限するURLフィルタリングポリシーを開発できます。たとえば、マルウェアをホストすることがわかっているサイトへのアクセスをブロックしたり、エンドユーザーが特定のカテゴリのサイトに企業の資格情報を入力するのを防ぐことができます。

カテゴリへのユーザーアクセスをきめ細かく制御するには、URLフィルタリングプロファイルを作成し、定義済みおよびカスタムURLカテゴリのサイトアクセスを定義します。次に、プロファイルをセキュリティポリシールールに適用します。URLカテゴリをセキュリティ ポリシー ルールの一致条件として使用することもできます。高度なURLフィルタリングのサブスクリプションが組織のWebセキュリティニーズを満たす方法の一覧については、URL フィルタリングのユース ケースを参照してください。

- Palo Alto NetworksのURLフィルタリング ソリューションについて
- URLフィルタリングのサポート
- ローカルインライン分類
- アドバンスドURLフィルタリングの仕組み
- URL フィルタリング プロファイル
- URL カテゴリ
- URL フィルタリングのユース ケース

Palo Alto NetworksのURLフィルタリング ソリューションについて

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)	❑ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

高度なURLフィルタリング（URLフィルタリングが先行）は、既知および未知を問わず、悪意のある脅威や回避的なWebベースの脅威からネットワークとそのユーザーを保護するサブスクリプションサービスです。サブスクリプションでは、URLフィルタリングと同じ機能（きめ細かなURLフィルタリング制御、ユーザーのWebアクティビティの可視化、安全な検索の実施、資格情報のフィッシング防止）に加え、インライン機械学習ベースのWebセキュリティエンジンを使用した完全なWebコンテンツ検査が提供されます。インラインWebセキュリティエンジンは、クライアントのカテゴリー検索要求を保留のクラウドベースのURLデータベースであるPAN-DBには存在しないURLのリアルタイム分析と分類を可能にします。その後、ファイアウォールが実行するアクションがエンジンによって決定されます。

高度なURLフィルタリングは、PAN-DBが分析してデータベースに追加する前に更新または導入された悪意のあるURLからトラフィックを保護します。Advanced URL Filtering を有効にすると、URL 要求は次のようになります。

- クラウドベースの高度なURLフィルタリング検出モジュールを使用したリアルタイムな分析。これは、PAN-DBのエントリと比較されるURLに追加されます。MLを搭載したWeb保護エンジンは、PAN-DBでは検出できない悪意のあるウェブサイトを検出してブロックします。
- 未知の悪意のある Web ページをリアルタイムでブロックできる firewall ベースの分析ソリューションである local インライン分類 を使用して、フィッシングと悪意のある JavaScript がないか検査。

PAN-OS 9.1以降を実行する次世代ファイアウォールでは、高度なURLフィルタリングライセンスがサポートされています。PAN-OSとPanoramaのWebインターフェイス、Prisma Access、Cloud NGFWプラットフォームでURLフィルタリング機能を管理できます。ただし、一部のURLフィルタリング機能は各プラットフォームでは利用できません。

企業のネットワーク セキュリティ要件によって firewall によるインターネットへの直接アクセスが禁止されている場合、Palo Alto Networks はPAN-DB Private Cloudを備えたオフライン URL

フィルタリング ソリューションを提供します。ネットワーク内のPAN-DB サーバとして機能する1つ以上のM-600アプライアンスにPAN-DBプライベートクラウドをデプロイできます。ただし、プライベートクラウドは高度なURLフィルタリング ソリューションで提供されるクラウドベースのURL分析機能をサポートしていません。

レガシー**URL**フィルタリングサブスクリプション

URLフィルタリングは、ローカルキャッシュまたはPAN-DBに保存されたウェブサイトにポリシールールを適用します。ユーザーがウェブサイトを要求すると、ファイアウォールはローカルキャッシュのURLカテゴリをチェックします。ウェブサイトがキャッシュにない場合、ファイアウォールはPAN-DBに問い合わせて、適用するアクションを決定します。その結果、攻撃者は、クラウドベースのデータベースに存在しないURLを使用して、精密な攻撃キャンペーンを開始できるようになります。

従来のサブスクリプション所有者は、ライセンス期間が終了するまで*URL*フィルタリングのデプロイメントを引き続き使用できます。

URLフィルタリングのサポート

高度なURLフィルタリング機能は、次世代ファイアウォール (仮想およびオンプレミス) AWS用クラウドNGFW、Prisma Access (Managed by Strata Cloud Manager)、Prisma Access (Managed by Panorama)、およびAzure用クラウドNGFWで使用できます。ただし、次世代ファイアウォールとCloud NGFW for Azureには高度なURLフィルタリングのサブスクリプションが必要ですが、Prisma AccessとCloud NGFW for AWSのライセンスには高度なURLフィルタリング機能がすべて含まれています。

機能のサポートは、プラットフォームと*URL*フィルタリングライセンスの種類によって異なります。高度な*RL*フィルタリング ライセンスでのみ利用可能な機能は、高度な*URL*フィルタリングのラベルで示されています。

URLフィルタリングをサポートしているPalo Alto Networksの各プラットフォームとの高度なURLフィルタリング機能の互換性を次の表に示します。

機能	サポートされている						メモ
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW for AWS	Cloud NGFW for Azure	
インライン分類 • ローカルインライン分類 • （PAN-OS 10.2以前はインラインMLと呼ばれていた）（高度なURLフィルタリング）クラウドイン	あり	あり	あり	あり	あり	あり	VM-50またはVM50Lアプライアンスではサポートされていません

機能	サポートされている						メモ
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW for AWS	Cloud NGFW for Azure	
ライン分類							
カスタムURL カテゴリ	あり	あり	あり	あり	あり	あり	
ユーザー証明書検出	あり	あり	あり	あり	あり	あり	
カスタムURLフィルタリング応答ページ	あり	あり	あり	あり	あり	あり	
セーフサーチの適用 • 厳密なセーフサーチがオフの場合の検索結果のブロック • 厳密なセーフサーチを強制する	あり	あり	あり	あり	あり	あり	
URL 管理オーバーライド	あり	あり	あり	あり	あり	あり	

機能	サポートされている						メモ
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW for AWS	Cloud NGFW for Azure	
SSL/TLS ハンドシェイク検査	あり	あり	あり	あり	あり	あり	
リモートブラウザ分離（RBI）との統合。	いいえ	なし	あり	あり	なし	いいえ	
ログコンテナページのみ（ユーザーが訪問したページのみログに記録）	いいえ	あり	あり	あり	あり	あり。	

ローカルインライン分類

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URLフィルタリングライセンス 注:Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

ローカル インライン分類 (以前はインライン ML と呼ばれていました) を使用すると、firewall データプレーンは Web ページに機械学習(ML)を適用して、フィッシングの亜種が検出されたときにユーザーに警告し、JavaScript エクスプロイトの悪意のある亜種がネットワークに侵入するのを防ぐことができます。ローカル インライン分類は、一連のMLモデルを使用してさまざまなWebページの詳細を評価することにより、悪意のあるコンテンツを動的に分析および検出します。各 ML モデルは、デコーダー フィールドやパターンなどのファイルの詳細を評価して、高確率の分類と判定を定式化することによって悪意のあるコンテンツを検出し、より大きな Web セキュリティ ポリシーの一部として使用されます。悪意のある URL は、追加の分析と検証のために PAN-DB に転送されます。URL 例外を指定して、検出される可能性のある誤検知を除外できます。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、プロファイルに対してより詳細なルールを作成できます。脅威の状況の最新の変更に追いつくために、インライン ML モデルは定期的に更新され、コンテンツ リリースを通じて追加されます。アクティブな Advanced URL Filtering サブスクリプションは、インライン分類 を構成するために必要です。

また、MLベースのインライン保護を有効にして、アンチウイルスプロファイル構成の一部として、悪意のあるポータブル実行ファイル（PE）、ELFファイル、MS Officeファイル、PowerShellおよびシェルスクリプトをリアルタイムで検出することもできます。詳細については、以下を参照してください:高度なWildFireインラインML。

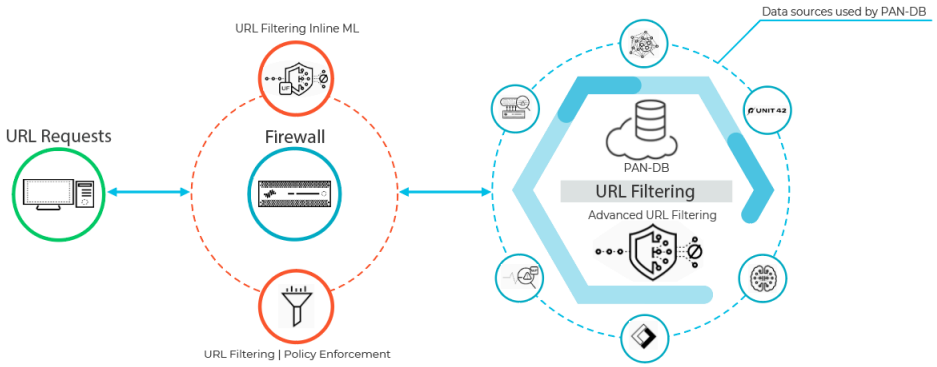
ローカルのインライン分類は、*VM-50*または*VM50L*仮想アプライアンスではサポートされていません。

アドバンスドURLフィルタリングの仕組み

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

アドバンスドURLフィルタリングは、サイトのコンテンツ、機能、および安全性に基づいてWeb サイトを分類します。URLには、サイトが脅威にさらされる可能性を示す最大4つのURLカテゴリを設定できます。アドバンストURLフィルタリングのURLデータベースであるPAN-DBがサイトを分類するため、アドバンストURLフィルタリングを有効にしたファイアウォールはその知識を活用して、組織のセキュリティポリシーを実施することができます。PAN-DBによって提供される保護に加えて、アドバンストURLフィルタリングでは、機械学習（ML）を用いたリアルタイム分析により、新しい脅威や未知の脅威に対する防御を実現します。これにより、URL フィルタリング データベースがコンテンツを分析して追加する機会が得られ、攻撃者が精密攻撃キャンペーンを開始できるオープン期間が提供される前に更新または導入された悪意のあるURL に対する保護が提供されます。アドバンストURLフィルタリングは、リクエストごとにリアルタイムでURLを分析することで、データベースソリューションに特有のカバレッジのギャップを補います。高度なURLフィルタリングで使用されるMLベースのモデルは、さまざまな悪意のあるURL、フィッシングWebページ、コマンドアンドコントロール（C2）を検出するために、トレーニングが行われ、継続的に更新されています。

特定の高度な脅威の存在を示すWebサイトは、クラウドベースのインライン深層学習システムで追加処理され、アドバンスドURLフィルタリングで使用されるMLモデルを補完するディテクターとアナライザーを介して処理されます。ディープラーニングによる検知は、より大きなデータセットを処理することができ、多層のニューラルネットワークによって、複雑な悪意のあるパターンや行動をよりよく識別することができます。アドバンストURLフィルタリングは、疑わしいWebリクエストを受信した際に、ファイアウォールからHTTPレスポンスデータを受け取ると、そのデータをさらにディープラーニングディテクターで分析し、回避的なゼロデイWeb攻撃に対するインライン防御を提供します。これには、未知のWebサイトからWebページのコンテンツを不正に取得するクローキングWebサイトが含まれます。具体的には、URLデータベースが対応できない悪意のあるコンテンツ、多段階攻撃、CAPTCHAチャレンジ、以前は見られなかったワンタイムURLなどが含まれます。回避可能な悪意のあるWebサイトは常に流動的であるため、Webサイトの分類に使用されるディテクターとアナライザーは、パロアルトネットワークスの脅威研究者が検出ロジックを改善する際に自動的に更新・展開され、管理者は更新パッケージをダウンロードする必要はありません。



ユーザーが Web ページを要求すると、ファイアウォールはユーザーが追加した例外と、サイトのリスク カテゴリの PAN-DB を照会します。PAN-DBは、ユニット42、ワイルドファイア、パッシブDNS、Palo Alto Networksテレメトリデータ、サイバー脅威同盟からのデータからのURL情報を使用し、カテゴリを決定するために様々なアナライザを適用します。URLに危険性や悪意のある特徴が見られる場合は、Webペイロードデータもクラウド上のアドバンストURLフィルタリングに送信してリアルタイムに解析し、追加の解析データを生成しています。その結果生じるリスク カテゴリはファイアウォールによって取得され、ポリシー構成に基づいて Web アクセス ルールを適用するために使用されます。さらに、ファイアウォールは新しいエントリのサイトのカテゴリ情報をキャッシュして、以降の要求に対して高速に取得できるようにしますが、ユーザーが最近アクセスしていない URL を削除して、ネットワーク内のトラフィックを正確に反映します。また、PAN-DB クラウド クエリに組み込まれているチェック機能により、ファイアウォールが最新の URL 分類情報を確実に受信するようにします。インターネットに接続されていない場合、またはURLフィルタリングライセンスが有効でない場合、PAN-DBへの問い合わせは行われません。

firewall は、Web サイトの URL カテゴリを、1) カスタム URL カテゴリ、2) 外部動的リスト (EDL)、および 3) 定義済みURLカテゴリのエントリと比較し、優先順位をつけてウェブサイトのURLカテゴリを決定します。

データプレーンで機械学習を使用して URL をリアルタイムで分析するように設定されたファイアウォールは、フィッシング Web サイトや JavaScript のエクスプロイトに対するセキュリティの追加レイヤーを提供します。ローカルインライン分類で使用される ML モデルは、Palo Alto Networks が悪意のあるものとして識別した特性に一致する URL ベースの脅威の現在未知および将来の亜種を識別します。最新の脅威の変化に対応するため、ローカルのインライン分類MLモデルは、コンテンツリリースによって追加・更新されます。

ファイアウォールが PAN-DB の URL をチェックするとき、以前は無害であると認定されていたが現在は悪意のある URL などの重要な更新も検索します。

PAN-DB がサイトを誤って分類したと思われる場合は、Test A Siteを介して、またはファイアウォール ログから直接、ブラウザで変更要求を送信できます。

補足

技術的には、ファイアウォールは管理プレーンとデータプレーンの両方で *URL* をキャッシュします。

- *PAN-OS 9.0* 以降のリリースでは、*PAN-DB* シードデータベースはダウンロードされません。代わりに、*URL* フィルタリング ライセンスがアクティベーションされると、ファイアウォールは *URL* クエリが行われるときにキャッシュを読み込みます。
- 管理プレーンはより多くの *URL* を保持し、*PAN-DB* と直接通信します。ファイアウォールは、キャッシュ内で *URL* のカテゴリを見つけることができず、*PAN-DB* で検索を実行すると、取得したカテゴリ情報を*management plane (* 管理プレーン *- MP)*にキャッシュします。*management plane (* 管理プレーン *- MP)*はその情報をデータプレーンに渡します。データプレーンもそれをキャッシュし、それを使用してポリシーを適用します。
- データプレーンは保持する *URL* が少なく、管理プレーンから情報を受信します。ファイアウォールがのURLカテゴリの例外リスト*(*カスタム*URL*カテゴリと外部動的リスト*)*を*URL*に対してチェックした後、次に表示される場所はデータプレーンです。ファイアウォールはデータプレーンで*URL*が見つからない場合、管理プレーンをチェックし、カテゴリ情報がない場合は*PAN-DB*をチェックします。

URL フィルタリング プロファイル

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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URLフィルタリングプロファイルは、ファイアウォールが特定のURLカテゴリへのトラフィックを処理する方法を定義します。URLフィルタリング プロファイルは、インターネットへのアクセスを許可する個々のセキュリティ ポリシー ルールに適用するURLフィルタリング コントロールの集合です。URLカテゴリのサイトアクセスの設定、ユーザー資格情報の提出の許可/不許可、安全な検索適用の有効化、その他のさまざまな設定を行うことができます。URLフィルタリングプロファイルで定義されたアクションを適用するには、プロファイルをセキュリティポリシールールに適用します。firewall は、Security ポリシー・ルールに一致するトラフィックにプロファイル・アクションを適用します (詳しくは、URL フィルタリングの設定 を参照してください)。

ファイアウォールには、脅威になりやすいカテゴリ（malware、phishing、Adultなど）をブロックするように設定されているデフォルト プロファイルが付属しています。このデフォルト プロファイルは、セキュリティ ポリシー規則で使用したり、コピーして新しいURLフィルタリング プロファイルを作成するときに利用したりできます。また、新しいURLフィルタリング プロファイルを追加することもできます。新しく追加されたこのURLフィルタリングプロファイルをカスタマイズして、常にブロックまたは許可する必要のあるある特定のWebサイトのリストを追加できます。たとえば、ソーシャルネットワークカテゴリをブロックしても、そのカテゴリの特定のウェブサイトへのアクセスを許可することができます。デフォルト設定では、基本URLフィルタリング プロファイルの作成を行う際、すべてのURLカテゴリに対してサイト アクセスが許可されるように設定されています。これは、ユーザーはすべてのサイトを自由に閲覧でき、トラフィックがログに記録されないことを意味しています。

ベストプラクティスのURLフィルタリング プロファイルを作成し、マルウェアあるいは悪意のあるコンテンツをホストしていることが分かっている*URL*から確実に保護されるようにします。

URLフィルタリング プロファイル ポリシー アクション

URLフィルタリングプロファイルでは、URLカテゴリのサイトアクセスを定義したり、URLカテゴリに基づいてユーザー資格情報の提出を許可または禁止したり(たとえば、中リスクおよび高

リスクのサイトへのユーザー資格情報提出をブロックしたり)、安全な検索の実施を有効にしたりできます。

操作	説明
サイト アクセス	
Alert [アラート]	Web サイトが許可され、URL フィルタリング ログにログ エントリが生成されます。 ブロックしないトラフィックのカテゴリーに対するアクションとして***alert*** **(**アラート**)**を設定し、トラフィックをログに記録して可視性を確保します。
allow [許可]	Web サイトが許可され、ログ エントリは生成されません。 ログに記録しないトラフィックに対する可視性が失われるため、ブロックしないトラフィックのカテゴリーに対するアクションとして***allow*** **(**許可**)**を設定しないでください。その代わりに、ブロックしないトラフィックのカテゴリーに対するアクションとして***alert*** **(**アラート**)**を設定し、トラフィックをログに記録して可視性を確保します。
block	Web サイトがブロックされ、応答ページが表示されます。Web サイトへのアクセスを続行することはできません。URL フィルタリング ログでログ エントリが生成されます。 ある URL カテゴリについてサイト アクセスをブロックすると、その URL カテゴリの User Credential Submissions (ユーザーの認証情報送信) もブロックに設定されます。
続行	会社のポリシーによりサイトがブロックされたことを示す応答ページが表示され、Web サイトへのアクセスを続行するオプションが表示されます。**[continue]** アクションは、通常、無害とみなされるカテゴリで使用され、ユーザーがサイトが正しく分類されていないと感じる場合に、操作を続行するためのオプションを提供することで、ユーザーの操作性を向上させるために使用されます。応答ページのメッセージをカスタマイズして、自社専用の詳細情報を含めることができます。URL フィルタリング ログでログ エントリが生成されます。

操作	説明
	プロキシ サーバーを使用するように設定されているクライアントシステムでは、*Continue* (続行) ページは正しく表示されません。
override [オーバーライド]	特定のカテゴリの Web サイトへのアクセスを許可するためにパスワードが必要であることを示す応答ページが表示されます。このオプションを使用して、セキュリティ管理者またはヘルプデスク担当者は、特定のカテゴリのすべての Web サイトに一時的なアクセスを付与するパスワードを提供します。URL フィルタリング ログでログ エントリが生成されます。特定のサイトへのパスワード アクセスを許可するを参照してください。 以前のバージョンでは、URL フィルタリングカテゴリのオーバーライドがカスタム URL カテゴリより優先されていました。PAN-OS 9.0 へのアップグレードの一環として、URL カテゴリのオーバーライドはカスタム URL カテゴリに変換され、他のカスタム URL カテゴリに優先されることはなくなりました。以前のバージョンでカテゴリのオーバーライドに対して定義したアクションの代わりに、最も厳格なURLフィルタプロファイルアクションを使用する新しいカスタムURLカテゴリがセキュリティポリシールールによって適用されます。最も厳格なものから最も緩やかなものまで、可能な URL フィルタリングプロファイルアクションは、ブロック、上書き、続行、警告、および許可となります。 つまり、アクション allow で URL カテゴリのオーバーライドを行った場合、PAN-OS 9.0 でカスタム URL カテゴリに変換された後にオーバーライドがブロックされる可能性があります。 プロキシ サーバーを使用するように設定されているクライアントシステムでは、*Override* (オーバーライド) ページは正しく表示されません。
none [なし]	**none** アクションはカスタム URL カテゴリにのみ適用されます。**none** を選択し、複数の URL プロファイルが存在する場合に、そのカスタム カテゴリが他のプロファイルに影響を与えないようにするためです。たとえば、2 つの URL プロファイルがあり、カスタム URL カテゴリが一方のプロファイルで**block** [ブロック]に設定されている場合、もう一方のプロファイルに対してブロック アクショ

操作	説明
	ンを適用したくない場合は、アクションを**none** [なし]に設定する必要があります。 また、カスタム URL カテゴリを削除するには、使用されるプロファイルで **[none]** に設定されている必要があります。
ユーザーの認証情報の権限 これらの設定では、最初の 設定された資格情報フィッシング防止 を設定する必要があります。	
Alert [アラート]	この URL カテゴリに属すサイトにユーザーが企業の認証情報を送信することを許可しますが、毎回 URL フィルタリング アラート ログを生成します。
allow（デフォルト）	この URL カテゴリに属すサイトにユーザーが企業の認証情報を送信することを許可します。
block	この URL カテゴリに属すサイトにユーザーが企業の認証情報を送信することをブロックします。デフォルトのアンチフィッシング応答ページは、ユーザーが企業の認証情報を送信することがブロックされているサイトにアクセスする際に表示されます。表示するブロックページをカスタマイズできます。
続行	応答ページを表示し、サイトにアクセスするためにユーザーが Continue（続行）を選択することを要求します。デフォルト設定では、認証情報を送信することが推奨されないサイトにユーザーがアクセスする際にアンチフィッシング続行ページが表示されます。応答ページをカスタマイズして、フィッシング詐欺の試みや認証情報を他のウェブサイトで再利用しないようにユーザーに警告することができます。

URL カテゴリ

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

Palo Alto Networksは、コンテンツ、機能、安全性に基づいてウェブサイトを分類しています。各URLカテゴリは、ポリシールールの作成に役立つ特性のセットに対応しています。ネットワーク上のユーザーがアクセスするURLは、Palo Alto NetworksのURLフィルタリングデータベースPAN-DBに追加されます。PAN-DBは、これらのウェブサイトにリスクカテゴリー（高、中、低）を含む最大4つのURLカテゴリーを割り当てています。

URLカテゴリは、Webトラフィックのカテゴリベースのフィルタリングと、サイトのきめ細かいポリシー制御を可能にします。URLフィルタリングプロファイルを設定して、URLカテゴリのサイトアクセスを定義し、インターネットへのトラフィックを許可するセキュリティポリシールールにプロファイルを適用できます。URLカテゴリをセキュリティポリシー規則の一致基準として使用し、それらの規則が指定されたカテゴリのウェブサイトにのみ適用されるようにすることもできます。たとえば、金融サービス カテゴリへのトラフィックの復号化を禁止する復号化ポリシー規則を設定できます。

特定のURLのカテゴリを確認するには、当社のURL検索エンジンであるTest A SiteにURLを入力します。URLが誤って分類されていると思われる場合は、カテゴリ変更リクエストを送信してください。

カスタム URL カテゴリ

カスタムURLカテゴリを作成して、カテゴリベースの強制から特定のウェブサイトを除外できます。カスタムURLカテゴリは、特定のURL（URLリスト）または他のカテゴリ（カテゴリマッチ）に基づいて設定できます。URLリストタイプのカスタムURLカテゴリは、ブロックリストと許可リストとして機能します。カテゴリマッチタイプのカスタムURLカテゴリでは、カスタムカテゴリの一部として定義されているすべてのカテゴリに一致するウェブサイトに対して、ターゲットを絞った強制が可能になります。

事前定義されたURLカテゴリ

次の表は、PAN-DBがURLのフィルタリングに使用する定義済みURLカテゴリの一覧です。エントリによっては、カテゴリから除外されるサイトを記述します。セキュリティ重視の URL カテ

ゴリはリスクカテゴリを記述します。リスクカテゴリは、すべてのURLに割り当てられるわけではありません。

URL カテゴリ	詳説
妊娠中絶	中絶に賛成または反対する情報またはグループに関連するサイト、中絶手順に関する詳細、中絶に賛成または反対するフォーラムの支援または支援、または中絶を追求する（またはしない）結果/効果に関する情報を提供するサイト。
薬物乱用	合法薬物と違法薬物の乱用、薬物関連器具の使用と販売、薬物の製造および/または販売を促進するサイト。
adult	性的に露骨な素材、メディア（言語、ゲーム、漫画を含む）、アート、または製品を含むサイト、性的に露骨な性質のオンライングループまたはフォーラム、およびビデオ会議や電話会議、エスコートサービス、ストリップクラブなどのアダルトサービスを宣伝するサイト。
アルコールとタバコ	アルコールおよび/またはタバコ製品および関連器具の販売、製造、または使用に関連するサイト。電子タバコに関連するサイトが含まれています。
人工知能	大規模言語モデルを含む機械学習とディープラーニングモデルを使用して、通常であれば人間の知能を必要とするサービスを提供するウェブサイト。提供されるサービスには、チャットボット、生産性、要約機能、トランスクリプター、ノーコード、音声または動画編集関連サービスが含まれますが、これらに限定されません。情報AIコンテンツではなく、実際のAIサービスをホストするWebサイトを重視している。
オークション	個人間の商品販売を促進するサイト。 寄付目的のオークションはこれに分類されます。
ビジネスと経済	マーケティング、経営、経済、起業、事業運営に関連するコンテンツを含むサイト。 • 広告・マーケティング会社向けサイト • fedex.comなど、配送サービスのサイト

URL カテゴリ	詳説
	• 電話、ケーブル、およびインターネットサービスプロバイダ向けのサイト • アンケートまたは投票のためのサイト • 商工会議所のためのサイト • カンファレンスのためのサイト* • 企業のウェブサイトは、このカテゴリではなく、そのテクノロジーで分類される可能性があります。 • #会議関連サイトは、内容に基づいて分類してください。サイトのコンテンツが具体的でない場合は、ビジネスとエコノミーに分類されます。
コマンドアンドコントロール	マルウェアや感染したホストが、密かに攻撃者のリモートサーバーと通信を行って悪意のあるコマンドを受信したりデータを盗んだりするために使用する、コマンドアンドコントロール(C2)URLおよびドメイン。
コンピュータとインターネット情報	コンピュータとインターネットに関する一般的な情報を提供するサイト。次のトピックに関するサイトが含まれます。 • 計算機科学 • 工学 • ハードウェアおよびコンピュータ部品 • software • セキュリティ • プログラミング プログラミングは「参照と研究」カテゴリと重複する部分もありますが、主要なカテゴリは「コンピュータとインターネット情報」にしてください。

URL カテゴリ	詳説
コンテンツ配信ネットワーク	広告、メディア、ファイル、画像サーバーなどの第三者にコンテンツを配信することを主な目的とするサイト。
著作権侵害	ソフトウェアまたはその他の知的財産の違法ダウンロードを許可するコンテンツなど、違法なコンテンツがあるドメインであり、潜在的な責任のリスクをもたらします。 ピアツーピアのファイル交換サービスや一般的なストリーミングメディアを提供するサイトは、それぞれのカテゴリに属します。
仮想通貨	暗号通貨を宣伝するサイト、暗号マイニング（ただし、埋め込まれた暗号マイナーではない）、暗号通貨取引所とベンダー、および暗号通貨ウォレットと元帳を管理するサイト。 暗号通貨に言及しているサイトや、暗号通貨に関連する悪意のあるサイトは、別途分類されます。例えば、暗号通貨やブロックチェーン技術の仕組みを説明するサイトは、*Computer and Internet Info*に該当します。
デート	オンライン出会い系サービス、アドバイス、その他の個人広告を提供するサイト。 性的なチャットルームを提供している出会い系サイトはアダルトに分類されます。
ダイナミックDNS	ドメイン名とダイナミックIPアドレスを関連付けるダイナミックDNSサービスを提供または利用するサイト。 ダイナミック*DNS*は、コマンド・アンド・コントロール通信やその他の悪意のある目的で攻撃者によって使用されることがよくあります。

URL カテゴリ	詳説
教育機関	学校、カレッジ、大学、学区、オンラインクラス、およびその他の学術機関の公式Webサイト。個別指導アカデミーのサイトも含まれています。 このカテゴリは、小学校、高校、大学などの大規模で確立された教育機関を指します。
暗号化DNS	DNSリゾルバサービスプロバイダ向けのサイト。DNS over HTTPS（DoH）のようなプロトコルを使用してDNSの要求と応答を暗号化することで、エンドユーザーにセキュリティとプライバシーを提供する。
エンターテイメントとアート	映画、テレビ、ラジオ、ビデオ、番組ガイド/ツール、コミック、舞台芸術、美術館、アート ギャラリー、図書館のサイト。以下のサイトが含まれます。 • エンターテインメント • 有名人やエンターテイメント業界のニュース • 小説 • ダンス教室 • イベント会場 • タトゥーアート
過激主義	テロ、人種差別、ファシズムや、民族的な出自や宗教、その他の考え方が異なる人や集団を差別するその他の過激な思想を喧伝するサイト。地域によっては、法規制により過激派サイトへのアクセスが禁止されている場合があり、アクセスを許可すると責任を問われる可能性があります。 物議を醸す政治的または宗教的見解を論じるウェブサイトは、それぞれ「哲学」および「政治的擁護と宗教」のカテゴリに分類されます。
金融サービス	オンラインバンキング、ローン、住宅ローン、債務管理、クレジットカード会社、外国為替（FOREX）、保険会社など、個人の財務情報やアド

URL カテゴリ	詳説
	バイスに関するサイト。健康保険、株式市場、証券会社、取引サービスに関連するサイトは除きます。
gambling	リアルマネーおよび/またはバーチャルマネーの交換を容易にする宝くじまたはギャンブルのサイト。オッズやプールの賭け方など、ギャンブルに関する情報、チュートリアル、アドバイスを提供する関連サイトが含まれています。 ギャンブルができないホテルやカジノの企業サイトは旅行のカテゴリーに入ります。
ゲーム	ビデオゲームやコンピュータゲームのオンラインプレイやダウンロード、ゲームレビュー、ヒント、チート、または関連する出版物やメディアを提供するサイト。電子的でないゲームの手順を提供するサイト、ボードゲームの販売や取引を促進するサイト、オンライン懸賞や景品をサポートまたは主催するサイトが含まれます。
政府	地方政府、州政府、および中央政府、ならびに関連機関、サービス、または法律の公式 Web サイト。 公共図書館や軍事機関のサイトは、それぞれ「リファレンス」と「研究」および「軍事」のカテゴリに分類されます。
グレイウェア	直接的なセキュリティ上の脅威にはならないが、その他の目障りな動作を表示し、エンドユーザーにリモートアクセスの許可やその他の許可されていない操作の実行を促すコンテンツを含むサイト。 グレーウェアには、次のものがあります。 • ハッキングされたサイト • 悪意のある挙動を示さず、標的ドメインによって所有されていないドメインをタイプスクワットする • 不正なソフトウェア、アドウェア、またはその他の迷惑なアプリケーション（組み込み暗号マイナー、クリックジャッキング、Webブラウザの要素を変更するハイジャッカーなど）を含むサイト

URL カテゴリ	詳説
	• 違法行為や犯罪行為に関する内容を含むサイト
ハッキング	通信機器またはソフトウェアへの違法または疑わしいアクセスまたは使用に関連するサイト（そのようなプログラムの開発および配布、操作方法のアドバイス、またはネットワークやシステムのセキュリティ侵害につながる可能性のあるヒントを含む）。ライセンスとデジタル著作権システムのバイパスを容易にするサイトも含まれます。
健康と医学	一般的な健康情報、問題、伝統的および非伝統的ヒント、救済策、治療法に関する情報を含むサイト。また、専門家だけでなく、さまざまな医療の専門、プラクティス、施設（ジムやフィットネスクラブなど）のサイトが含まれています。医療保険や美容整形に関連するサイトも含まれています。
ホーム＆ガーデン	住宅の修理とメンテナンス、建築、設計、建設、装飾、ガーデニングに関する情報、製品、およびサービスがあるサイト。
狩猟と釣り	狩猟や釣りのヒントや指示を提供したり、関連機器やパラフェナリアの販売を容易にするサイト。 主に銃器を販売するサイト（狩猟目的であっても）は武器カテゴリに該当する。
コンテンツが不十分	テストページを表示したり、コンテンツを表示しなかったり、エンドユーザが表示することを意図していない API アクセスを提供したり、別の分類を示唆している他のコンテンツを表示せずに認証を要求したりするウェブサイトやサービス。
インターネット通信とテレフォニー	ビデオチャット、インスタントメッセージ、テレフォニー機能をサポートまたはサービスを提供するサイト。
インターネットポータル	ユーザーの出発点として機能するサイト（通常は、コンテンツとトピックの広範なセットを集約することによって）。

URL カテゴリ	詳説
求人検索	求人情報、雇用者のレビュー、面接のアドバイスやヒント、または雇用者と求職者双方のための関連サービスを提供するサイト。
法務	法律、法律サービス、法律事務所、またはその他の法的関連事項に関する情報、分析または助言を提供するサイト。
マルウェア	悪意のあるコンテンツ、実行可能ファイル、スクリプト、ウイルス、トロイの木馬、コードを含む、またはホストすることがわかっているサイト。
マリファナ	娯楽目的か薬用目的かを問わず、マリファナとその無数の別名について、議論、奨励、宣伝、提供、販売、供給、またはその他の方法で使用、栽培、製造、配布を提唱するサイト。マリファナ関連のパラフェナリアに関するコンテンツを含むサイトを含みます。
軍事	軍事部門、募集、現在または過去の作戦、または関連する道具に関する情報または解説があるサイト。軍人会や退役軍人会のためのサイトも含まれています。
自動車	自動車、オートバイ、ボート、トラック、レクリエーショナルビークル（RV）のレビュー、販売、取引、改造、部品、その他関連する議論に関する情報を含むサイト。
音楽	音楽の販売、配信、情報に関するサイト。音楽アーティスト、グループ、レーベル、イベント、歌詞、および音楽ビジネスに関するその他の情報に関するWeb サイトが含まれます。音楽ストリーミングサイトを除く。
新しく登録されたドメイン	過去32日以内に登録されたサイト。新しく登録されたドメインは、意図的にまたはドメイン生成アルゴリズムによってしばしば生成され、悪意のある活動に使用されます。
ニュース	オンライン出版物、ニュースワイヤーサービス、および現在の出来事、天気、またはその他の現代の問題を集約するその他のウェブサイト。以下の内容が含まれています。

URL カテゴリ	詳説
	• 新聞 • ラジオ局 • 雑誌 • ポッドキャスト • ニュースに特化したテレビ番組 • reddit.comなどのソーシャルブックマークサイト 雑誌やニュースのウェブサイトがスポーツ、旅行、ファッションなど特定のトピックに焦点を当てている場合、サイト上の支配的なコンテンツに基づいて分類されます。
未解決	このカテゴリは、Webサイトがローカル URLフィルタリングデータベースに見つからず、ファイアウォールがカテゴリを確認するためにクラウドデータベースに接続できなかったことを示します。
裸体	アートワークなど、文脈や意図に関係なく、人体のヌードまたはセミヌードの描写を含むサイト。参加者の画像を含むヌーディストまたはナチュリストのサイトが含まれます。
オンラインストレージとバックアップ	無料またはサービスとしてファイルのオンラインストレージを提供するサイト。写真共有サイトも含まれます。
駐車	限定コンテンツやクリックスルー広告をホストするURL。ホストエンティティに収益をもたらす可能性があるが、一般的にエンドユーザーに役立つコンテンツは含まれていない。販売対象のドメインを含みます。 アダルトコンテンツを含む公園サイトはアダルトに分類されます。
ピアツーピア	トレント、ダウンロードプログラム、メディアファイル、またはその他のソフトウェアアプリケーションのピアツーピア共有のためのアクセスまたはクライアントを提供するサイト。主にBitTorrentのダウンロード機能を持つサイトに適用される。シェアウェアやフリーウェアのサイトは対象外です。

URL カテゴリ	詳説
個人サイトとブログ	個人またはグループによる個人のウェブサイトやブログ。そのようなサイトが他のカテゴリに関連付けられた支配的なトピックを持っている場合、両方のカテゴリに分類されます。
哲学と政治的主張	哲学的または政治的見解に関する情報、見解、キャンペーンを含むサイト。
フィッシング	ログイン認証情報、クレジットカード情報、口座番号、PIN、その他の個人識別情報（PII）などの情報を、ソーシャルエンジニアリングの手法を用いて、被害者から任意または不本意に収集しようとするWebコンテンツ。テクニカルサポート詐欺やスケアウェアも含まれます。
プライベート IP アドレス	このカテゴリには、RFC 1918「プライベートイントラネットのためのアドレス割り当て」で定義されたIPアドレスが含まれます。IPアドレスは次のとおりです。 • 10.0.0.0～10.255.255.255(10/8プレフィックス) • 172.16.0.0~172.31.255.255(172.16/12プレフィックス) • 192.168.0.0~192.168.255.255(192.168/16プレフィックス) パブリックDNSシステムに登録されていないドメイン（*.localや*.onionなど）も含まれます。
プロキシ回避とアノニマイザ	URLフィルタリングや監視を迂回するプロキシサーバやその他の方法。 企業レベルの用途のVPNは、インターネット通信およびテレフォニーのカテゴリに分類されます。
疑わしい	個人やグループの特定の層を標的とした、悪趣味なユーモアや不快なコンテンツを含む Web サイト。
ランサムウェア	ランサムウェアキャンペーンの実施に関わるランサムウェアまたは悪意のあるトラフィックをホストすることがわかっているサイト。一般的に、要求された身代金が支払われるまで、プライベートデータを公開したり、特定のデータやシステムへのアクセスをブロックしたりする恐れがある。ランサムウェア

URL カテゴリ	詳説
	のペイロードを運ぶ可能性のある、関連するステルス、ワイパー、ローダーを配信するURLが含まれています。
不動産	物件の賃貸、販売、および関連するヒントや情報を提供するサイト。以下のサイトが含まれます。 • 不動産会社とエージェント • レンタルサービス • リスティング(および集計) • 特性改善 • 住宅所有者団体 • プロパティ管理グループまたは個人 住宅ローンやローン業者向けのサイトは金融サービスに分類されます。
リアルタイム検出(高度なURLフィルタリングのみ)	「高度なURLフィルタリング」の一環として、リアルタイムインライン解析で解析・検出されたURL。
レクリエーションと趣味	レクリエーションや趣味に関連する情報、フォーラム、協会、グループ、出版物で構成されるサイト。 *REI.com*など、レクリエーションや趣味に関する商品を販売するサイトもショッピングに該当する。
リファレンスとリサーチ	オンライン辞書、地図、年鑑、国勢調査情報、図書館、系譜、科学情報など、個人、職業、学術の参照ポータル、資料、サービスを提供するサイト。以下のサイト、または関連するサイトを含みます。 • イエローページ • カレンダー • 公共図書館 • 研究機関 • ライトおよび車両追跡サービス • 不動産、交通等に関する書類及び記録（行政に属する場合でも）
宗教	さまざまな宗教、関連する活動またはイベントに関する情報を含むサイト。宗教団体、宗教関係者、礼

URL カテゴリ	詳説
	拝所、占い、占星術、星占い、宗教パラフェナリアのサイトが含まれます。 カトリック系学校など、宗教団体に加盟する私立の初等・中等教育学校のうち、一般宗教教育や世俗科目を教えるカリキュラムを持つ学校が教育機関に該当する。
スキャン アクティビティ(高度なURLフィルタリングのみ)	攻撃者が行うキャンペーンで、セキュリティ侵害の指標となるもの、標的型攻撃や既存の脆弱性の調査を試みるもの。これらは通常、敵対者が行う偵察活動の一部である。
検索エンジン	キーワード、フレーズ、またはその他のパラメータを使用した検索インターフェイスを提供し、結果として情報、ウェブサイト、画像、またはその他のファイルを返す可能性のあるサイト。
性教育	生殖、性的発達、安全な性行為、性感染症、避妊、より良いセックスのためのヒント、ならびに関連する製品または関連器具に関する情報を提供するサイト。関連するグループ、フォーラム、または組織のサイトが含まれます。
シェアウェアとフリーウェア	ソフトウェア、スクリーンセーバー、アイコン、壁紙、ユーティリティ、着信音、テーマ、ウィジェットへのアクセスを無料または寄付で提供するサイト。オープンソースプロジェクトも含まれます。
ショッピング	商品やサービスの購入を容易にするサイト。オンライン加盟店、百貨店向けサイト、小売店向けサイト、カタログ、価格集計ツールまたは監視ツールが含まれます。このカテゴリのサイトは、さまざまな商品を販売している（またはネット販売を主目的とする）オンラインマーチャントである必要があります。 たまたまネット購入が可能な化粧品会社のサイトは化粧品カテゴリに該当します。

URL カテゴリ	詳説
ソーシャル ネットワーキング	ユーザー同士がやり取りしたり、メッセージや画像を投稿したり、ユーザーのグループと通信したりするユーザーコミュニティやサイト。 個人サイト、ブログ、フォーラムは、個人サイトおよびブログに分類されます。
社会	一般の人々に関連するコンテンツ、ファッション、美容、慈善団体、社会、子供など、多種多様な人々に影響を与える問題のあるサイト。レストランのウェブサイトが含まれます。 バーガーキングなど、食に関する企業サイトはビジネス・エコノミーカテゴリーに該当する。
スポーツ	スポーツイベント、アスリート、コーチ、役員、チームまたは組織、スポーツスコア、スケジュール、関連ニュース、および関連する道具に関する情報。ファンタジースポーツやバーチャルスポーツリーグのウェブサイトを含む。 スポーツ用品の販売を主な目的とするサイトはショッピングカテゴリに該当します。
株式投資アドバイスとツール	株式市場、株式またはオプションの取引、ポートフォリオ管理、投資戦略、相場、または関連ニュースに関する情報があるサイト。
ストリーミングメディア	オンラインラジオ局、ストリーミング音楽サービス、ポッドキャストのアーカイブなど、オーディオまたはビデオコンテンツを無料または購入するストリーミングサイト。
水着と下着・寝間着	水着、親密な服装、その他の挑発的な衣服に関する情報や画像を含むサイト
トレーニングとツール	オンライン教育訓練および関連資料を提供するサイト。自動車学校または交通学校、職場のトレーニング、ゲーム、アプリケーション、教育目的のツール、および個別指導アカデミーが含まれます。

URL カテゴリ	詳説
	特定の技能クラスは、その科目に基づいて分類されます。例えば、音楽教室のウェブサイトは音楽カテゴリに分類されます。
翻訳	ユーザー入力と URL 翻訳の両方を含む翻訳サービスを提供するサイト。これらのサイトでは、ターゲットページのコンテンツが翻訳者のURLのコンテキスト内に表示されるため、ユーザーはフィルタリングを回避できます。
トラベル	ヒント、お得な情報、価格、目的地情報、観光、予約ツールや価格監視ツールなどの関連サービスなど、旅行に関する情報を提供するサイト。以下のウェブサイトを含みます。 • 地元の観光スポット • ホテル • 航空会社 • クルーズライン • カジノ（サイトがオンラインギャンブルを許可していない場合） • 旅行会社 • 車両レンタル • 駐車場設備
未知	Palo Alto Networks によってまだ識別されていないサイトです。 このサイトの可用性がビジネスにとって重要であり、トラフィックを許可し、未知のサイトに警告し、トラフィックにベストプラクティスセキュリティプロファイルを適用し、アラートを調査する必要がある場合。

URL カテゴリ	詳説
	*PAN-DB*リアルタイム更新は、未知のサイトへの最初のアクセス試行後に未知のサイトを学習するため、未知の*URL*は迅速に識別され、ファイアウォールが実際の*URL*カテゴリに基づいて処理できる既知の*URL*となります。
兵器	武器、防具、防弾チョッキ、およびその使用に関するレビュー、説明、指示を扱う、または提供するサイト。 クレー射撃、射撃場、アーチェリーに関するサイトには、武器のプライマリーカテゴリーとスポーツのセカンダリーカテゴリーがあります。
ウェブ広告	広告、メディア、コンテンツ、バナーのあるサイト。ニュースレターや広告を購読・解除するためのページを含みます。
Web ベース電子メール	電子メールの受信トレイへのアクセスと電子メールの送受信機能を提供するすべての Web サイト。そのようなサービスへの無料または有料のパブリックアクセスを提供するウェブサイトに重点が置かれています。
ウェブホスティング	ウェブページの無料または有料ホスティングサービスを提供しているサイト。ウェブ開発、公開、プロモーション、およびその他のトラフィック増加の方法に関する情報を含むサイトが含まれます。

セキュリティ重視の URL カテゴリ

PAN-DBは、悪意のあるものと分類されていないURL、または少なくとも30日間良性の活動しか表示されていないために悪意のあるものと分類されなくなったURLに対して、リスクカテゴリ（高リスク、中リスク、低リスク）を自動的に評価して割り当てます。各リスクカテゴリには、URLが所定のカテゴリを受け取るために満たす必要がある特定の基準があります。サイトのコンテンツが変更されると、リスクカテゴリとポリシーの適用が動的に適応されます。

*PAN-DB*は、*URL*が悪意のあるURLカテゴリに属していると判断した場合、そのサイトにリスクカテゴリを割り当てません。その代わり、ほとんどの環境では受け入れがたいリスクが生じるため、ファイアウォールは自動的にサイトをブロックします。

プライベート *IP* アドレス (およびホスト) はホスト環境に固有であり、*PAN-DB* からは見えません。その結果、*Palo Alto Networks*はこのカテゴリのサイトにリスク評価を割り当てません。

セキュリティに重点を置いたURLカテゴリにより、標的を絞った復号化とポリシー適用が容易になり、攻撃対象領域の削減に役立ちます。たとえば、高リスクおよび中リスクのウェブサイトや新しく登録されたドメインへのアクセスをブロックしたり、これらのカテゴリへのトラフィックを復号化したりすることができます。

次の表に、各リスクカテゴリの説明とデフォルトおよび推奨ポリシーアクションを示します。

セキュリティに重点を置いた *URL* カテゴリの変更要求を送信することはできません。

URL カテゴリ	詳説
高リスク	• MLモデルによってドメインが、既知の悪意のあるドメインにリンクされているプロパティを持っているか、Webレピュテーションシグナルが低いと判断されたサイト。 • 以前にマルウェア、フィッシング、またはコマンドアンドコントロール（C2）サイトであることが確認されたサイト。 • 確認された悪意のある活動に関連するサイト、または悪意のあることがわかっているサイトとドメインを共有するサイト。 • 防弾 ISP によってホストされているサイト。 • アクティブな動的 DNS 設定が存在するため、DDNS として分類されたドメイン。 • 悪意のあるコンテンツを許可することが知られている ASN から IP でホストされているサイト。 • サイトは不明として分類されています。 これらのサイトは、*PAN-DB*がサイトの分析と分類を完了するまで、高いリスクのままです。 • サイトは、少なくとも30日間はこのカテゴリのままになります。

URL カテゴリ	詳説
	デフォルトおよび推奨ポリシーアクション:アラート
中リスク	• マルウェア、フィッシング、または C2 サイトであることが以前に確認されたサイトで、少なくとも 30 日間は良性の活動しか示されていないもの。 • すべてのクラウドストレージサイト（オンラインストレージおよびバックアップに分類されるサイト）。 • 不明として分類されたIPアドレス。  *PAN-DB*がサイト分析と分類を完了するまでは、これらの*IP*アドレスは中リスクとして分類されます。 • サイトは、さらに60日間このカテゴリのままになります。 デフォルトおよび推奨ポリシーアクション:アラート
低リスク	リスクが中または高ではないサイト。これらのサイトは最低 90 日間良性の活動を見せています。 デフォルトおよび推奨ポリシーアクション:**Allow** [許可]
新しく登録されたドメイン	過去 32 日以内に登録されたサイトを識別します。新しいドメインは、悪意のあるキャンペーンツールとして頻繁に使用されます。  新しく登録されたドメインは、意図的にまたはドメイン生成アルゴリズムによってしばしば生成され、悪意のある活動に使用されます。この*URL*カテゴリをブロックするのがベストプラクティスです。 デフォルトのポリシーアクション:アラート 推奨されるポリシー アクション:ブロック

不正な URL カテゴリ

以下のURLカテゴリは、悪意のあるコンテンツや搾取的なコンテンツ、挙動を識別するため、ブロックすることを強く推奨します。

- コマンドと制御
- 著作権侵害
- ダイナミック**DNS**
- 過激主義
- グレイウェア
- マルウェア
- 新しく登録されたドメイン
- パーク
- **phishing**
- プロキシ回避とアノニマイザ
- 疑わしい
- ランサムウェア
- スキャン活動
- **unknown**

ブロックする代わりにアラートを出すカテゴリでは、ユーザーがサイトコンテンツと対話する方法を厳格に制御できます。例えば、研究目的の開発者ブログやクラウドストレージサービスなど、必要なリソースへのアクセスをユーザーに許可しますが、ウェブベースでの脅威にさらされる可能性を減らすために次の予防策を講じます。

- アンチスパイウェア、脆弱性対策、ファイル遮断の ベストプラクティスに従ってください。危険なファイルタイプのダウンロードをブロックし、警告を出しているサイトの難読化されたJavaScriptをブロックすることが保護手段となります。
- URL カテゴリに基づく ターゲット復号化 です。高リスクと中リスクのサイトを復号化することから始めることを推奨します。
- 応答ページを表示して、ユーザーに高リスクおよび中リスクのサイトにアクセスしたことを知らせます。ユーザーにアクセスしようとしているサイトが悪意のある可能性があることを警告し、そのサイトにアクセスする場合の予防策についてアドバイスします。
- 高リスクおよび中リスクのサイトを含むサイトにユーザーが企業の資格情報を送信するのをブロックして、認証情報フィッシングを防止します。

次の表にプライベートIPアドレスを除き、PAN-DBが悪意のあるカテゴリと見なし、デフォルトでブロックするカテゴリを示します。プライベート IP アドレス (およびホスト) はホスト環境に固有であり、PAN-DB からは見えません。その結果、Palo Alto Networksはこのカテゴリのサイトにリスク評価を割り当てません。

カテゴリ	デフォルト アクション
コマンドアンドコントロール	ブロック
グレイウェア	
マルウェア	
フィッシング	
ランサムウェア	
スキャン アクティビティ	
プライベート **IP** アドレス	許可済み (デフォルトのアクションなし)

URL フィルタリングのユース ケース

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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

Webページへのアクセスを強制するには、特定のサイトをブロックして許可するだけでなく、多くの方法があります。たとえば、URL ごとに複数のカテゴリを使用して、ユーザーがサイトにアクセスできるようにしますが、企業の認証情報の送信やファイルのダウンロードなどの特定の機能をブロックできます。URL カテゴリを使用して、認証、復号化、QoS、セキュリティなどのさまざまなtypes of policy（ポリシータイプ）を適用することもできます。

URL フィルタリングを展開するさまざまな方法の詳細については、以下をお読みください。

URL カテゴリに基づいた Web アクセスの制御

URLカテゴリのアクションを指定し、プロファイルをセキュリティ ポリシー ルールに関連付けるURLフィルタリング プロファイルの作成を行うことができます。ファイアウォールは、プロファイルの設定に基づいて、トラフィックに対してポリシーを適用します。たとえば、すべてのゲームのWebサイトをブロックするには、URLフィルタリング プロファイルでゲームカテゴリのブロック アクションを設定します。その後、Webアクセスを許可するセキュリティ ポリシー ルールにプロファイルを添付します。

マルチカテゴリ URL フィルタリング

すべての URL には最大 4 つのカテゴリを含めることができます。これには、サイトが脅威にさらされる可能性を示すリスクカテゴリが含まれます。よりきめ細かいURL分類により、ウェブアクセスへの基本的な「ブロックまたは許可」アプローチ以上のことができます。代わりに、ビジネス上必要とされていて、サイバー攻撃の一部として使用される可能性が高いオンライン コンテンツとユーザーがどのように相互作用するかを制御できます。

たとえば、特定の URL カテゴリは組織にとって危険であると考えるかもしれませんが、貴重なリソースまたはサービス（クラウド ストレージ サービスやブログなど）も提供するため、完全にブロックすることを躊躇します。これで、ユーザーがこれらの種類のカテゴリに分類されるサイトにアクセスできるようにしながら、トラフィックを復号化して検査し、コンテンツへの読み取り専用アクセスを強制することができます。

また、**Category Match** を選択し、新しいカテゴリで構成される 2 つ以上の PAN-DB カテゴリを指定することで、カスタム URL カテゴリを定義することもできます。複数のカテゴリからカスタムカテゴリを作成すると、カスタム URL カテゴリオブジェクトで指定されたすべてのカテゴリに一致する Web サイトまたはページの適用をターゲットにできます。

URL カテゴリに基づいて企業の認証情報の送信をブロックまたは許可する

資格情報フィッシングを防止する を有効にして、サイトへの企業資格情報の送信をファイアウォールで検出し、URL カテゴリに基づいて送信を制御します。ユーザーが悪意のあるサイトや信頼されていないサイトに認証情報を送信するのをブロックし、ユーザーが未知のサイトで企業の認証情報を入力する際に警告を発し、企業外のサイトで企業の認証情報を再利用する際は警告し、ユーザーが企業のサイトや確認済みのサイトに認証情報を送信するのを明示的に許可します。

セーフサーチ設定の適用

多くの検索エンジンには、検索結果からアダルト画像やアダルト動画を除外するセーフ サーチ設定が備わっています。エンドユーザーが厳格なセーフサーチ設定を使用していない場合にファイアウォールに検索結果をブロックさせたり、ユーザーのセーフサーチを透過的に有効化したりできます。ファイアウォールは次の各プロバイダーのセーフ サーチをサポートしています。Google、Yahoo、Bing、Yandex、YouTube。セーフ サーチの適用の使用を開始する方法をご覧ください。

特定のサイトへのパスワード アクセスを実施

特定のユーザーがサイトにアクセスすることを許可しながら、ほとんどのユーザーに対してサイトへのアクセスをブロックできます。特定のサイトへのパスワードアクセスを許可する方法を参照してください。

特定の **URL** カテゴリからのリスクの高いファイルのダウンロードをブロック

ファイルブロックプロファイルがアタッチされたセキュリティポリシールールを作成することで、特定のURLカテゴリからの高リスクのファイルダウンロードをブロックできます。

URL カテゴリに基づいたセキュリティ、復号化、認証、**QoS**ポリシーの適用

URL カテゴリに基づいて、さまざまなタイプのファイアウォール ポリシーを適用できます。たとえば、復号化を有効にしたが、特定の個人情報を復号化から除外したいとします。この場合、URL カテゴリ *financial-services* および *health-and-medicine* に一致する Web サイトを復号化から除外する Decryption ポリシー ルールを作成できます。他の例では、QoS ポリシーで *streaming-media* という URL カテゴリを使用して、このカテゴリに分類される Web サイトに対して帯域幅の制御を適用できます。

以下の表では、URL カテゴリを一致条件として受け入れるポリシーについて説明します。

ポリシーのタイプ	詳説
復号	URL カテゴリを使用して復号化を段階的に導入し、機密情報や個人情報を含む可能性のある URL カテゴリを

ポリシーのタイプ	詳説
	復号化から除外することもできます（金融サービスや健康と医療など）。 最も危険なトラフィックを最初に復号化する計画 (ゲームや危険度の高いなどの悪意のあるトラフィックを収容する可能性が最も高い URL カテゴリ) し、経験を積むにつれてさらに復号化を行います。あるいは、ビジネスに影響を与えない URL カテゴリを最初に復号化します (問題が発生してもビジネスに影響を与えない) などのニュース フィード。どちらの場合も、いくつかの URL カテゴリの暗号化を解除し、ユーザーからのフィードバックを聞き、レポートを実行して、復号化が期待どおりに機能していることを確認し、さらにいくつかの URL カテゴリを徐々に復号化します。技術的な理由で復号化できない、または復号化しないことを決めた多売に、復号化から除外するために復号化除外の作成を計画します。  *URL* カテゴリに基づくトラフィックの復号化は、*URL*フィルタリングとDecryption（復号化）の両方のベストプラクティスです。
認証	特定のカテゴリへのアクセスが許可される前に、ユーザーが確実に認証されるようにするために、URL カテゴリを認証ポリシールールの一致条件として 関連付けることができます。
QoS	URL カテゴリを使用して、特定の Web サイトのカテゴリのスループット レベルを割り当てることができます。たとえば、*streaming-media* カテゴリを許可するが、QoS ポリシー ルールに URL カテゴリを追加することでスループットを制限できます。
セキュリティ	URLカテゴリを一致条件として使用することも、カテゴリごとにアクションを指定するURLフィルタリングプロファイルを作成してセキュリティポリシールールに関連付けることもできます。

ポリシーのタイプ	詳説

	URLカテゴリを一致基準として使用する方法と***URL***フィルタリング プロファイルをセキュリティポリシー ルールに適用する
	• *URL*カテゴリを一致基準として使用するのは、次のような場合です。
	  • URLカテゴリ強制の例外を作成するには。
	  • カスタムまたは定義済みの*URL*カテゴリに特定のアクションを割り当てるには。たとえば、個人サイトとブログのカテゴリのサイトへのアクセスを許可するセキュリティポリシールールを作成できます。
	• *URL*フィルタリング プロファイルは、次のような場合に使用します。
	  • *URL*フィルタリング ログに*URL*カテゴリへのトラフィックを記録するには
	  • また、特定のカテゴリのトラフィックに対するアラートなど、より多くのアクションを指定することもできます。
	  • ユーザーがブロックされたウェブサイトまたはブロック継続ウェブサイトにアクセスしたときに表示される応答ページを構成するには。
	*URL*フィルタリング プロファイルでは、各*URL*カテゴリに指定されたアクションは、セキュリティ ポリシー規則で指定されたカテゴリ宛てのトラフィックにのみ適用されます。特定のプロファイルを複数のルールに適用することもできます。

ポリシーのタイプ	詳説
	たとえば、会社の IT セキュリティ グループにハッキングカテゴリへのアクセスが必要で、一方その他すべてのユーザーからそのカテゴリへのアクセスは拒否する場合は、以下のルールを作成する必要があります。 • IT セキュリティ グループにハッキングと分類されたコンテンツへのアクセスを許可するセキュリティポリシー ルール。このセキュリティポリシー ルールは、**Services/URL Category**（サービス/**URL** カテゴリ）タブの ハッキングカテゴリと **Users**（ユーザー）タブの IT セキュリティ グループを参照します。 • すべてのユーザーに一般的な Web アクセスを許可する別のセキュリティポリシー ルール。このルールに、ハッキングカテゴリをブロックするURLフィルタリング プロファイルを関連付けます。 ハッキングをブロックするポリシーの前に、ハッキングへのアクセスを許可するポリシーを配置する必要があります。これは、ファイアウォールがセキュリティポリシールールを上から評価するため、セキュリティグループに属するユーザーが *hacking* サイトにアクセスしようとすると、ファイアウォールはアクセスを許可するポリシー ルールを評価し、ユーザーにアクセスを許可するためです。ファイアウォールは、ハッキングサイトへのアクセスをブロックする一般的な Web アクセス ルールに対してその他すべてのグループのユーザーを評価します。

URL フィルタリングの設定

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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

「URLフィルタリングの基本」の概念を理解したら、URLフィルタリングを開始する準備が整いました。Advanced URL Filteringライセンスのアクティベーション (該当する場合) から構成のテストまで、この章では効果的なURLフィルタリングの導入に必要な内容について説明します。展開を最大限に活用するには、URLフィルタリングのベストプラクティスに従ってください。

- 高度なURLフィルタリングライセンスを有効にする
- URL フィルタリングを開始する
- URL フィルタリングの設定
- インライン分類の設定
- URL カテゴリの例外
- URL フィルタリングのベストプラクティス
- テスト URL フィルタリング構成

Advanced URL Filteringライセンスをアクティベートする

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)	❑ Advanced URL Filteringライセンス (またはレガシーURLフィルタリングライセンス) 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

Advanced URL Filteringサブスクリプションは、リアルタイムのURL分析とマルウェア防止を提供します。Palo Alto Networksが開発した高性能URLルックアップ用のURLフィルタリングデータベースであるPAN-DBアクセスに加えて、悪意のあるURLやIPアドレスに対するカバレッジも提供します。

Advanced URL Filtering機能は、次世代ファイアウォール (仮想およびオンプレミス) AWS用クラウド NGFW Strata Cloud Manager、Prisma Access (Managed by Panorama)、および Azure 用クラウド NGFW で使用できます。ただし、次世代ファイアウォールとAzure向けCloud NGFWにはAdvanced URL Filteringサブスクリプションが必要ですが、すべての Prisma AccessCloud NGFW for AWSライセンスにはAdvanced URL Filtering機能が含まれています。

URL フィルタリングをサポートしている Palo Alto Networks の各プラットフォームとのAdvanced URL Filtering機能の互換性を確認するには、URLフィルタリングサポートを確認してください。

- Strata Cloud Manager
- PAN-OS & Panorama

高度なURLフィルタリングライセンス（Strata Cloud Manager）を有効化

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

[**PAN-OS & Panorama**]タブに切り替え、ガイダンスに従ってライセンス認証を行います。

Strata Cloud Managerを使っている場合:

❑ URLフィルタリングライセンスを検証します。

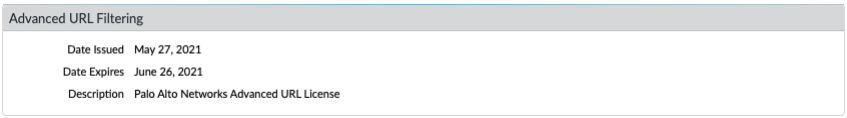
❑ 高度な URL フィルタリングの使用を開始する。

高度なURLフィルタリングライセンスの有効化（PAN-OS & Panorama）

STEP 1 | Advanced URL Filteringライセンスを取得してインストールします。

Advanced URL Filtering ライセンスには、*PAN-DB* へのアクセスが含まれます。ライセンスの有効期限が切れると、ファイアウォールはすべての*URL*フィルタリング機能、*URL*カテゴリの適用、および*URL*クラウドルックアップの実行を停止します。また、有効なライセンスをインストールするまで、他のすべてのクラウドベースの更新プログラムは機能しません。

1. **Device (デバイス) > Licenses (ライセンス)** の順に選択し、License Management (ライセンス管理) セクションで、ライセンスのインストール方法を選択します。
   - ライセンス サーバーからライセンス キーを取得
   - 認証コードを使用した機能のアクティベーション
2. [Advanced URL Filtering]セクションの[**Date Expires (日付の有効期限)**]フィールドに有効な日付が表示されていることを確認します。



*Advanced URL Filtering*ライセンスをアクティベートすると、*PAN-DB* および*Advanced URL Filtering*のライセンス資格がファイアウォールに正しく表示されないことがあります – これは表示の異常であり、ライセンスの問題ではなく、サービスへのアクセスには影響しません。次の *CLI* コマンドを使用して、ファイアウォールのライセンスを更新して表示の問題を修正できます。ライセンス取得を要求します。

STEP 2 | 最新の PAN-OS コンテンツ リリース をダウンロードしてインストールします。PAN-OS アプリケーションと脅威コンテンツリリース 8390-6607以降では、PAN-OS 9.x 以降を動作するファイアウォールが、Advanced URL Filteringで導入されたリアルタイム検出カテゴリを使用して分類されたURLを識別できます。この更新プログラムの詳細については、「アプリケーション」および「脅威コンテンツのリリース ノート」を参照してください。また、Palo Alto Networks のサポート ポータル上、あるいはファイアウォールの Webインターフェースで直接、アプリケーションおよび脅威に関するコンテンツ リリースノートを確認できます。**Device (デバイス) > Dynamic Updates (ダイナミック更新)** を選択し、特定のコンテンツ リリースのバージョンについての Release Note (リリースノート) を開いてください。

最新のコンテンツ リリース バージョンに更新する場合は、 のベスト プラクティスに従ってアプリケーションと脅威のコンテンツ更新 を更新します。

STEP 3 | アプリケーションおよび脅威のダイナミック更新をダウンロードするようにファイアウォールをスケジュールします。

アンチウイルス、アプリケーションおよび脅威を含むコンテンツの更新を受信するには、脅威防御ライセンスが必要です。

1. **Device**（デバイス） > **Dynamic Updates**（動的更新）を選択します。
2. Applications and Threats [アプリケーションおよび脅威]セクションの Schedule [スケジュール]フィールドで、**None** [なし]リンクをクリックし、定期的な更新をスケジュールします。

   ファイアウォールからインターネットに直接アクセスできる場合、ダイナミック更新のみをスケジュールできます。セクションで更新がすでにスケジュールされている場合、リンク テキストにスケジュール設定が表示されます。

   アプリケーションおよび脅威更新には、セーフ サーチの適用に関連する URL フィルタリングの更新が含まれていることがあります。

次のステップ：

1. URLフィルタリング プロファイル を設定して、組織の Web 利用ポリシーを定義します。
2. URL フィルタリング構成をテストします。

URL フィルタリングを開始する

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)	❑ Advanced URL Filteringライセンス (またはレガシーURLフィルタリングライセンス) 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URLフィルタリングを始める最初のステップは、ネットワーク上のユーザーのWebアクティビティパターンを理解することです。

これらのパターンを安全に観察するために、以下のことを推奨いたします。

- ❑ Palo Alto Networksの定義済みURLカテゴリを確認する。
- ❑ Test A SiteエンジンにURLを入力し、PAN-DBがどのように分類するかを確認します。
- ❑ 大抵のカテゴリについて警告を出す (おおよそ) パッシブな URL フィルタリング プロファイルを作成します。URLカテゴリのアラート設定を選択すると、ファイアウォールはそのカテゴリへのトラフィックをログに記録します。すると、ユーザーがアクセスしているサイトが表示され、URLカテゴリや特定のサイトに適したサイトアクセスを決定できます。

  すべての*Web*アクティビティで

  アラートが発生すると、大量のログファイルが作成される可能性があります。結果として、初期導入の一部としてのみこれを行う場合があります。その時点では、*URL*フィルタリング プロファイルで***Log container page only***(コンテナ ページのみロギング)オプションを有効にすると、カテゴリに一致するメイン ページのみがログに記録され、コンテナ ページ内にロードされる可能性のある後続のページ/カテゴリは記録されないため、*URL*フィルタリング ログを削減することもできます。
- ❑ 好ましくないことが分かっているURLカテゴリ (マルウェア、C2、フィッシング) をブロックします。

- Strata Cloud Manager
- PAN-OS & Panorama

Advanced URL Filteringを開始する (Strata Cloud Manager)

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

*[**PAN-OS & Panorama**]* タブに切り替えて、そこにあるガイダンスに従います。

Strata Cloud Managerをお使いの場合は、こちらに進んでください。

STEP 1 | Test A Siteを使用して、PAN-DBが特定のウェブサイトをどのように分類しているかを確認します。

プラットフォームを使用して、誤って分類されたと思われるすべてのウェブサイトの分類変更を要求することもできます。

STEP 2 | すべてのカテゴリでアラートを発するパッシブURLアクセス管理プロファイルを作成します。

ファイアウォールは、*allow* (許可)以外のアクションを持つURLカテゴリのWebサイトに対してURLフィルタリング ログ エントリを生成します。

1. **[Manage (管理)] > [Configuration (設定)] > [Security Services (セキュリティサービス)] > [URL Access Management (URL**アクセス管理**)]**を順に選択します。
2. [URL Access Management Profiles (URLアクセス管理プロファイル)]で、ベスト プラクティス プロファイルの横にあるチェックボックスをオンにし、プロファイルを複製します。

   複製されたプロファイルは、`best-practices-1`という名前のプロファイルの下に表示されます。
3. **best-practices-1**プロファイルを選択し、名前を変更します。たとえば、`url-Monitoring`と名前を変更します。

STEP 3 | マルウェア、コマンド アンド コントロール、フィッシングを除くすべてのカテゴリについて警告します。これらは引き続きブロックする必要があります。

1. **[Access Control (**アクセス制御**)]**で、すべてのカテゴリを選択し、[マルウェア]、[コマンドアンドコントロール]、[フィッシング]を除外します。
2. カテゴリがハイライト表示された状態で、**[Set Access (**アクセスの設定**)]**をクリックし、**[Alert (**アラート**)]**を選択します。
3. マルウェア、コマンド アンド コントロール、フィッシングなどの既知の危険な URL カテゴリへのアクセスをブロックします。
   - phishing
   - ダイナミックDNS
   - unknown
   - 過激主義
   - 著作権侵害
   - プロキシ回避とアノニマイザ
   - 新しく登録されたドメイン

- グレイウェア
- パーク

4. プロファイルを保存します。

STEP 4 | URLアクセス管理プロファイルを、トラストゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティポリシールールに適用します。

URLアクセス管理プロファイルは、セキュリティポリシー規則が参照するプロファイルグループに含まれている場合にのみアクティブになります。

手順に従って、URLアクセス管理プロファイル（および任意のセキュリティプロファイル）をアクティブにします。

*URL*アクセス管理プロファイルを追加するセキュリティポリシールールのソースゾーンが、保護された内部ネットワークに設定されていることを確認します。

STEP 5 | 設定をコミットするには、**[Push Config (設定をプッシュ)]**を実行します。

STEP 6 | URLログをチェックして、ユーザーがアクセスしているWebサイトのカテゴリを確認します。ブロックされたウェブサイトも記録されます。

ログの表示およびレポートの生成の詳細は、Web アクティビティのモニターを参照してください。

[アクティビティ] > [ログ ビューア] > URLを選択します。URLフィルタリング レポートでは、24時間のWebアクティビティを表示できます。

STEP 7 | 次のステップ：

- 許可またはブロックしないものについては、リスク カテゴリを使用して、Web サイトの安全性に基づいた簡単なポリシーを作成します。PAN-DBはすべてのURLをリスク レベル(高、中、低)で分類します。高および中リスクのあるサイトは悪意があると確定されているわけではありませんが、悪意のあるサイトと密接に関連しています。例えば、悪意のあるサイトと同じドメインであったり、つい最近まで悪意のあるコンテンツをホストしていたりする可能性があります。

  安全上の懸念があるサイトであっても、ユーザーアクセスを許可したい場合があるため、リスクの高いサイトでのユーザーの操作を制限する予防策を講じることができます。 (例えば開発者のブログを調査目的で使用することを許可しようとしますが、ブログは一般的にマルウェアをホストしていることが知られているカテゴリです）。
- URLフィルタリングをUser-IDとペアにして、組織または部門に基づいてWebアクセスを制御し、認可されていないサイトへの企業の認証情報の送信をブロックします。
  - URLフィルタリングは、サイトカテゴリに基づいてサイトへの企業の認証情報の送信を検出することにより、認証情報の盗難を防ぎます。ユーザーが悪意のあるサイトや信頼されていないサイトに認証情報を送信するのをブロックし、ユーザーが未知のサイトで企業の認証情報を入力する際、および企業外のサイトで企業の認証情報を再利用する際に警告し、ユーザーが企業のサイトに認証情報を送信するのを明示的に許可します。
  - パッシブURLアクセス管理プロファイルを使用してセキュリティ ポリシー ルールを追加または更新し、マーケティングやエンジニアリングなどの部門ユーザー グループに

適用します。部門のアクティビティを監視し、部門メンバーからのフィードバックを取得して、彼らの仕事に不可欠なWebリソースを把握します。

- URLフィルタリングを活用して攻撃対象領域を減らすあらゆる方法を検討してください。例えば、学校ではURLフィルタリングを使用して、生徒に厳格な安全検索を強制する場合があります。あるいは、セキュリティオペレーションセンターがある場合、調査のために侵害されたサイトや危険なサイトへのパスワードアクセスを脅威アナリストにのみ許可する場合もあります。
- URLフィルタリングのベストプラクティスに従います。

Advanced URL Filteringを開始する (PAN-OS&Panorama)

STEP 1 | Test A Siteを使用して、PAN-DBが特定のウェブサイトをどのように分類しているかを確認します。

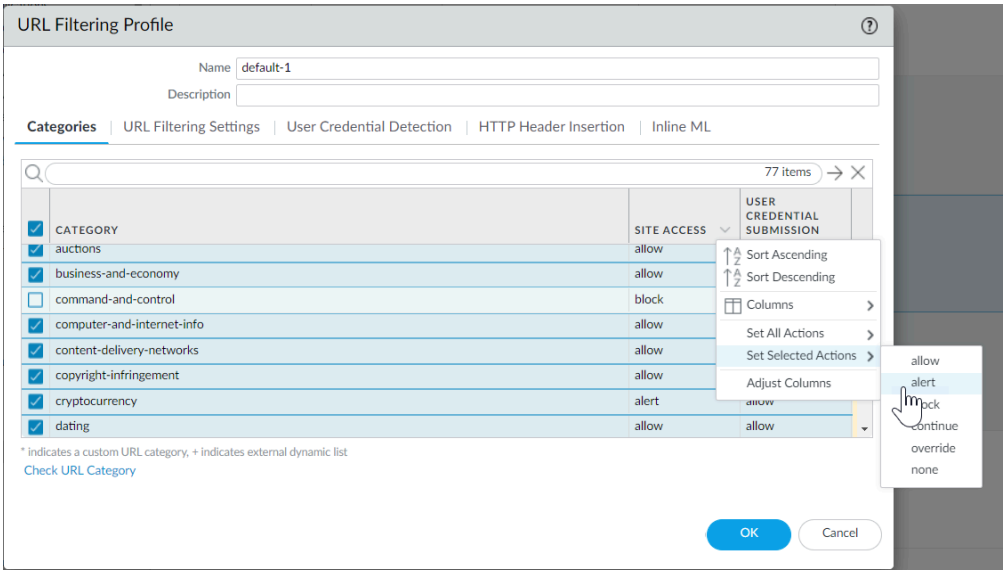
プラットフォームを使用して、誤って分類されたと思われるすべてのウェブサイトの分類変更を要求することもできます。

STEP 2 | すべてのカテゴリについて警告を出すパッシブなURLフィルタリング プロファイルを作成します。

1. **[Objects (オブジェクト)] > [Security Profiles (セキュリティ プロファイル)] > [URL Filtering (URLフィルタリング)]**の順に選択します。
2. デフォルト プロファイルを選択し、**Clone[コピー]**をクリックします。新しいプロファイルには **default-1** という名前が付けられます。
3. **default-1** プロファイルを選択して、名前を変更します。たとえば、URL-Monitoring と名前を変更します。

STEP 3 | ブロック状態を維持しなければならないマルウェア、コマンド アンド コントロール、フィッシングを除き、すべてのカテゴリのアクションを **alert (アラート)** に設定します。

1. すべての URL カテゴリをリストするセクションでは、すべてのカテゴリを選択して、マルウェア、command-and-control およびフィッシングを解除します。
2. *[アクション]* 列のヘッダーの右にマウスを重ね、下向き矢印を選択して、**[選択したアクションの設定]** を選択し、**[alert]** を選択します。



3. 既知の危険な URL カテゴリへのアクセスを **Block**（ブロック）します。

   マルウェア、フィッシング、ダイナミック *DNS*、未知、コマンド&コントロール、過激思想、著作権侵害、プロキシ回避・アノニマイザー、新しく登録されたドメイン、グレイウェアおよびドメインパーキングに使用された *URL* カテゴリへのアクセスをブロックします。

4. **OK** をクリックしてプロファイルを保存します。

STEP 4 | URLフィルタリングプロファイルを、トラストゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティポリシールールに適用します。

*URL*アクセス管理プロファイルを追加するセキュリティポリシールールのソースゾーンが、保護された内部ネットワークに設定されていることを確認します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。次に、変更するセキュリティポリシールールを選択します。
2. アクションタブでプロファイル設定を編集します。
3. [プロファイルタイプ]で[プロファイル]を選択します。プロファイルのリストが表示されます。
4. **[URL**フィルタリングプロファイル]で、作成したプロファイルを選択します。
5. **OK** をクリックして変更内容を保存します。

STEP 5 | 設定を **Commit**（コミット）します。

STEP 6 | URL フィルタリング ログを表示して、ユーザーがアクセスしているすべての Web サイトのカテゴリを確認します。また、ブロックすることにしたカテゴリはログに記録されます。

ログの表示およびレポートの生成の詳細は、Web アクティビティのモニターを参照してください。

[Monitor (モニター)] > [Logs (ログ)] > [URL Filtering (URLフィルタリング)]を選択します。アクションが **allow (許可)** 以外に設定されているカテゴリに含まれる URL フィルタリング データベースに存在するすべてのウェブサイトでログ エントリが作成されます。URL フィルタリング レポートでは、24 時間の Web アクティビティを表示できます。(**[Monitor (監視)] > [Logs (ログ)]**)。

STEP 7 | 次のステップ：

- PAN-DB はすべての URL を最大 4 つのカテゴリに分類し、すべての URL にはリスク カテゴリ（高、中、低）があります。高および中リスクのあるサイトは悪意があると確定されているわけではありませんが、悪意のあるサイトと密接に関連しています。例えば、悪意のあるサイトと同じドメインであったり、つい最近まで悪意のあるコンテンツをホストしていたりする可能性があります。許可またはブロックしていないものすべてについて、リスクカテゴリを使用して、Webサイトの安全性に基づいた簡単なポリシールールを作成できます。

  安全上の懸念があるサイトであっても、ユーザーアクセスを許可したい場合があるため、リスクの高いサイトでのユーザーの操作を制限する予防策を講じることができます。 (例えば開発者のブログを調査目的で使用することを許可しようとしますが、ブログは一般的にマルウェアをホストしていることが知られているカテゴリです）。
- URLフィルタリングをUser-IDとペアにして、組織または部門に基づいてWebアクセスを制御し、認可されていないサイトへの企業の認証情報の送信をブロックします。
  - URLフィルタリングは、サイトカテゴリに基づいてサイトへの企業の認証情報の送信を検出することにより、認証情報の盗難を防ぎます。ユーザーが悪意のあるサイトや信頼されていないサイトに認証情報を送信するのをブロックし、ユーザーが未知のサイトで企業の認証情報を入力する際、および企業外のサイトで企業の認証情報を再利用する際に警告し、ユーザーが企業のサイトに認証情報を送信するのを明示的に許可します。
  - パッシブ URL フィルタリング プロファイルを使用してセキュリティ ポリシー ルールを追加または更新し、部門のユーザー グループ (たとえば、マーケティングまたはエンジニアリング (**[Policies (ポリシー)] > [Security (セキュリティ)] > [User (ユーザー)]**) に適用されるようにします。部門の活動を監視し、部門のメンバーからフィードバックを得て、部門のメンバーが行う作業に不可欠な Web リソースを理解します。
- URLフィルタリングを活用して攻撃対象領域を減らすあらゆる方法を検討してください。例えば、学校ではURLフィルタリングを使用して、生徒に厳格な安全検索を強制する場合があります。あるいは、セキュリティオペレーションセンターがある場合、調査のために侵害されたサイトや危険なサイトへのパスワードアクセスを脅威アナリストにのみ許可する場合もあります。
- URLフィルタリングのベストプラクティスに従います。

URL フィルタリングの設定

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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URLフィルタリングの展開を計画したら、ユーザーがアクセスするWebサイトの種類について基本的な理解を深める必要があります。この情報を使用して、ファイアウォールが特定のURLカテゴリへのトラフィックを処理する方法を定義するURLフィルタリング プロファイルを作成します。また、ユーザーが企業の資格情報を送信できるサイトを制限したり、厳格なセーフサーチを実施したりすることもできます。これらの設定を有効にするには、Webアクセスを許可するセキュリティ ポリシー ルールにURLフィルタリング プロファイルを適用します。

- Strata Cloud Manager
- PAN-OS & Panorama

URLフィルタリングの設定 Strata Cloud Manager)

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

*[**PAN-OS & Panorama**]* タブに切り替えて、そこにあるガイダンスに従います。

Strata Cloud Managerをお使いの場合は、こちらに進んでください。

URLフィルタリングはStrata Cloud Managerでは*URL*アクセス管理と呼ばれています

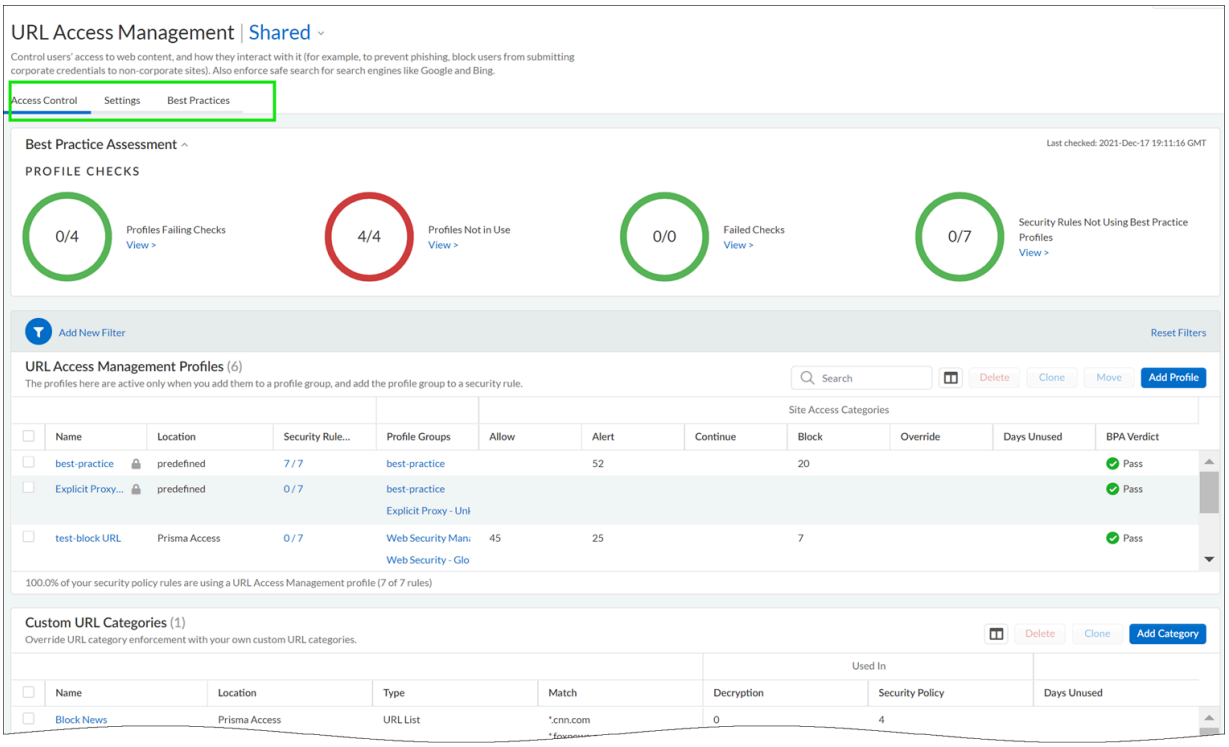
STEP 1 | Prisma Access契約が［高度なURLフィルタリング］をカバーしていることを確認します。

- ［Manage (管理)］>［Service Setup (サービスセットアップ)］>［Overview (概要)］>［Licenses (ライセンス)］に進み、サブスクリプションに含まれている内容を確認します。

STEP 2 | URLアクセス管理ダッシュボードをご覧ください。

[Manage (管理)] > [Configuration (設定)] > [Security Services (セキュリティサービス)] > [URL Access Management (URLアクセス管理)]を順に選択します。

［**Access Control (アクセス制御)**］、［**Settings (設定)**］、および［**Best Practices (ベストプラクティス)**］タブ間を移動し、利用可能なURLフィルタリング機能を確認します。



STEP 3 | URLフィルタリングの全般設定を確認してカスタマイズします。

ダッシュボードの[設定]に移動し、お使いのPrisma Access環境全体に適用される次のようなURLフィルタリングのデフォルト設定を確認します。

- URLフィルタリングのタイムアウトとルックアップの設定
- URLフィルタリングは特定の管理者のオーバーライド
- URLフィルタリング応答ページ
- リモートブラウザ分離(RBI)設定

カスタム***URL***カテゴリまたは外部動的リストの***URL***にエンドトークンを自動的に付加します

（*PAN-OS 10.1以前*）*URL*リストタイプのカスタム*URL*カテゴリや外部動的リスト（*EDL*）に*URL*を追加し、末尾にスラッシュ（/）を付けないと、意図しない数の*URL*をブロックしたり許可したりする可能性があります。たとえば、***example.com***の代わりに***example.com***を入力すると、一致する*URL*が *example.com.website.info*または*example.com.br* に展開されます。*Prisma Access*は、カスタム *URL* カテゴリまたは*EDL*の*URL*の末尾に自動的にスラッシュを付加できます。これにより、***example.com***を入力した場合、*Prisma Access*は***example.com***と同様に扱い、ドメインとそのサブディレクトリのみが一致すると見なします。***[Settings (***設定***)]*** > ***[General Settings (***一般設定***)]***を開き、***[Append End Token to Entries (***エントリに終了トークンを付加する***)]***オプションを有効にします。

（*PAN-OS 10.2以降*）*Prisma Access*では、ドメインエントリの末尾に自動的にスラッシュが追加されます。

これらの設定は、デプロイメントタイプ(モバイルユーザ、リモートネットワーク、またはサービス接続)ごとにカスタマイズできます。

STEP 4 | URL アクセス管理プロファイルの作成

URLアクセス管理ダッシュボードで、プロファイルを追加し、引き続きウェブアクセス設定を指定します。

- ［**Access Control(**アクセス制御**)**］では、Webアクセスおよび使用状況ポリシーを定義できるURLカテゴリとリストを確認できます。デフォルトでは、**Site Access**（サイト アクセ

ス）権限と **User Credential Submission**（ユーザー証明書送信）権限は、すべてのカテゴリで **Allow**（許可）に設定されます。

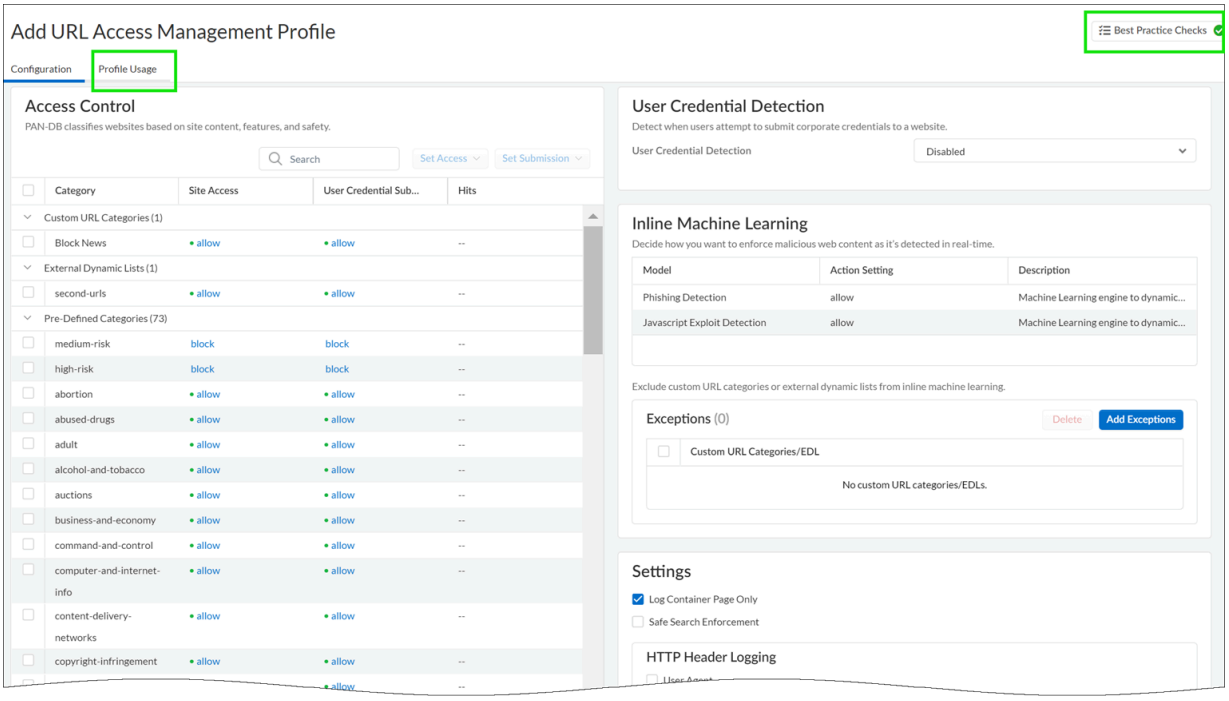
- URLカテゴリごとに、ユーザーが指定されたURLカテゴリのサイトにのみ資格情報を送信できるようにユーザー資格情報検出を設定します。
- **[セーフサーチ適用]**を有効にして、厳密なセーフサーチフィルタを適用します。
- 指定されたコンテンツタイプに一致するURLのみをログに記録するには、**[ログコンテナページのみ]**を有効にします。
- **HTTP**ヘッダーのロギングを有効にすると、サーバに送信された HTTP 要求に含まれる属性を表示できます。
- 詳細**URL**インライン分類を使用して、リアルタイムのWebページ分析を有効にして構成し、URL例外を管理します。
  - ローカルのインライン分類を有効にする-機械学習モデルを使用してURLトラフィックをリアルタイムで分析し、悪意のあるフィッシングの亜種やJavaScriptエクスプロイトがネットワークに侵入するのを検出して防止します。
  - クラウドのインライン分類を有効にする–ローカルのインラインMLで使用される分析エンジンを補完する機械学習ベースの検出器を使用して、疑わしいWebページ コンテ

ンツをクラウドに転送して補足分析を行うことで、URLのリアルタイム分析を可能にします。

- インライン機械学習アクションから除外する特定のWebサイトのURL例外を定義できます。

次のことに注意してください。

- ベスト・プラクティス・チェックがプロファイルに組み込まれており、構成をライブ評価できます。
- プロファイルの有効化が終了したら、プロファイルの使用状況を調べて、セキュリティポリシールールがプロファイルを参照しているかどうかを確認できます。



STEP 5 | URLアクセス管理プロファイルをセキュリティポリシールールに適用します。

URLアクセス管理プロファイルは、セキュリティポリシー規則が参照するプロファイルグループに含まれている場合にのみアクティブになります。

手順に従って、URLアクセス管理プロファイル（および任意のセキュリティプロファイル）をアクティブにします。必ず**[Push Config (**設定のプッシュ**)]**を行ってください

URLフィルタリングの設定 (PAN-OS & Panorama)

STEP 1 | URL フィルタリング プロファイルを作成します。

まだ行っていない場合は、最良の URL フィルタリング プロファイルを設定し、マルウェアあるいは悪意のあるコンテンツをホストしている *URL* から確実に保護されるようにします。

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。

STEP 2 | URL カテゴリ毎にサイト アクセスを定義します。

Categories (カテゴリ**)** を選択し、各 URL カテゴリ毎に Site Access (サイト アクセス) を設定します。

- その URL カテゴリ宛てのトラフィックを**allow**（許可）します。許可されたトラフィックは記録されません。
- ユーザーがアクセスしているサイトに可視性をもたらすには、**alert (**アラート**)** を選択します。そのカテゴリに一致するトラフィックは許可されますが、ユーザーがそのカテゴリのサイトにいつアクセスしたかを記録する URL フィルタリング ログが生成されます。
- そのカテゴリに一致するトラフィックへのアクセスを拒否し、ブロックされたトラフィックのロギングを有効にするには、**block (**ブロック**)** を選択します。
- **continue (**続行**)** を選択し、ユーザーに警告付きのページを表示し、サイトにアクセスするためにカテゴリーの中から **Continue(**続行**)** をクリックするよう求めます。
- ユーザーが設定されたパスワードを入力した場合にのみアクセスを許可するには、**override** を選択します。詳細については、特定のサイトへのパスワード アクセスを許可するを参照してください。

STEP 3 | 許可する URL カテゴリに属すウェブサイトに対して行う、企業の認証情報の送信を検知する URL フィルタリング プロファイルを設定します。

最高のパフォーマンスを維持して誤検出の頻度を下げるために、マルウェアあるいはフィッシングのコンテンツをホストしていることが一度も判明していないサイトに関連付けられた *App-ID*™ について、ファイアウォールは自動的に認証情報の送信のチェックをスキップします（対応するカテゴリでチェックを有効にしている場合でも）。ファイアウォールが認証情報のチェックをスキップするサイトのリストは、アプリケーションおよび脅威コンテンツ更新を通じて自動的に更新されます。

1. **User Credential Detection (**ユーザーの認証情報検出**)** を選択します。
2. ユーザー資格情報検出 ドロップダウンから、Web ページの企業資格情報の送信 を確認する方法のいずれかを選択します。
   - **Use IP User Mapping**（**IP** ユーザー マッピングの使用）–企業のユーザー名送信が正当なものであり、セッションの送信元 IP アドレスにログインしたユーザーにユーザー名が一致することが確認されます。ファイアウォールは、送信されたユーザー名を IP アドレスからユーザー名へのマッピング テーブルと照合します。Map IP アドレスからユーザー に説明されているユーザー マッピングメソッドを使用できます。
   - **Use Domain Credential Filter**（ドメイン認証情報フィルタを使用）–有効な企業ユーザー名とパスワード送信をチェックし、ユーザー名が、ログイン ユーザーの IP アドレスに対応することを確認します。User-ID をセットアップしてこの方式を有効にする方法については、Windows ベースの User-ID エージェントを使用する認証情報検知を設定を参照してください。
   - グループ マッピングを使用する] - ユーザーをグループにマップする場合に設定されたユーザーからグループへのマッピング テーブルに基づいて有効なユーザー名の送信をチェックします

     グループ マッピングの場合、最も重要なアプリケーションにアクセスできる IT のようなグループなど、特定のグループ、あるいはディレクトリの **any (**いずれか**)** の部分に認証情報検知を割り当てることができます。

     この方法は、一意に構造化されたユーザー名を持たない環境では誤検知が発生しやすいため、価値の高いユーザー アカウントを保護するためにのみこの方法を使用する必要があります。
3. ファイアウォールが企業の認証情報送信の検知をロギングするために使用する **Valid Username Detected Log Severity (**有効なユーザー名が検知されたログの重大度**)** を設定します（デフォルトは中）。

STEP 4 | ローカルインライン分類を使用してフィッシングや悪意のあるJavaScriptをリアルタイムで検出するようにURLフィルタリングプロファイルを設定します。

STEP 5 | フィッシング認証を防止する資格情報 への URL カテゴリに基づいて、ユーザーがサイトに企業資格情報を送信できないようにすることを許可または禁止します。

マルウェアあるいはフィッシングのコンテンツをホストしていることが一度も判明していないサイトに関連付けられた *App-ID* については、そのカテゴリでチェックを有効にしている場合でも、ファイアウォールは自動的に認証情報の送信のチェックをスキップし、最高のパフォーマンスを維持して誤検出の頻度を下げます。ファイアウォールが認証情報のチェックをスキップするサイトのリストは、アプリケーションおよび脅威コンテンツ更新を通じて自動的に更新されます。

1. **Site Access (**サイト アクセス**)** を許可する各 URL カテゴリについて、**User Credential Submissions (**ユーザー証明書送信**)** をどのように扱いたいか選択します。
   - **alert** – ユーザーが Web サイトに資格情報を送信できるようにしますが、ユーザーがこの URL カテゴリのサイトに資格情報を送信するたびに URL フィルタリング アラート ログを生成します。
   - **allow (**許可**)**（デフォルト）–ユーザーが認証情報を Web サイトに送信することを許可します。
   - **block (**ブロック**)**–アンチフィッシング ブロックページを表示し、ユーザーが認証情報をウェブサイトに送信するのをブロックします。
   - **continue** – フィッシング対策の続行ページを表示します。このページでは、サイトにアクセスするには **[Continue (**続行**)]** をクリックする必要があります。
2. 許可するURLカテゴリに属すウェブサイトに対して行う、企業の認証情報の送信を検知するURLフィルタリング プロファイルを設定します。

STEP 6 | URLカテゴリの例外を定義して、URLカテゴリに関係なく、常にブロックまたは許可するWebサイトを指定します。

たとえば、URL フィルタリング ログを減らすには、企業の Web サイトを許可リストに追加して、それらのサイトのログが生成されないようにしたり、過度に使用されている Web サイトがあり、作業に関連していない場合は、そのサイトをブロック リストに追加できます。

カスタム URL カテゴリ用に構成されたポリシー アクションは、外部動的リスト内の一致する URL よりも優先的に適用されます。

ブロックリストの Web サイトへのトラフィックは、関連付けられたカテゴリのアクションにかかわらず、常にブロックされ、許可リストの URL へのトラフィックは常に許可されます。

適切な形式とワイルドカードの使用方法の詳細については、URLカテゴリの例外ガイドラインをご覧ください。

STEP 7 | セーフ サーチの適用を有効化します。

STEP 8 | URL フィルタリングイベントについて、ユーザーがアクセスしたページのみを記録します。

1. **URL Filtering Settings (ULR**フィルタリングセッティング**)**を選択し**Log container page only (**コンテナ ページのみロギング**)**（デフォルト）が有効にすることで、ファイア

ウォールはコンテナ ページ内にロードされた後続のページまたはカテゴリではなく、カテゴリに一致するメイン ページのみをログに記録します。

2. すべてのページおよびカテゴリのロギングを有効にするには、**Log container page only**（コンテナ ページのみロギング）オプションを無効にします。

STEP 9 | サポートされている 1 つ以上の HTTP ヘッダー フィールドで HTTP ヘッダーのロギングを有効にします。

URL Filtering Settings (URL フィルタリング設定**)** を選択し、ログに記録する以下のフィールドを 1 つ以上選択します。

- ユーザーエージェント
- リファラー
- **X-Forwarded-For (XFF)**

STEP 10 | URLフィルタリングプロファイルを保存します。

OK をクリックします。

STEP 11 | URLフィルタリングプロファイルを、トラストゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティポリシールールに適用します。

*URL*フィルタリングプロファイルを追加するセキュリティポリシールールのソースゾーンが、保護された内部ネットワークに設定されていることを確認します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。次に、変更するセキュリティポリシールールを選択します。
2. アクションタブでプロファイル設定を編集します。
3. [プロファイルタイプ] で [プロファイル] を選択します。プロファイルのリストが表示されます。
4. [**URL**フィルタリングプロファイル]で、作成したプロファイルを選択します。
5. **OK** をクリックして変更内容を保存します。

STEP 12 | 設定を **Commit**（コミット）します。

STEP 13 | URL フィルタリング構成をテストします。

STEP 14 | (ベストプラクティス) ファイアウォールが URL カテゴリ検索を実行している間、クライアント要求をブロックするには、**Hold client request for category lookup**（カテゴリ検索のクライアント要求を保持）を有効にします。

1. **Device (** デバイス**) > Setup (**設定**) > Content-ID**の順に選択します。
2. **Hold client request for category lookup**（カテゴリ検索のクライアント要求を保持）を選択します。
3. 変更を**Commit (**コミット**)**します。

STEP 15 | URL カテゴリ検索がタイムアウトするまでの時間を秒単位でセットします。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Content-ID** > **gear icon**（ギアアイコン）の順に選択します。
2. [カテゴリ検索タイムアウト **(**秒**)**] に数値を入力します。
3. **OK** をクリックします。
4. 変更を**Commit (**コミット**)**します。

インライン分類の設定

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)	☐ Advanced URL Filteringライセンス (またはレガシーURLフィルタリングライセンス) 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

インライン分類を有効にするには、インライン分類設定で構成されたURLフィルタリング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(基本セキュリティポリシーの設定を参照)。

URL フィルタリングのローカル インライン分類は、*VM-50* または *VM50L* 仮想アプライアンスでは現在サポートされていません。

- Strata Cloud Manager
- PAN-OS & Panorama

インライン分類の設定 (Strata Cloud Manager)

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

*[**PAN-OS & Panorama**]* タブに切り替えて、そこにあるガイダンスに従います。

Strata Cloud Managerをお使いの場合は、こちらに進んでください。

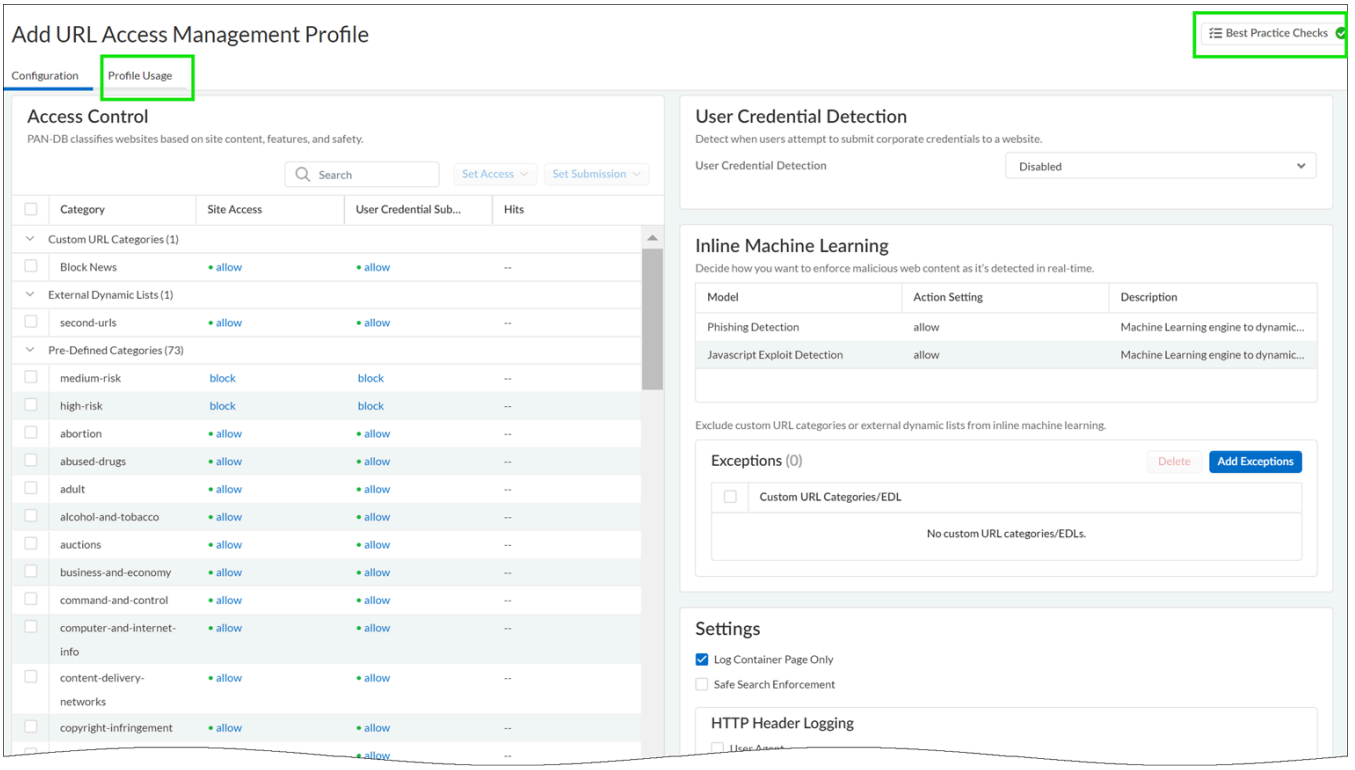
STEP 1 | URLアクセス管理プロファイルを更新または作成します。

1. **[Manage (管理)]** > **[Configuration (構成)]** > **[Security Services (セキュリティサービス)]** > **[URL Access Management (URL**アクセス管理**)]**に移動します。
2. URLアクセス管理ダッシュボードで、URLアクセス管理プロファイルまたは**[Add Profile (**プロファイルの追加**)]**を選択します。

   新しいプロファイルを作成する場合は、プロファイルでURLカテゴリのサイトアクセス（アクセス制御）などの設定を行います。「URLフィルタリングの設定(クラウド管理)」で、使用可能な設定について説明します。
3. [**URL**インライン分類の詳細]で、インライン分類タイプを選択します。

   どちらのオプションも、リアルタイムのウェブページ分析を可能にし、URL例外を管理します。

- クラウドのインライン分類を有効にする–ローカルのインラインMLで使用される分析エンジンを補完する機械学習ベースの検出器を使用して、疑わしいWebページ コンテンツをクラウドに転送して補足分析を行うことで、URLのリアルタイム分析を可能にします。
- ローカルのインライン分類を有効にする-機械学習モデルを使用してURLトラフィックをリアルタイムで分析し、悪意のあるフィッシングの亜種やJavaScriptエクスプロイトがネットワークに侵入するのを検出して防止します。
- 特定のウェブサイトをインライン機械学習アクションから除外するURL例外を定義することもできます。



4. プロファイルを保存します。

STEP 2 | URLアクセス管理プロファイルをセキュリティポリシールールに適用します。

URLアクセス管理プロファイル（および任意のセキュリティプロファイル）をアクティブにするには、プロファイルグループに追加し、セキュリティポリシー規則でプロファイルグループを参照します。

インライン分類の設定 (PAN-OS & Panorama)

*PAN-OS10.2*では、*URL*フィルタリング インライン*ML*機能の名前がインライン分類に変更されました。その結果、*PAN-OS 10.1*タスクでは*[URL Filtering inline ML (URL*フィルタリング インライン*ML)]*というフレーズが使用され、*PAN-OS 10.2*以降のタスクでは*[Inline Categorization (*インライン分類*)]*が使用されます。詳細については、PAN-OS 10.2のアップグレード/ダウングレードの考慮事項に記載されている、*URL*フィルタリング インライン*ML*エントリを参照してください。

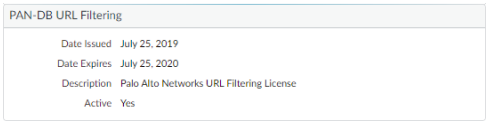
- PAN-OS 10.1
- PAN-OS 10.2以降

インライン分類の設定（PAN-OS 10.1）

STEP 1 | PAN-OS Web インターフェイスにログインします。

STEP 2 | 有効なレガシーURLフィルタリングまたは高度なURLフィルタリングのサブスクリプションがあることを確認します。

[Device (デバイス)] > [Licenses (ライセンス)]を順に選択し、URLフィルタリングライセンスが使用可能で期限切れになっていないことを確認します。

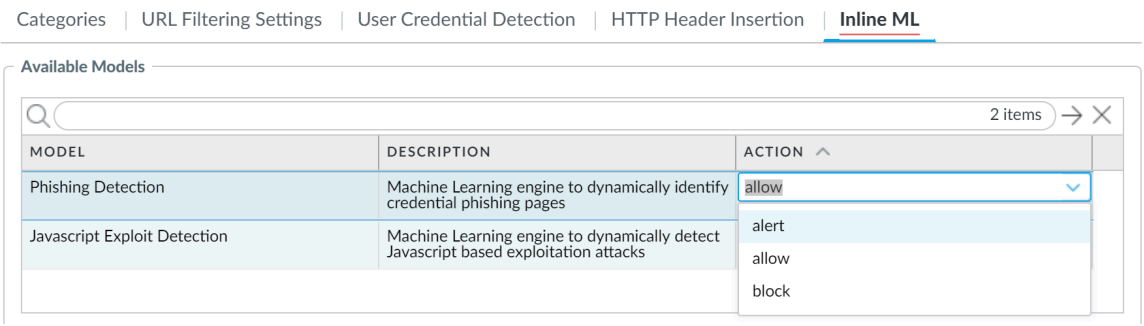


STEP 3 | URLフィルタリングプロファイルでURLフィルタリングインラインMLの設定を行います。

1. **[Objects (オブジェクト)] > [Security Profiles (セキュリティプロファイル)] > [URL Filtering (URL**フィルタリング**)]**を選択し、[URL Filtering profile (URLフィルタリングプロファイル)]を追加または選択します。
2. **[インライン**ML**]**を選択し、各インラインMLモデルに**[**アクション**]**を定義します。

   悪意のあるウェブページのコンテンツの種類ごとに、2つの分類エンジンが用意されています。**[**フィッシング**]**と**[JavaScript**エクスプロイト**]**を参照してください。

   - **Block (**ブロック**)**– ファイアウォールがフィッシング コンテンツを含む Web サイトを検出すると、ファイアウォールは URL フィルタリング ログ エントリを生成します。
   - **Alert (**アラート**)**–ファイアウォールはWebサイトへのアクセスを許可するとともに、URLフィルタリング ログエントリ も生成します。
   - **Allow (**許可**)**–ファイアウォールはWebサイトへのアクセスを許可し、URL フィルタリング ログ エントリを生成しません。



3. **OK** をクリックして変更内容を保存します。
4. 変更を **Commit (**コミット**)** します。

STEP 4 | (任意) 誤検知が発生した場合は、URLフィルタリング プロファイルにURLの例外を追加します。

例外を追加するには、URLフィルタリング プロファイルから外部動的リストを指定するか、URLフィルタリング ログからカスタムURLカテゴリにWebページ エントリを追加します。

1. **[Objects] > [**セキュリティ プロファイル**] > [URL** フィルタリング**]** の順に選択します。
2. 特定のURLを除外したいURLフィルタリング プロファイルを選択してから、**Inline ML (**インライン **ML)**を選択します。
3. URLタイプの既存の外部動的リストを追加します。使用可能なリストがない場合は、外部動的リストを新規作成します。
4. **OK** をクリックして変更内容を保存します。
5. 変更を **Commit (**コミット**)** します。

URL フィルタリング ログ エントリからファイル例外を追加します。

1. Select **Monitor (**監視**) > Logs (**ログ**) > URL Filtering (URL** フィルタリング**)** を選択し、**malicious-javascript (**悪意のある**javascript)** または **phishing** (フィッシング) のインライン ML 判定を含む URL エントリのためのログをフィルタリングします。例外を作成する URL の URL フィルタリング 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、**Inline ML Verdict (**インライン **ML** 判定**)** と隣にある **Create Exception (**例外を作成**)** を選択します。

3. URL 例外のカスタム カテゴリを選択し、**[OK]**をクリックします。

   新しい URL の例外は、**Objects (**オブジェクト **> Custom Objects (**カスタム オブジェクト**) > URL Category (URL** カテゴリ**)** 下の、追加されたリスト内にあります。

STEP 5 | (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
```

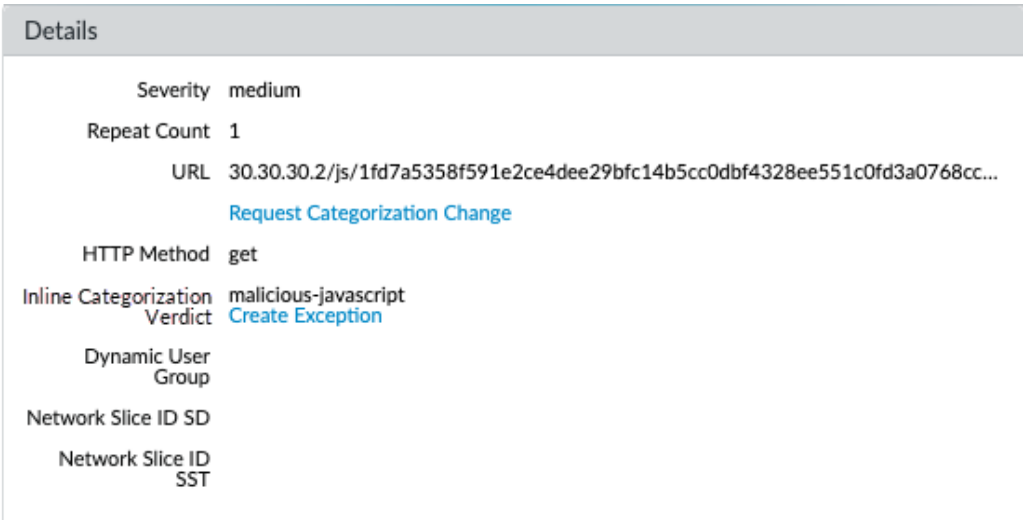
以下に例を示します。

```
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、MLドメイン ml.service.paloaltonetworks.com がブロックされていないことを確認してください。

STEP 6 | URLフィルタリング デプロイメントの計画。

URLフィルタリング インラインMLを使用して処理されたWebページの情報を表示するには、ログを**Inline ML Verdict (インライン ML 判定)**基準でフィルタリングします (**[Monitor (監視)] > [Logs (ログ)] > [URL Filtering (URL フィルタリング)]**。脅威が含まれていると判断された Web ページは、フィッシングまたは悪意のある **javascript**のいずれかの判定で分類されます。例：



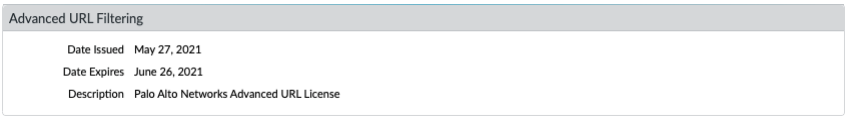
インライン分類の設定（PAN-OS 10.2以降）

STEP 1 | PAN-OS Web インターフェイスにログインします。

STEP 2 | インライン分類を利用するには、アクティブな高度なURLフィルタリングのサブスクリプションが必要です。

ローカルのインライン分類は、従来の *URL Filtering* サブスクリプションの既存の所有者である場合に有効にできます。

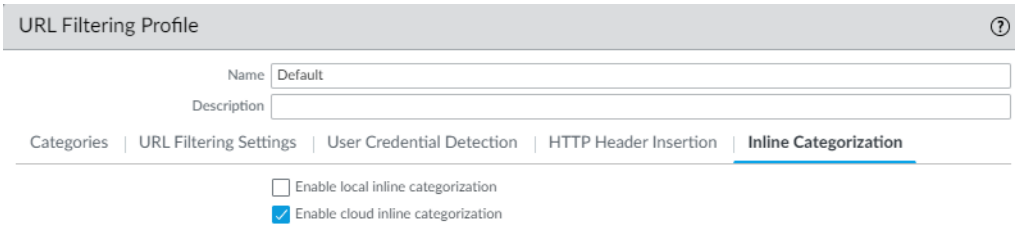
高度な URL フィルタリング サブスクリプションがあることを確認します。現在アクティブなライセンスがあるサブスクリプションを確認するには、**Device > Licenses** を選択し、適切なライセンスが使用可能で有効期限が切れていないことを確認します。



STEP 3 | 新しいURLフィルタリング セキュリティ プロファイルを更新または作成して、クラウドのインライン分類を有効にします。

ローカルおよびクラウドのインライン分類で使用されるポリシーアクションは、***Categories*** タブで構成されている設定によって異なります。

1. 既存の**URL Filtering Profile**（**URL** フィルタリング プロファイル）を選択するか、新しい **(Objects (オブジェクト) > Security Profiles (セキュリティプロファイル) > URL Filtering (URL** フィルタリング**)**を **Add**（追加）します。
2. URL Filtering プロファイルを選択し、**Inline Categorization** に移動し、デプロイするインライン分類メソッドを有効にします。
   - クラウド インライン分類を有効にする – 疑わしい Web ページのコンテンツをリアルタイムで分析し、標的型フィッシング攻撃や高度な回避手法を使用するその他の Web ベースの攻撃など、ゼロデイ Web 攻撃からユーザーを保護するクラウドベースのインライン ディープ ラーニング エンジン。
   - ローカルのインライン分類を有効にする – 機械学習技術を使用して、Web ページに埋め込まれた JavaScript エクスプロイトやフィッシング攻撃の悪意のある亜種を防止する firewall ベースの検出エンジン。



3. **OK** をクリックし、変更を **Commit (**コミット**)** します。

STEP 4 | (任意) 誤検知が発生した場合は、URLフィルタリング プロファイルにURLの例外を追加します。URL Filtering プロファイルで外部動的リストまたはカスタム URL カテゴリ リストを指定することで、例外を追加できます。指定された例外は、クラウドとローカルのインライン分類の両方に適用されます。

カスタム *URL* カテゴリ *(**Objects** > **Custom Objects** > **URL** カテゴリ)*

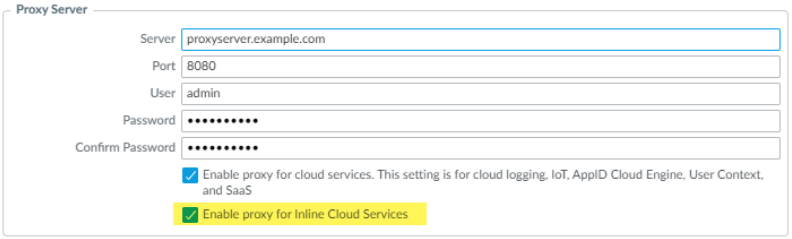
にエントリを追加する他のメカニズムによって作成された *URL* 例外も、インライン分類の例外として機能します。

1. **[Objects] > [**セキュリティ プロファイル**] > [URL** フィルタリング**]** の順に選択します。
2. 特定のURLを除外するURLフィルタリング プロファイルを選択し、**[Inline Categorization (**インライン分類**)]** を選択します。
3. **Add** をクリックして、既存の URL ベースの外部動的リストまたはカスタム URL カテゴリを選択します。使用可能なものがない場合は、それぞれ新しいexternal dynamic listまたはCustom URL Categoryを作成します。
4. **OK** をクリックして URL フィルタリング プロファイルを保存し、変更を **Commit (**コミット**)** コミットします。

STEP 5 | (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. (次のリリースのみ:PAN-OS 10.2.11以降および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 は無効になっている。
```

STEP 6 | (Optional)インライン分類サービス要求を処理するために firewall によって使用される Cloud Content Fully Qualified Domain Name (FQDN) を設定します。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。

Cloud Content 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します。

firewall がお住まいのリージョンに対して正しい Content Cloud FQDN (**Device** > **Setup** > **Content-ID** > **Content Cloud Setting**) を使用していることを確認し、必要に応じて FQDN を変更します。

- US—**us.hawkeye.services-edge.paloaltonetworks.com**
- EU—**eu.hawkeye.services-edge.paloaltonetworks.com**
- UK — **uk.hawkeye.services-edge.paloaltonetworks.com**

  英国ベースのクラウド コンテンツ *FQDN* は、*EU (eu.hawkeye.services-edge.paloaltonetworks.com)* にあるバックエンド サービスに接続することにより、高度な *URL* フィルタリングのインライン分類サービス サポートを提供します。
- APAC—**apac.hawkeye.services-edge.paloaltonetworks.com**

STEP 7 | (Optional)インライン分類サーバーへの firewall の接続状況を確認します。

1. ml.service.paloaltonetworks.com サーバーは、クラウドおよびローカルのインライン分類の操作に関連する firewall ベースのコンポーネントの定期的な更新を提供します。

   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。

   ```
   sow 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、次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.

2. hawkeye.services-edge.paloaltonetworks.com サーバーは、クラウドのインライン分類によってサービス要求を処理するために使用されます。

   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 ctd-agent status security-client
   ```

   以下に例を示します。

   ```
   show ctd-agent status security-client ...Security Client
    AceMlc2(1) Current cloud server: hawkeye.services-
   edge.paloaltonetworks.com Cloud connection: connected ...
   ```

   CLI 出力は簡潔にするために短縮されました。

   Advanced URL Filtering クラウド サービスに接続できない場合は、次のドメインがブロックされていないことを確認します: hawkeye.services-edge.paloaltonetworks.com。

STEP 8 | 高度なURLフィルタリング クラウド 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。クラウドのインライン分類が有効になっているすべての firewall について、この手順を繰り返します。

STEP 9 | URLフィルタリング デプロイメントの計画。

URL カテゴリの例外

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URL カテゴリの適用から特定の Web サイトを除外して、URL カテゴリに関連付けられたポリシー アクションに関係なく、これらの Web サイトがブロックまたは許可されるようにすることができます。たとえば、ソーシャル ネットワーキング URL カテゴリをブロックし、LinkedIn へのアクセスを許可する場合があります。URLカテゴリポリシー適用の例外を作成するには:

- **URL**リストタイプのカスタムURLカテゴリに、ブロックまたは許可したいサイトのIPアドレスまたはURLを追加します。次に、URL フィルタリング プロファイルでカテゴリのサイト アクセスを定義します。最後に、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。

  カスタム*URL*カテゴリをセキュリティ ポリシールールの一致条件として使用することもできます。例外ルールは、*URL* 例外が属するカテゴリをブロックまたは許可するルールの上に必ず配置してください。

- ブロックまたは許可したいサイトのURLを**URL**リストタイプの外部動的リストに追加します。次に、URLフィルタリング プロファイルで外部動的リストを使用https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/enforce-policy-on-an-external-dynamic-list#id931ea7ea-00e9-4fa7-a2d9-ebb4dee276faURLフィルタリングプロファイル、またはセキュリティポリシールールの一致基準として、外部ダイナミックリストを使用します。外部動的リストを使用する利点は、ファイアウォールで構成変更やコミットを実行せずにリストを更新できることです。

URLリストタイプの外部動的リストは、ドメインリストの外部動的リストまたはIPアドレスリストのタイプと混同しないでください。*URL* の外部動的リストはドメインと *IP* アドレスを許可しますが、その逆は当てはまらず、無効なエントリになります。

- URLカテゴリの例外のガイドライン
- カスタム URL カテゴリの作成
- URLフィルタリング プロファイルで外部動的リストを使用

URLカテゴリの例外のガイドライン

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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

次のガイドラインでは、URLカテゴリの例外リスト(カスタムURLカテゴリまたはURLの外部動的リスト)を設定する方法について説明します。ワイルドカードの使用例と特定のエントリを示します。

URL カテゴリ例外リストの基本的なガイドライン

エントリを URL カテゴリの例外リストに追加する前に、エントリが一致する可能性があるかどうかを検討してください。次のガイドラインでは、意図した Web サイトやページをブロックまたは許可するエントリを作成する方法を指定します。

デフォルトでは、*firewall* は、末尾のスラッシュ *(/)* またはアスタリスク *(*)* で終わらないドメインエントリに、末尾のスラッシュ *(/)* を自動的に追加します。末尾にスラッシュを追加すると、*firewall* が一致と見なし、ポリシーを適用する *URL* が変更されます。ワイルドカードでないドメインエントリでは、末尾のスラッシュは、指定されたドメインとそのサブディレクトリにマッチを限定します。たとえば、***example.com*** *(*処理後の ***example.com/*** *)* は、自分自体と ***example.com/search*** とマッチします。

ワイルドカードドメインのエントリ（アスタリスクまたはキャレットが付いたエントリ）では、最後のスラッシュが、指定されたパターンに一致する*URL*へのマッチングを限定します。たとえば、エントリ ****.example.com*** と一致するには、*URL* に少なくとも *1* つのサブドメインが含まれ、ルート ドメイン ***example.com*** で終わる必要があります。パターンは ***<subdomain>.example.com***; ***news.example.com*** はマッチしますが、***example.com*** はサブドメインがないためマッチしません。

末尾にスラッシュを手動で追加して、エントリを検査するすべてのユーザーに対して、エントリの意図されたマッチ動作を明確にすることをお勧めします。末尾のスラッシュは、*firewall* によって追加されると見えなくなります。

PAN-OS® 10.2 を実行している *Panorama™* 管理サーバーは、同じソフトウェアバージョンのファイアウォールに対してのみこの機能を有効にすることができます。*PAN-OS 10.1* 以前を実行している *firewall* に対してこの機能を有効にするには、各 *firewall* で次の *CLI* コマンドを使用します:

```
admin@PA-850> debug device-server append-end-token on
```

```
admin@PA-850> configure
```

```
admin@PA-850# commit
```

この機能を無効にするには、***Device*** > ***Setup*** > ***Content-ID*** > ***URL Filtering*** を選択します。次に、***Append Ending Token*** の選択を解除します。ただし、この機能を無効にすると、予想よりも多くの *URL* へのアクセスをブロックまたは許可されます。*firewall* は、*/* または *** で終わらないドメインエントリの末尾に 暗黙のアスタリスク を追加します。たとえば、許可された *Web* サイトの *URL* リストに ***example.com*** を追加すると、*firewall* はそのエントリを ***example.com.**** と解釈します。その結果、*firewall* は ***example.com.domain.xyz*** などのサイトへのアクセスを許可します。URL Category Exceptions*(PAN-OS 10.1* 以前*)* では、この機能を無効にした場合の *firewall* の動作について説明します。

- リストエントリは大文字と小文字を区別しません。
- URL エントリから `http` と `https` を省略します。
- 各 URL エントリの長さは最大255文字です。
- ブロックまたは許可するIPアドレスまたはURLと完全に一致するものを入力するか、ワイルドカードを使用してパターンマッチを作成します。

  エントリが異なると、完全一致も異なります。特定の *Web* ページ (***example.com/contact***) の *URL* を入力すると、*firewall* は、そのページのみに一致を限定します。ドメインの完全一致は、ドメイン自体とそのサブディレクトリに一致を限定します。
- 元のエントリが URL 以外のエントリからアクセスできる場合は、Web サイトまたはページへのアクセスに最も一般的に使用される URL を例外リストに追加することを検討してください (たとえば、**blog.paloaltonetworks.com** や **paloaltonetworks.com/blog**)。
- エントリ **example.com** は **www.example.com** とは異なります。ドメイン名は同じですが、2 番目のエントリには *www* サブドメインが含まれています。

Palo Alto Networks は、カスタム *URL* カテゴリまたは外部動的リストエントリでの正規表現の使用をサポートしていません。特定の *URL* を知っているか、ワイルドカードと次の文字を使用して照合する *URL* パターンを作成する必要があります: `. / ? & = ; +`。

URL カテゴリ例外リストのワイルドカードのガイドライン

URL カテゴリの例外リストでアスタリスク (*) とキャレット (^) を使用すると、正確な URL を指定せずに、複数のサブドメイン、ドメイン、トップレベルドメイン (TLD)、またはページに一致するように 1 つのエントリを設定できます。

アスタリスク（*）およびキャレット（^）ワイルドカードの使用方法

次の文字はトークン区切り文字です: `. / ? & = ; +`。これらの文字の 1 つまたは 2 つで区切られたすべての文字列はトークンです。ワイルドカード文字をトークン プレースホルダとして使用すると、特定のトークンに任意の値を含めることができます。エントリ **docs.paloaltonetworks.com** では、トークンは "docs"、"paloaltonetworks"、および "com" です。

次の表は、アスタリスクとキャレットの仕組みとその例です。

*	^
1 つ以上の可変サブドメイン、ドメイン、TLD、またはサブディレクトリーを示します。 末尾のスラッシュの後にアスタリスクを使用できます (**example.com/*** など)。	1 つの可変サブドメイン、ルート・ドメイン、または TLD を示します。 末尾のスラッシュの後にキャレットを使用することはできません。次のエントリは無効です: **example.com/^**。

*	^
例: ***.domain.com** は **docs.domain.com** と **abc.xyz.domain.com** に一致します。	例: **^.domain.com** は **docs.domain.com** と **blog.domain.com** に一致します。

Key Point:アスタリスクは、キャレットよりも広い範囲の URL に一致します。アスタリスクは任意の数の連続するトークンに対応し、キャレットは 1 つのトークンのみに対応します。

xyz.*.com のようなエントリは、**xyz.^.^.com** よりも多くのサイトに一致します。**xyz.*.com** は、文字列間の任意の数のトークンを持つサイトに一致し、**xyz.^.^.com** は、正確に 2 つのトークンを持つサイトに一致します。

- ワイルドカード文字はトークン内の唯一の文字でなければなりません。たとえば、**example*.com** は、example と * が同じトークン内にあるため 、無効なエントリです。ただし、1 つのエントリに複数のトークンにワイルドカードを含めることができます。
- 同じエントリ内でアスタリスクとキャレットを使用できます (***.example.^** など)。

連続するアスタリスク *(**)* または *9* つ以上の連続するキャレット *(^)* を含むエントリを作成しないでください。このようなエントリは、*firewall* のパフォーマンスに影響を与える可能性があります。

たとえば、***mail.*.*.com*** のようなエントリを追加しないでください。代わりに、アクセスを制御する *Web* サイトの範囲に応じて、***mail.*.com*** または ***mail.^.^.com*** と入力します。

URL カテゴリ除外リスト - 例

次の表は、URLリストエントリーの例、マッチングサイト、およびファイアウォールが自動的に末尾のスラッシュを追加する場合のマッチング動作の説明を示しています。

*The entries in this table do not contain a trailing slash to reflect that the firewall appends one to applicable entries in the background.*さらに、例外リストには、末尾のスラッシュのガイダンスの前に追加された項目が含まれることがあります。URL カテゴリ例外:例 *(PAN-OS 10.1)*は、ファイアウォールがデフォルトで末尾のスラッシュを追加しない場合に一致する動作を示しています。

末尾にスラッシュを手動で追加して、エントリを検査するすべてのユーザーに対して、エントリの意図されたマッチ動作を明確にすることをお勧めします。末尾のスラッシュは、ファイアウォールによって追加された場合は見えません。

URL 例外リストのエントリ	サイト一致	説明
セット **1** の例		

URL 例外リストのエントリ	サイト一致	説明
paloaltonetworks.com	paloaltonetworks.com paloaltonetworks.com/network-security/security-subscriptions	firewall はエントリの末尾にスラッシュを追加し、正確なドメインとそのサブディレクトリへの一致を限定します。
paloaltonetworks.com/example	paloaltonetworks.com/example	firewall は、サブディレクトリー **example** がドメインの後に続くため、このエントリーに末尾のスラッシュを追加しません。特定の Web ページの URL を入力すると、firewall は指定された Web ページに例外アクションを適用します。
Example Set 2— アスタリスク		
*.example.com	www.example.com docs.example.com support.tools.example.com	アスタリスクは、すべての **example.com** サブドメインに一致を拡張します。 firewall は、ルートドメインである **example.com** の右側に一致するものを除き、エントリに末尾のスラッシュを追加します。
mail.example.* このエントリは、末尾のスラッシュ機能を有効にしてもしなくても、同じマッチを生成します。	mail.example.com mail.example.co.uk mail.example.com/#inbox	アスタリスクは、**mail.example.*<TLD>**パターンに続くすべてのURLにマッチするように拡張します。
example.*.com	example.yoursite.com example.es.domain.com example.abc.xyz.com	アスタリスクは、左端のサブドメインが **example** で、最上位ドメインが **com** の URL に一致を拡張します。末尾のスラッシュは、TLD の右側にある一致を除外します。

URL 例外リストのエントリ	サイト一致	説明
example.com/*	example.com/photos example.com/blog/latest 任意の example.com サブディレクトリ	ドメインの後には、/ と、サブディレクトリーが存在しなければならないことを示すアスタリスクが続きます。アスタリスクは、任意の **example.com** サブディレクトリーのトークン・プレースホルダーとして機能します。 firewall は、エントリーがアスタリスクで終わるため、末尾にスラッシュを追加しません。
Example Set 3— キャレット		
google.^ *example.co.^* などのパターンは、通常、***example.co.jp*** などの国固有のドメインを照合するために使用されます。ただし、汎用トップレベルドメイン *(gTLD)* では、*example.co.^* マッチング *example.co.info* や *example.co.amzn* などのパターンが発生し、同じ組織に属していない可能性があります。	google.com google.info google.com/search?q=paloaltonetworks	キャレットは、**google** で始まり、単一の TLD で終わる URL に一致を拡張します。末尾のスラッシュは、最後のトークンの右側にある一致を除外します。
^.google.com	www.google.com news.google.com	キャレットは、一致を **google.com** の単一レベル サブドメインに展開します。firewall は、ルートドメインの右側にある一致を除

URL 例外リストのエントリ	サイト一致	説明
		き、エントリの末尾にスラッシュを追加します。
^.^.google.com	www.maps.google.com support.tools.google.com	2 つのキャレットは、**google.com** の前に 2 つの連続するサブドメインを含む URL に一致を拡張します。firewall は、ルートドメインの右側にある一致を除き、エントリの末尾にスラッシュを追加します。
google.^.com	google.example.com google.company.com	キャレットは、**google**が一番左のサブドメインで、その後に1つのトークンと**.com**が続くURLにマッチするように展開されます。 firewall は、TLD の右側にある一致を除き、エントリの末尾にスラッシュを追加します。

カスタム URL カテゴリの作成

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)	❑ Advanced URL Filteringライセンス (またはレガシーURLフィルタリングライセンス) 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

あなたは、カスタムURLカテゴリを使用して、URLカテゴリの適用の例外を定義するか、複数のカテゴリから新しいURLカテゴリを定義します。

URLカテゴリ適用の例外の定義 **(URL**リスト**)**

URLのリスト(1つのカスタムカテゴリにグループ化)を指定し、事前定義されたURLカテゴリとは無関係に適用します。このカテゴリへのアクセスは、セキュリティポリシールールに適用するURLフィルタリングプロファイルで制御したり、セキュリティポリシールールの一致基準とし

てカテゴリを使用したりできます。たとえば、ソーシャル ネットワーキングカテゴリをブロックしつつ、LinkedIn へのアクセスを許可することができます。

複数の**PAN-DB** カテゴリに基づくカスタム**URL**カテゴリの定義**(**カテゴリ一致**)**

カスタムカテゴリの一部として定義されたすべてのカテゴリに一致するWebサイトまたはページに適用対象を設定するために、新しいカテゴリを作成します。たとえば、PAN-DB では、エンジニアが調査に使用する開発者ブログを `personal-sites-and-blogs`、`computer-and-internet-info`、および `high-risk` に分類できます。エンジニアがブログや類似の Web サイトにアクセスしてさらにこれらのWebサイトを表示できるようにするには、3つのカテゴリに基づいてカスタムURLカテゴリを作成し、URLフィルタリング プロファイルで警告するカテゴリにサイト アクセスを設定します。

*PAN-DB*は、外部ダイナミックリストおよび事前定義された*URL*カテゴリの前に、カスタム*URL*カテゴリに対して*URL*を評価します。したがって、ファイアウォールは、カスタム*URL*リスト内の*URL*のセキュリティ ポリシー ルールを、その*URL*が存在する個々の*URL*カテゴリに関連付けられたポリシー ルールよりも優先して適用します。

複数のセキュリティ ポリシー ルールにカスタム*URL*カテゴリが含まれている場合、ファイアウォールは、一致するトラフィックに対して最も厳格な*URL*フィルタリング プロファイル アクションを持つセキュリティ ポリシー ルールを適用します。

- Strata Cloud Manager
- PAN-OS & Panorama

カスタムURLカテゴリの作成(Strata Cloud Manager)

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

*[**PAN-OS & Panorama**]* タブに切り替えて、そこにあるガイダンスに従います。

Strata Cloud Managerをお使いの場合は、こちらに進んでください。

STEP 1 | **[Manage (管理)]** > **[Configuration (設定)]** > **[Security Services (セキュリティサービス)]** > **[URL Access Management (URL**アクセス管理**)]** > **[Access Control (**アクセス制御**)]**を順に選択します。

STEP 2 | [カスタムURLカテゴリ]で**[Add Category (**カテゴリを追加**)]**を選択します。

カテゴリのわかりやすい名前を入力します。

STEP 3 | カスタムURLカテゴリの種類を**[URL List (URL**リスト**)]**または**[Category Match (**カテゴリマッチ**)]**に設定します。

- ［**URL List**］：このリスト タイプは、そのリスト タイプが属するURLカテゴリとは異なる強制を行うURLを追加したり、カスタム カテゴリに属するURLのリストを定義したりするために使用します。URLリストのエントリを作成する際は、URLカテゴリの例外のガイドラインを参照してください。

- **Category Match (カテゴリ一致)**–一連のカテゴリにマッチするウェブサイトに絞って適用します。Web サイトまたはページは、カスタム カテゴリで定義されているカテゴリ *all* と一致する必要があります。

STEP 4 | [項目]で、URLまたは既存のカテゴリのいずれかを追加します。

STEP 5 | カスタム URL カテゴリを保存します。

STEP 6 | カスタムURLカテゴリのサイトアクセスとユーザー認証情報の提出設定を定義します。

1. **[Manage (管理)] > [Configuration (設定)] > [Security Services (セキュリティサービス)] > [URL Access Management (URLアクセス管理)] > URL Access Management Profiles (URLアクセス管理)]**を順に選択します。
2. 変更する既存のプロファイルを選択するか、［**Add Profile (プロファイルの追加)]**をクリックします。
3. [Access Control (アクセス制御)]で、先ほど作成したカスタムURLカテゴリを選択します。`Custom URL Categories (カスタムURLカテゴリ)`の下、`Pre-Defined Categories (事前定義カテゴリ)`の上にあります。
4. カテゴリに**[サイトアクセス]**を設定します。
5. カテゴリのユーザー資格情報提出書類を設定します。
6. プロファイルを保存します。

STEP 7 | URLアクセス管理プロファイルをセキュリティポリシールールに適用します。

URLアクセス管理プロファイルは、セキュリティポリシー規則が参照するプロファイルグループに含まれている場合にのみアクティブになります。

手順に従って、URLアクセス管理プロファイル（および任意のセキュリティプロファイル）をアクティブにします。必ず**[Push Config (設定のプッシュ)]**を行ってください

カスタム*URL*カテゴリをセキュリティ ポリシールールの一致条件として使用することもできます。このシナリオでは、*URL*フィルタリング プロファイルで*URL*カテゴリのサイトアクセスを定義しません。代わりに、カスタム*URL*カテゴリを作成した後、カスタム*URL*カテゴリを追加するセキュリティポリシールールを選択します（***[Manage (管理)] > [Configuration (構成)] > [Security Services (セキュリティサービス)] > [Security Policy (セキュリティポリシー)]***。***[Applications (アプリケーション)]***、***[Services (サービス)]***と*[URL Category Entities (URLとURLカテゴリエンティティ)]*で***[Add URL Categories (URL**カテゴリを追加**)]***をクリックします。作成したカスタム*URL*カテゴリを選択し、セキュリティポリシールールを保存します。

カスタムURLカテゴリの作成(PAN-OS & Panorama)

STEP 1 | **[Objects (オブジェクト)] > [Custom Objects (カスタム オブジェクト)] > [URL Category (URL カテゴリ)]**を選択します。

STEP 2 | を追加するか、カスタム URL カテゴリを変更し、カテゴリに説明的な **Name** を付けます。

STEP 3 | カテゴリの **Type (タイプ)** を **Category Match (カテゴリ一致)** あるいは **URL List (URL リスト)** のいずれかに設定します：

- **URL List (URL リスト)**–属する対象の URL カテゴリとは別に適用したい URL を追加します。このリスト・タイプを使用して、URL カテゴリーの適用に対する例外を定義したり、URL のリストをカスタム・カテゴリーに属するものとして定義したりします。URL リスト エントリの作成に関するガイドラインについては、URL Category Exceptions を参照してください。

  デフォルトでは、ファイアウォールは、末尾のスラッシュまたはアスタリスク (*) で終わらないドメイン・エントリー (***example.com***) に、末尾のスラッシュ (/) を自動的に追加します。末尾のスラッシュは、*firewall* がドメインの右側に暗黙のアスタリスクを仮定するのを防ぎます。ワイルドカードでないドメインエントリでは、末尾のスラッシュは、指定されたドメインとそのサブディレクトリにマッチを限定します。たとえば、***example.com***(処理後の ***example.com/***) は、自分自体と***example.com/search***とマッチします。

  ワイルドカード・ドメイン項目 (アスタリスクまたはキャレットを使用する項目) では、末尾のスラッシュ制限は、指定されたパターンに準拠する *URL* と一致します。たとえば、エントリ ****.example.com*** に一致させるには、*URL* は厳密に *begin* を *1* つ以上のサブドメインで、ルート ドメイン ***example.com*** で終わる必要があります。***news.example.com*** は一致しますが、***example.com*** はサブドメインがないためではありません。

  末尾にスラッシュを手動で追加して、*URL* リストを調べるすべてのユーザーに対して、エントリの意図された一致動作を明確にすることをお勧めします。末尾のスラッシュは、*firewall*によって追加されると見えなくなります。URL Category Exceptions では、末尾のスラッシュと一致の動作についてさらに詳しく説明します。

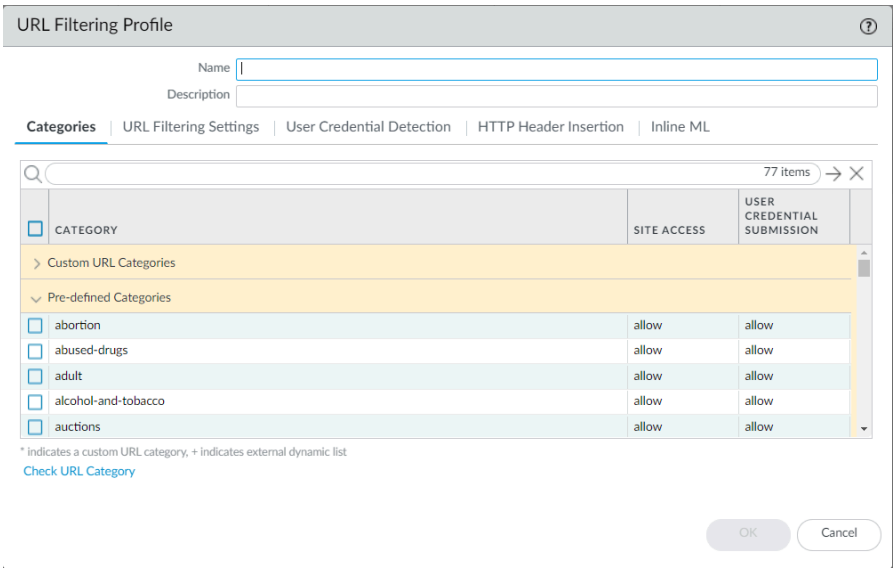
  この機能を無効にするには、 ***[Device (デバイス)]*** > ***[Setup (セットアップ)]*** > ***[Content-ID (コンテンツID)]*** > ***[URL Filtering (URL**フィルタリング**)]***に進みます。次に、***Append Ending Token*** の選択を解除します。この機能を無効にすると、意図したよりも多くの *URL* へのアクセスをブロックまたは許可する可能性があります。URL Category Exceptions*(PAN-OS 10.1 以前)* では、この機能が無効になっている場合の *firewall* の動作について説明します。

- **Category Match (カテゴリ一致)**–一連のカテゴリにマッチするウェブサイトに絞って適用します。Web サイトまたはページは、カスタム カテゴリで定義されているカテゴリ *all* と一致する必要があります。

STEP 4 | ［**OK**］をクリックしてカスタムURLカテゴリを保存します。

STEP 5 | **[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。

新しいカスタム カテゴリが **Custom URL Categories** の下に表示されます。



STEP 6 | カスタム URL カテゴリに サイト アクセス と のユーザー資格情報送信 を適用する方法を決定します。(ユーザーが会社の資格情報を送信できるサイトを制御するには、Prevent Credential Phishing を参照してください。

STEP 7 | URL Filtering プロファイルを Security ポリシールールにアタッチして、そのルールに一致するトラフィックを適用します。

[Policies (ポリシー)] > [Security (セキュリティ)] > [Actions (アクション)] を選択し、更新した URL フィルタリング プロファイルに基づいてトラフィックを適用するセキュリティ ポリシー ルールを指定します。変更を忘れずに **Commit (コミット)** してください。

カスタム *URL* カテゴリを *Security* ポリシールールの一致条件として使用することもできます。この場合、*URL Filtering* プロファイルで *URL* カテゴリのサイトアクセスを定義しません。カスタム カテゴリを作成したら、カスタム *URL* カテゴリを追加する *Security* ポリシー ルールに移動します *(**[Policies (ポリシー)] > [Security (セキュリティ)]**)*。次に、***Service/URL Category*** を選択して、カスタム *URL* カテゴリをルールの一致条件として使用します。

URLフィルタリング プロファイルで外部動的リストを使用

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)	❑ Advanced URL Filteringライセンス (またはレガシーURLフィルタリングライセンス) 注：

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	• レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

外部ダイナミック リストは外部の Web サーバーでホストされているテキストファイルです。このリストを使用してURLをインポートし、それらのURLにポリシーを適用することができます。ファイアウォールは設定済みの間隔で動的にリストをインポートし、リスト内の URL（IPアドレスやドメインは無視されます）に対してポリシーを適用します。WEBサーバー上でリストが更新されるとファイアウォールが変更内容を取得し、ファイアウォール上でコミットすることなくポリシーを変更されたリストに適用できます。

新たに検出された脅威やマルウェアからネットワークを保護するために、URL フィルタリング プロファイルで の外部動的リスト を使用できます。URL フォーマットのガイドラインについては、「URLカテゴリの例外のガイドライン」を参照してください。

- Strata Cloud Manager
- PAN-OS & Panorama

URLフィルタリング プロファイルで外部動的リストを使用する (Strata Cloud Manager)

> ***Panorama***を使用して***Prisma Access***を管理している場合:
>
> *[**PAN-OS & Panorama**]* タブに切り替えて、そこにあるガイダンスに従います。
>
> ***Strata Cloud Manager***をお使いの場合は、こちらに進んでください。

STEP 1 | Prisma Accessが外部の動的リストを参照できるようにします。

外部動的リストは、インポートされたIPアドレス、URL、またはドメイン名のリストを定義できます。ポリシー ルールでこれらの情報を使用してトラフィックをブロックまたは許可できます。

外部動的リストを設定するには、**[Manage (管理)]** > **[Configuration (設定)]** > **[Objects (オブジェクト)]** > **[External Dynamic Lists (外部動的リスト)]**に移動します。

- リストにIPアドレスやドメイン名を含めないでください。ファイアウォールはURL以外のエントリーをスキップします。
- リストの書式を確認するには、 カスタム URL リストのガイドライン を使用します。
- **[List Type (リストタイプ)]**を**[URL List (URL**リスト**)]**に指定します。

STEP 2 | URLフィルタリングで外部動的リストを使用します。

[Manage (管理)] > **[Configuration (設定)]** > **[Security Services (セキュリティ サービス)]** > **[URL Access Management (URL**アクセス管理**)]**の順に移動します。

- 外部動的リストのURLにサイトアクセスを指定します。

- 外部動的リストのURLを高度なインライン分類から除外します。

外部の動的リストを使用してカスタム*URL*カテゴリを作成することもできます（*URL*アクセス管理ダッシュボードに戻ってこれを行います）。

外部動的リストに含まれる*URL*がカスタムURLカテゴリにも含まれている場合、またはブロックと許可リストに含まれる場合、カスタム カテゴリで指定されたアクションが外部動的リストよりも優先されます。

STEP 3 | ポリシー アクションが適用されているかどうかテストします。

1. 外部動的リストエントリ(**[Manage (管理)]** > **[Configuration (設定)]** > **[Objects (オブジェクト)]** > **[External Dynamic Lists (外部動的リスト)]**)を表示し、リストからURLへのアクセスを試みます。
2. 定義したアクションがブラウザに適用されることを確認します。

URLフィルタリング プロファイルで外部動的リストを使用する (PAN-OS & Panorama)

STEP 1 | 外部動的リストにアクセスするようにファイアウォールを設定する。

- リストにIPアドレスやドメイン名を含めないでください。ファイアウォールはURL以外のエントリーをスキップします。
- リストの書式を確認するには、カスタム URL リストのガイドライン を使用します。
- Type (タイプ) ドロップダウンリストから **URL List (URL** リスト**)** を選択します。

STEP 2 | URLフィルタリング プロファイル内で外部動的リストを使用します。

1. **Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > URL Filtering (URL フィルタリング)** の順に選択します。
2. **Add** [追加]、あるいは既存のURLフィルタリング プロファイルを変更します。
3. このプロファイルに**Name** [名前]を付け、**Categories** [カテゴリ]タブのCategory [カテゴリ]リストから外部動的リストを選択します。
4. Action [アクション]を選択し、外部動的リスト内のURLに対する細かなアクションを選択します。

   外部動的リストに含まれる*URL*がカスタムURLカテゴリにも含まれている場合、またはブロックと許可リストに含まれる場合、カスタム カテゴリで指定されたアクションが外部動的リストよりも優先されます。
5. **OK** をクリックします。
6. URL フィルタリング プロファイルをセキュリティポリシー ルールに適用します。
   1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
   2. **Actions** [アクション]タブを選択し、Profile Setting [プロファイル設定]セクションの**URL Filtering** [URLフィルタリング]ドロップダウンリストで新しいプロファイルを選択します。
   3. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 3 | ポリシー アクションが適用されているかどうかテストします。

1. 外部動的リストエントリ を表示し、リストから URL にアクセスします。
2. 定義したアクションがブラウザに適用されることを確認します。
3. ファイアウォール上のアクティビティを監視するには：
   1. **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたURLのNetwork Activity [ネットワーク アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
   2. 詳細ログ ビューにアクセスするには、**Monitor (監視) > Logs (ログ) > URL Filtering (URL フィルタリング)** を選択します。

STEP 4 | 外部動的リストのエントリーが無視されたかスキップされたかを検証します。

タイプがURLのリストでは、ファイアウォールはURL以外のエントリーを無効なものとしてスキップし、ファイアウォール モデルの限度を超えるエントリーは無視します。

外部動的リストの種類について制限に達しているかどうか確認するためには、***Objects*** **(**オブジェクト**)** **>** ***External Dynamic Lists*** **(**外部動的リスト**)** を選択し、***List Capacities*** **(**キャパシティをリストアップ**)** をクリックします。

ファイアウォール上で次のCLIコマンドを実行し、リストの詳細情報を表示します。

```
request system show type url name <list_name>
```

以下に例を示します。

```
request system external-list show type url name My_URL_List
 vsys5/My_URL_List:次の更新:Tue Jan 3 14:00:00 2017 Source: http://
example.com/My_URL_List.txt Referenced:はい 有効:はい認証有効:Yes 有
効なエントリの合計数:3 無効なエントリの合計数:0 有効な URL: www.URL1.com
 www.URL2.com www.URL3.com
```


URL フィルタリング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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

Palo Alto Networks URLフィルタリングソリューションは、Webベースの脅威からお客様を保護し、Webアクティビティを監視および制御する簡単な方法を提供します。URL フィルターの展開を最大限に活用するには、まず、ビジネスを行うために依存しているアプリケーションの許可ルールを作成する必要があります。次に、悪意のあるコンテンツおよび悪用されるコンテンツを分類する URL カテゴリを確認します。これらを完全にブロックすることをお勧めします。次に、他のすべてについて、これらのベストプラクティスは、ユーザーが必要とする Web コンテンツへのユーザーのアクセスを制限することなく、Web ベースの脅威にさらされるリスクを減らす方法を案内します。

- 開始する前に、ベスト プラクティスのインターネット ゲートウェイ セキュリティ ポリシーの構築の一環として、許可するアプリケーションを特定し および アプリケーション許可ルールの作成 を実行します。

  許可するアプリケーションには、ビジネスとインフラストラクチャの目的でプロビジョニングまた管理するアプリケーションだけでなく、ユーザーが業務を行うために必要なアプリケーションや、個人的利用のために使用を許可する一部のアプリケーションも含まれます。

  これらの承認済みアプリケーションを特定したら、URL フィルターを使用して、許可リストにないすべての Web アクティビティを制御および保護できます。
- ユーザーのWebアクティビティを可視化して、組織にとって最も効果的なURLフィルタリング ポリシーを計画できるようにします。これには次のものが含まれます:
  - Test A Site を使用して、PAN-DB (Palo Alto Networks URL フィルタリング クラウド データベース) が特定の URL を分類する方法を確認し、考えられるすべての URL カテゴリについて学習します。
  - URL カテゴリについてアラートを出す (おおよそ) パッシブな URL フィルタリング プロファイルから始めます。これにより、ユーザーがアクセスするサイトに対する可視性を得て、何を許可、制限、ブロックするべきか判断できるようになります。
  - Web アクティビティを監視して、ユーザーがアクセスしているサイトを評価し、ビジネスニーズにどのように対応しているかを確認します。

- 悪質で悪用されるWebコンテンツを分類するURLカテゴリをブロックします。これらのカテゴリは危険であることがわかっていますが、ブロックすることを決定した URL カテゴリはビジネスニーズに依存する可能性があることに常に注意してください。
- URL カテゴリを使用して復号化を段階的に導入し、機密情報または個人情報（金融サービスや健康と医療など）を復号化から除外します。

  最も危険なトラフィックを最初に復号化する計画 (ゲームや危険度の高いなどの悪意のあるトラフィックを収容する可能性が最も高い URL カテゴリ) し、経験を積むにつれてさらに復号化を行います。あるいは、ビジネスに影響を与えない URL カテゴリを最初に復号化します (問題が発生してもビジネスに影響を与えない) などのニュース フィード。どちらの場合も、いくつかの URL カテゴリの暗号化を解除し、ユーザーからのフィードバックを聞き、レポートを実行して、復号化が期待どおりに機能していることを確認し、さらにいくつかの URL カテゴリを徐々に復号化します。技術的な理由で復号化できない、または復号化しないことを決めたサイトに、復号化から除外するために復号化除外の作成を計画します。

  URL カテゴリに基づいて復号化をターゲットにすることも、Decryption（復号化）のベストプラクティスです。
- ファイアウォールを有効にすることにより認証情報の盗難を防止して、サイトへの企業の認証情報の送信を検出し、URL カテゴリに基づいてそれらの送信を制御します。ユーザーが悪意のあるサイトや信頼されていないサイトに認証情報を送信するのをブロックし、ユーザーが未知のサイトで企業の認証情報を入力する際に警告を発し、企業外のサイトで企業の認証情報を再利用する際は警告し、ユーザーが企業のサイトや確認済みのサイトに認証情報を送信するのを明示的に許可します。
- JavaScript エクスプロイトの悪意がある亜種やフィッシング攻撃を、リアルタイムでブロックします。ローカルインライン分類を有効にすると、ファイアウォールで機械学習を使用してWebページを動的に分析できます。
- インライン分類を有効にして、インライン ディープ ラーニング、MLベースの検出エンジンを使用して、疑わしいWebページ コンテンツを分析し、ゼロデイWeb攻撃からユーザーを保護します。クラウドのインライン分類は、高度な標的型フィッシング攻撃や、クローキング、マルチステップ攻撃、CAPTCHAチャレンジ、以前は見られなかったワンタイム使用URLなどの高度な回避技術を使用するその他のWebベースの攻撃を検出して防止することができます。
- の高リスクおよび中リスクのコンテンツとのユーザーの対話方法を解読し、検査し、厳密に制限します (ビジネス上の理由から、の悪質なURLカテゴリをブロックしないことにした場合は、ユーザーがそれらのカテゴリと対話する方法も厳密に制限する必要があります)。

  認可する Web コンテンツと完全にブロックする悪意のある URL カテゴリは、Web トラフィック全体の一部にすぎません。ユーザーがアクセスしている残りのコンテンツは、良性（低リスク）と危険なコンテンツ（高リスクと中リスク）の組み合わせです。高および中リスクのコンテンツは悪意があると確定されているわけではありませんが、悪意のあるサイトと密接に関連しています。たとえば、リスクの高いURLが悪意のあるサイトと同じドメインにある場合や、過去に悪意のあるコンテンツをホストしていた場合などです。

  ただし、組織にリスクをもたらす多くのサイトは、ユーザーに貴重なリソースとサービスも提供しています（クラウドストレージサービスは良い例です）。これらのリソースとサービスはビジネスに必要ですが、サイバー攻撃の一部として使用される可能性も高くなります。

ユーザーに優れたユーザーエクスペリエンスを提供しながら、この潜在的に危険なコンテンツを操作する方法を制御する方法は次のとおりです。

- URL フィルタリング プロファイルで、高リスクと中リスクのカテゴリを**continue(**続行**)**に設定し、応答ページを表示して、ユーザーに危険性のあるサイトにアクセスしていることを警告します。ユーザーがサイトにcontinue (続行)することを決定した場合に予防策をとる方法をアドバイスします。ユーザーに応答ページを表示したくない場合は、リスクの高いカテゴリとリスクが中程度のカテゴリで警告します。
- 高リスクおよび中リスクのサイトを復号します。
- 高リスクおよび中リスクのサイトのためのアンチスパイウェア、脆弱性対策、ファイル遮断の ベストプラクティスに従ってください。危険なファイルタイプのダウンロードをブロックし、難読化された JavaScript をブロックすることが保護手段となります。
- 高リスクおよび中リスクのサイトにユーザーが企業の認証情報を送信するのをブロックすることにより、認証情報の盗難を防止します。

- 学校や教育機関は、セーフ サーチを適用して、検索エンジンが検索結果からアダルト画像や動画を確実に除外するようにする必要があります。
- URLカテゴリ検索中に最初のWebリクエストを保持する。

  ユーザーがウェブサイトにアクセスすると、Advanced URL Filteringはキャッシュされたカテゴリをチェックしてサイトを分類します。ファイアウォールがURLカテゴリをキャッシュで見つけられない場合、ファイアウォールはPalo Alto NetworksのURLデータベースであるPAN-DBで検索を実行します。デフォルトでは、このクラウドルックアップ中にユーザーのウェブリクエストが許可されます。

  ただし、Web要求を保持することを選択した場合、Advanced URL Filteringは、URLカテゴリが見つかるか、タイムアウトになるまで要求をブロックできます。検索がタイムアウトした場合、ファイアウォールは解決されていない URL カテゴリと見なします。この機能は、URLフィルタリング設定の「クライアントのカテゴリー検索要求を保留」で見つけてください。

テスト URL フィルタリング構成

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)	❑ Advanced URL Filteringライセンス (またはレガシーURLフィルタリングライセンス) 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URLフィルタリング ポリシー構成をテストするには、Palo Alto Networks URLフィルタリング テスト ページを使用します。これらのページは、すべての定義済みURLカテゴリとAdvanced URL Filteringリアルタイム検出カテゴリを安全にテストするために作成されています。

テストページには*HTTP*および*HTTPS*接続でアクセスできます。ただし、*HTTPS*経由でテストページを表示するには、*SSL*復号化を有効にする必要があります。

特定の *Web* サイトの分類は、*Palo Alto Networks* の *URL* カテゴリ検索ツール Test A Site を使用して確認できます。

URLフィルタリング サブスクリプションに対応する手順に従います。

URL フィルタリングの確認

従来のURLフィルタリング サブスクリプションがある場合は、ファイアウォールがエンドユーザがアクセスするカテゴリのURLを正しく分類、適用、およびログに記録することをテストおよび検証します。

STEP 1 | 目的のURLカテゴリのWeb サイトにアクセスします。

ブロックされた URL カテゴリのサイトをテストすることを検討してください。test page (urlfiltering.paloaltonetworks.com/test-<*url-category*>) を使用すると、サイトに直接アクセスしないようにすることができます。たとえば、ブロック ポリシーでマルウェアをテストするには、「https://urlfiltering.paloaltonetworks.com/test-malware」を参照してください。

STEP 2 | トラフィックログとURフィルタリングログを確認して、ファイアウォールがサイトを正しく処理していることを確認します。

たとえば、組織のポリシーに違反するサイトにアクセスしたときに表示されるブロック ページを構成した場合は、テスト サイトにアクセスしたときにブロック ページが表示されることを確認します。

検証 Advanced URL Filtering

Advanced URL Filteringサブスクリプションをお持ちの場合は、Advanced URL Filteringに送信されたURLが適切に分析されていることをテストおよび検証します。

*Palo Alto Networks*では、リアルタイム検出（クラウドインライン分類）アクション設定を設定して、アクティブな*URL*フィルタリングプロファイルに対してアラートを表示することをお勧めします。これにより、リアルタイムで分析された *URL* の可視性が提供され、特定の *Web* 脅威に対して構成されたカテゴリ設定に基づいてブロック *(*またはポリシー設定に応じて許可*)* されます。

ファイアウォールは、特定の *URL* の検出された *URL* カテゴリに対して構成されたアクションの最も重大なアクションを実行します。たとえば、*example.com* が、それぞれアラート、ブロック、許可アクションが設定されたカテゴリであるリアルタイム検出、コマンドアンドコントロール、ショッピングに分類されるとします。ブロックは検出されたカテゴリからの最も重大なアクションであるため、ファイアウォールは*URL*をブロックします。

STEP 1 | 次の各テストURLにアクセスして、Advanced URL Filteringサービスが URLを正しく分類していることを確認します。

- マルウェア–http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-malware
- フィッシング–http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-phishing
- **C2**–http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-command-and-control
- グレーウェア–http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-grayware

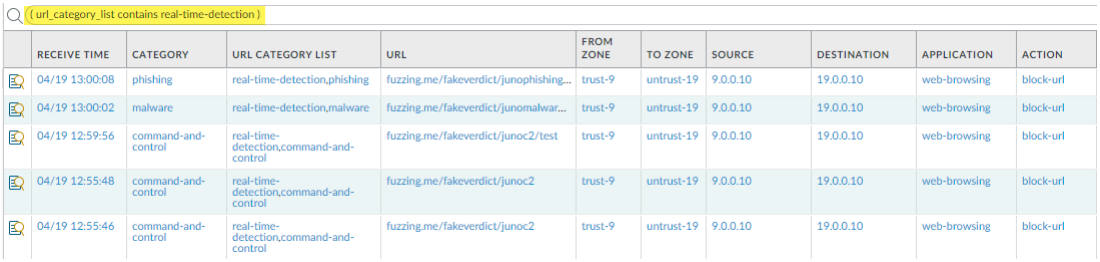
Cloud Inline Categorizationが有効になっている場合は、次のURLを使用して機能の動作をテストしてください。

- マルウェア–http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-malware
- フィッシング–http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
- グレーウェア–http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-grayware
- パーク–http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-parked
- アダルト–http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-adult

STEP 2 | Webアクティビティを監視して、テストURLがAdvanced URL Filteringによって適切に分類されていることを確認します。

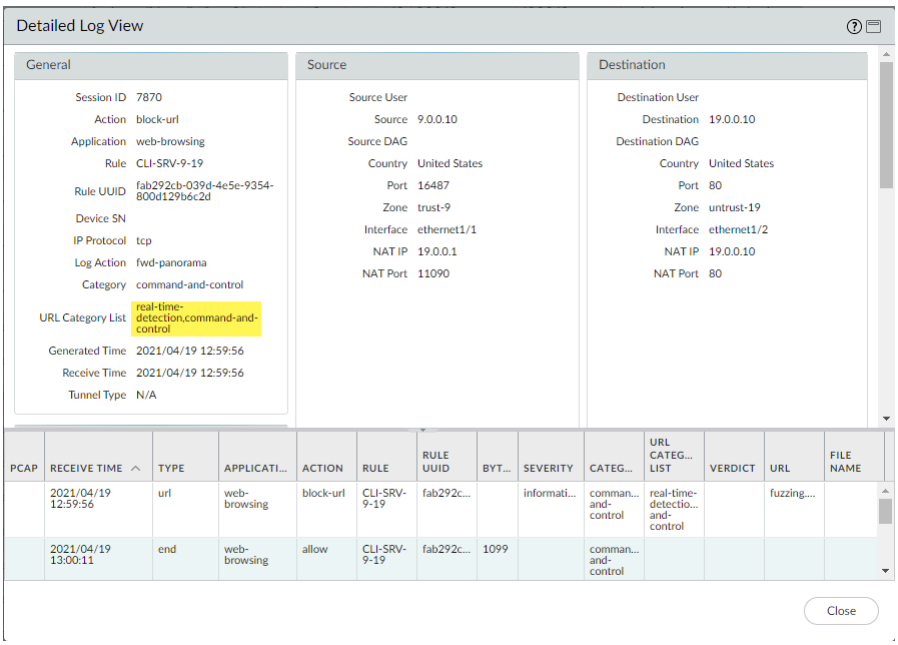
1. URLフィルタリングのログを次の方法でフィルタリングします。`(url_category_list contains real-time-detection)`。

   追加のWebページカテゴリの一致も表示され、PAN-DBで定義されているカテゴリに対応します。



2. ログを詳しく見て、各種類の Web の脅威が正しく分析され、分類されていることを確認します。

   次の例では、URL は real-time で分析され、コマンド・アンド・コントロール (C2) として定義する特徴を持っているものとして分類されます。C2 カテゴリにはリアルタイム検出よりも厳しいアクションが関連付けられているため (アラートではなくブロック)、URL はコマンド アンド コントロールに分類され、ブロックされます。



URLフィルタリング機能

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)	❑ Advanced URL Filteringライセンス (またはレガシーURLフィルタリングライセンス) 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URLフィルタリングのデプロイメントの基本コンポーネントを設定したら、次の機能の設定を検討してください。

- インライン分類
- SSL/TLS ハンドシェイク検査
- URL 管理オーバーライド
- 認証情報フィッシングの防止
- URL フィルタリング応答ページ
- セーフ サーチの適用
- (Prisma Accessのみ) Remote Browser Isolation (RBI) Integration (リモートブラウザ分離統合)

SSL/TLSハンドシェイクの検査

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

SSL/TLSハンドシェイクを調べると、ネットワークセキュリティが向上し、レガシーおよび高度なURLフィルタリングサブスクリプションが最適化されます。SSL/TLSハンドシェイク検査を有効にすると、高度なURLフィルタリングは、ハンドシェイク内のデータを使用してトラフィックを識別し、適用可能なセキュリティポリシールールをできるだけ早い段階で適用します。

仕組みはこちら

まず、クライアントHelloメッセージは、要求されたウェブサイトのホスト名を含むTLSプロトコル拡張である*Server Name Indication (SNI)*フィールドのためにスキャンされます。そして、ホスト名からトラフィックのURLカテゴリとサーバの宛先を決定します。次に、トラフィックはそのURLカテゴリに基づいて強制されます。SNIフィールドに悪意のあるWebサーバが存在するなど、脅威が検出された場合、またはセキュリティポリシールールによってWebサイトがブロックされた場合、ハンドシェイクは終了し、Webセッションは直ちに終了します。脅威が検出されず、ポリシーごとにトラフィックが許可されている場合、SSL/TLSハンドシェイクを完了し、セキュア接続を介してアプリケーション データを交換できます。

*SSL/TLS*ハンドシェイク検査中にブロックされたサイトでは、ファイアウォールが*HTTPS*接続をリセットするため、*URL*フィルタリングの応答ページは表示されません。接続のリセットによって*SSL/TLS*ハンドシェイクが終了し、応答ページによるユーザー通知が行われなくなります。ブラウザは標準の接続エラー メッセージを代わりに表示します。

成功した*SSL/TLS*ハンドシェイクとセッションの詳細は、トラフィックログと復号ログに記録されます。失敗したセッションの詳細は*URL*フィルタリングログで確認できますが、*SSL/TLS*ハンドシェイク中にブロックされた*Web*セッションの復号ログは生成されません。

- Strata Cloud Manager
- PAN-OS & Panorama

SSL/TLSハンドシェイクの検査(Strata Cloud Manager)

> ***Panorama***を使用して***Prisma Access***を管理している場合:
>
> *[**PAN-OS & Panorama**]* タブに切り替えて、そこにあるガイダンスに従います。
>
> ***Strata Cloud Manager***をお使いの場合は、こちらに進んでください。

SSLハンドシェイクの検査の要件は、SSLフォワードプロキシまたは SSLインバウンド検査のいずれかを介してSSL/TLSトラフィックを復号化することです。

STEP 1 | Prisma Accessライセンスに高度なURLフィルタリングのサブスクリプションが含まれていることを確認します。

1. **[Manage (管理)] > [Service Setup (サービスセットアップ)] > [Overview (概要)]**を選択し、ハイパーリンクされている[Quantity value (数量)]の値をクリックします。セキュリティサービスなどの情報が表示されます。
2. [Security Services (セキュリティサービス)]で[URL Filtering (URLフィルタリング)]の隣にチェックマークがあることを確認します。

STEP 2 | SSL フォワード プロキシ または SSL インバウンドインスペクション を介して SSL/TLS トラフィックを復号化することを確認します。

STEP 3 | CTD による SSL/TLS ハンドシェイクのインスペクションを有効にします。デフォルトでは、このオプションは無効になっています。

1. **[Manage (管理)] > [Configuration (構成)] > [Security Services (セキュリティサービス)] > [Decryption (復号化)]**を選択します。
2. [Decryption Settings (復号化の設定)]で、設定アイコンを選択します。次に、**[Inspect TLS Handshake Messages (TLS** ハンドシェイクメッセージを検査**)]** を選択します。

   あるいは、**`set deviceconfig setting ssl-decrypt scan-handshake <yes|no>`** CLI コマンドを使用することもできます。
3. 変更を保存します。[Decryption Settings (復号設定)]のTLSハンドシェイクメッセージの検査の設定が[Enabled (有効)]になっているはずです。

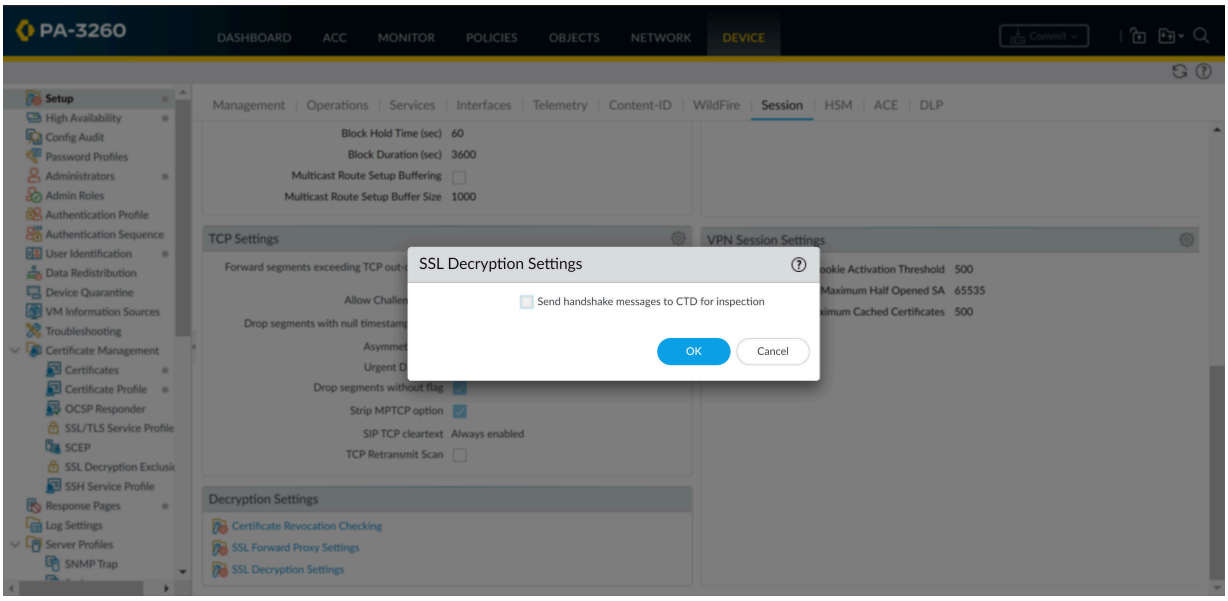
STEP 4 | **[Push Config (設定をプッシュ)]**して変更を保存し、コミットします。

SSL/TLSハンドシェイクの検査(PAN-OS & Panorama)

STEP 1 | デバイス>ライセンス を選択して、アクティブな Advanced URL Filtering ライセンスまたはレガシ URL Filtering ライセンスがあることを確認します。

STEP 2 | SSL フォワード プロキシ または SSL インバウンドインスペクション を介して SSL/TLS トラフィックを復号化することを確認します。

STEP 3 | CTD による SSL/TLS ハンドシェイクのインスペクションを有効にします。既定では、このオプションは無効になっています。



1. デバイス > **Setup** > セッション > 復号化設定 > **SSL** 復号化設定 を選択します。
2. [検査のために **CTD** にハンドシェイク メッセージを送信 を選択します。

   あるいは、**set deviceconfig setting ssl-decrypt scan-handshake<*yes*|*no*>**CLIコマンドを使用することもできます。
3. **OK** をクリックします。

STEP 4 | 設定の変更を **Commit (コミット)** します。

特定のサイトへのパスワード アクセスを許可する

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)	☐ Advanced URL Filteringライセンス (またはレガシーURLフィルタリングライセンス) 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

場合によっては、特定のカテゴリのウェブサイトへのパスワードアクセスを要求する必要がある場合があります。たとえば、従業員の安全性と幸福を脅かすURLカテゴリを会社がブロックする可能性があります。ただし、特定の従業員は、研究やその他の合法的な目的のために、これらのカテゴリへのアクセスを必要とする場合があります。安全性とビジネスニーズのバランスを取るには、URL管理者オーバーライドの実装が効果的な解決策となります。

URL管理者オーバーライドを作成するには、オーバーライドするカテゴリのアクションを設定します。次に、このカテゴリのサイトにアクセスするためにユーザが入力しなければならないパスワードを作成します。ユーザーがオーバーライドしたカテゴリのWebサイトにアクセスしようとすると、［Continue and Override (続行とオーバーライド)］応答ページが表示されます。このページでは、ウェブサイトがブロックされていることをユーザーに通知し、サイトに進むためのパスワードの入力を促します。

- Strata Cloud Manager
- PAN-OS & Panorama

特定のサイトへのパスワード アクセスを許可する (Strata Cloud Manager)

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

[PAN-OS & Panorama] タブに切り替えて、そこにあるガイダンスに従います。

***Strata Cloud Manager*をお使いの場合は、こちらに進んでください。**

STEP 1 | URLアクセス管理ダッシュボードに移動します。

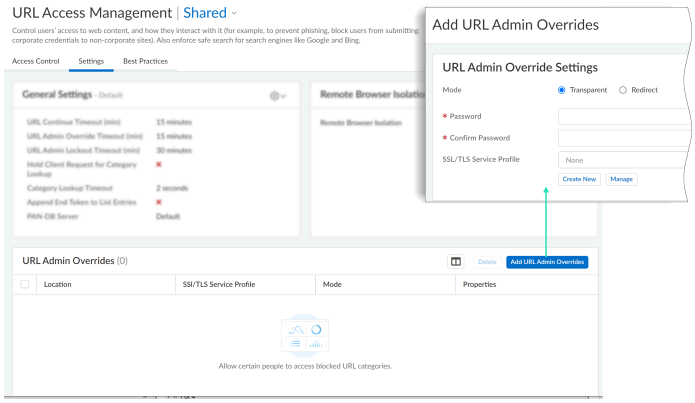
[Manage (管理)] > [Configuration (設定)] > [Security Services (セキュリティ サービス)] > [URL Access Management (URLアクセス管理)] を選択します。

STEP 2 | **Settings**[設定]を選択します。

STEP 3 | URL管理オーバーライド パスワードを作成します。

1. URL管理者オーバーライド、および**[Add URL Admin Overrides (URL**管理者オーバーライド**)]**の追加に移動します。
2. （任意）ユーザにパスワードの入力を求めるモードを選択します。
   - 透過：パスワード プロンプトは元の宛先URLから発信されたように見えます。ファイアウォールは、上書きするよう設定されたURLカテゴリのサイト宛てのブラウザトラフィックを傍受し、パスワードの入力を求めるHTTP302を発行します。これはvsysレベルごとに適用されます。
   - リダイレクト：指定したアドレス（IPアドレスまたはDNSホスト名）からパスワード プロンプトが表示されます。ファイアウォールは、上書きするよう設定されたURLカテゴリへのHTTPまたはHTTPSトラフィックを代行受信し、HTTP 302リダイレクトを使用してファイアウォール上のレイヤ3インターフェイスに要求を送信します。
3. **[Password (**パスワード**)]**を入力し、再度**[Confirm Password (**パスワードの確認**)]**に入力します。
4. （任意）**SSL/TLS** サービス プロファイルを選択します。

   SSL/TLS サービスプロファイルを作成および管理するには、それぞれ［**Create New (**新規作成**)**］および［**Manage (**管理**)**］をクリックします。
5. 変更を保存します。



STEP 4 | （オプション）オーバーライドアクセスとパスワードロックアウトの期間を設定します。

既定では、ユーザーはオーバーライドパスワードの入力に成功したカテゴリのウェブサイトに15分間アクセスできます。デフォルトまたはカスタム間隔が経過した後に、ユーザはパスワードを再入力する必要があります。

デフォルトでは、パスワードの入力に3回失敗すると、30分間、ユーザはブロックされます。ユーザーがデフォルトまたはカスタム期間ロックアウトされた後、ウェブサイトへのアクセスを再試行できます。

1. 一般設定をカスタマイズします。
2. [**URL Admin Override Timeout (URL**管理オーバーライドタイムアウト**)**]に、1～86,400の値(分単位)を入力します。
3. [**URL Admin Lockout Timeout (URL**管理ロックアウトタイムアウト**)**]に、1～86,400の値(分単位)を入力します。
4. 変更を保存します。

STEP 5 | パスワードアクセスが必要なURLカテゴリを指定します。

1. URLアクセス管理ダッシュボードの**[Access Control (**アクセス制御**)]**タブで 、 「[URL Access Management Profiles (URLアクセス管理プロファイル)]に移動し 、 プロファイルを変更または追加します。
2. [Access Control (アクセス制御)]で、パスワードによるアクセスを必要とするカテゴリを選択します。
3. すべてのカテゴリを選択した状態で、**[Set Access (**アクセス設定**)]**をクリックし、**[**オーバーライド**]**を選択します。

   強調表示されているカテゴリのサイトアクセスがオーバーライドと表示されているはずです。
4. 変更を保存します。

STEP 6 | URLアクセス管理プロファイルをセキュリティポリシールールに適用します。

URLアクセス管理プロファイルは、セキュリティポリシー規則が参照するプロファイルグループに含まれている場合にのみアクティブになります。

手順に従って、URLアクセス管理プロファイル（および任意のセキュリティプロファイル）をアクティブにします。設定が終わったら、必ず**Push Config (**設定のプッシュ**)**を行ってください。

特定のサイトへのパスワード アクセスを許可する許可 (PAN-OS & Panorama)

STEP 1 | URL管理オーバーライド パスワードを設定します。

1. **Device (デバイス) > Setup (設定) > Content-ID**の順に選択します。
2. **[URL** 管理オーバーライド] セクションで、[追加] をクリックします。
3. [場所]フィールドで、このパスワードを適用する仮想システムを選択します。
4. **[Password (**パスワード)]を入力し、再度**[Confirm Password (**パスワードの確認)]に入力します。
5. **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）を選択します。

   SSL/TLSサービスプロファイルでは、オーバーライドが設定されたサイトがHTTPSサイトの場合にファイアウォールからユーザーに提供される証明書を指定します。
6. ユーザーにパスワードを要求するモードを選択します。
   - 透過的：パスワード プロンプトは元の宛先 URL から発信されたように見えます。ファイアウォールは、上書きするよう設定されたURLカテゴリのサイト宛てのブラウザトラフィックを傍受し、パスワードの入力を求めるHTTP302を発行します。これはvsysレベルごとに適用されます。

     証明書が信頼されていない場合、クライアント ブラウザに証明書エラーが表示されます。
   - リダイレクト：指定したアドレス（IPアドレスまたはDNSホスト名）からパスワード プロンプトが表示されます。ファイアウォールは、上書きするよう設定されたURLカテゴリへのHTTPまたはHTTPSトラフィックを代行受信し、HTTP 302リダイレクトを使用してファイアウォール上のレイヤ3インターフェイスに要求を送信します。
7. **OK** をクリックします。

STEP 2 | （任意）上書きアクセスおよびパスワードロックアウトの期間を設定します。

既定では、ユーザーはオーバーライドパスワードの入力に成功したカテゴリのウェブサイトに15分間アクセスできます。デフォルトまたはカスタム間隔が経過した後に、ユーザはパスワードを再入力する必要があります。

デフォルトでは、パスワードの入力に3回失敗すると、30分間、ユーザはブロックされます。ユーザーがデフォルトまたはカスタム期間ロックアウトされた後、ウェブサイトへのアクセスを再試行できます。

1. URL Filtering （URL フィルタリング）セクションを編集します。
2. **[URL Admin Override Timeout (URL**管理オーバーライドタイムアウト)]に、1～86,400の値(分単位)を入力します。デフォルトでは、ユーザーはパスワー

ドを再入力せずに15分以内であればカテゴリ内のサイトにアクセスすることができます。

3. [**URL Admin Lockout Timeout (URL**管理ロックアウトタイムアウト)]に、1～86,400の値(分単位)を入力します。
4. **OK** をクリックします。

STEP 3 | （リダイレクト モードのみ）オーバーライド用に設定したカテゴリのサイトに Web 要求をリダイレクトするレイヤー 3 インターフェイスを作成します。

1. 管理プロファイルを作成して、インターフェイスに URL Filtering Continue and Override Page （URL フィルタリングの続行とオーバーライド ページ）の応答ページを表示できるようにします。
   1. **Network**（ネットワーク） > **Interface Mgmt**（インターフェイス **Mgmt**）を選択し、**Add**（追加）をクリックします。
   2. **Name** [名前]フィールドにプロファイル名を入力し、**Response Pages** [応答ページ]を選択してから **OK** をクリックします。
2. レイヤー 3 インターフェイスを作成します。作成した管理プロファイルが関連付けられていることを確認します（イーサネット インターフェイス ダイアログの**Advanced**（詳細） > **Other Info**（その他の情報） タブ)。

STEP 4 | (リダイレクト モードのみ) 証明書エラーを表示せずにユーザーを透過的にリダイレクトするには、オーバーライド用にURLカテゴリで設定されたサイトにWebリクエストをリダイレクトする IP アドレスに一致する証明書をインストールします。自己署名証明書を生成するか、外部 CA によって証明された証明書をインポートできます。

自己署名証明書を使用するには、以下のとおり、まずルート CA の証明書を作成してから、その CA を使用して URL 管理オーバーライドに使用する証明書に署名する必要があります。

1. ルート CA 証明書を作成するには、**Device** > **Certificate Management** > **Certificates** > **Device Certificates**(デバイス > 証明書の管理 > 証明書 > デバイス証明書) の順に選択し、**Generate**(生成) をクリックします。**Certificate Name** [証明書名]に「RootCA」などの名前を入力します。**Signed By** [署名者]フィールドの値は選択しないでください（その証明書が自己署名証明書であることを示すものであるため）。[認証局] チェックボックスがオンになっていることを確認してから [生成] をクリックすると、証明書が生成されます。
2. URL 管理オーバーライドに使用する証明書を作成するには、[生成] をクリックします。[証明書名] に名前を入力し、インターフェイスの DNS ホスト名または IP アドレスを [共通名] として入力します。**Signed By** [署名者]フィールドで、前の手順で作成した CA を選択します。IP アドレスの属性を追加し、override アクションが設定されている URL カテゴリに Web 要求をリダイレクトするレイヤー 3 インターフェイスの IP アドレスを指定します。
3. 証明書を **Generate**[生成] します。
4. クライアントが証明書を信頼するように設定するには、[デバイス証明書] タブで CA 証明書を選択し、[エクスポート] をクリックします。次に、証明書を信頼されたルート CA としてすべてのクライアント ブラウザにインポートする必要があります。インポートはブラウザから手動で設定するか、または証明書を Active Directory のグループ ポリシー オブジェクト（GPO）の信頼されたルートに追加します。

STEP 5 | アクセスを有効にするためにオーバーライド パスワードが必要な URL カテゴリを指定します。

1. オブジェクト > **URL** フィルタリング を選択し、既存の URL フィルタリング プロファイルを選択するか、または新しい URL フィルタリング プロファイルを 追加 を選択します。
2. [カテゴリ] タブで、パスワードを必要とする各カテゴリの [アクション] を **[override]** に設定します。
3. URL フィルタリング プロファイルの残りのセクションをすべて完了し、[**OK**] をクリックしてプロファイルを保存します。

STEP 6 | URL フィルタリング プロファイルをセキュリティ ポリシー ルールに適用し、アクセスのためにパスワードの上書きを要求するサイトにアクセスできるようにします。

1. [ポリシー > セキュリティ] を選択し、適切なセキュリティ ポリシーを選択して変更します。
2. [アクション] タブを選択して、[プロファイル設定] セクションで、**[URL** フィルタリング] のドロップダウンをクリックし、プロファイルを選択します。
3. **OK** をクリックして保存します。

STEP 7 | 設定を **Commit**（コミット）します。

認証情報フィッシングの防止

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

フィッシング サイトとは、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提供する資格情報を盗もうとする正当な Web サイトを偽装するサイトです。フィッシングのメールがネットワークに侵入すると、いずれかのユーザーがリンクをクリックして認証情報を提供するだけで、セキュリティの穴が顕在化してしまいます。サイトの URL カテゴリに基づき、ユーザーが企業の認証情報を送信できるサイトを制御することで、進行中のフィッシング攻撃を検知・阻止できるので、証明書の盗難を防止します。これにより、信頼されていないサイトに資格情報を送信できないようにし、企業サイトや認可されたサイトへの資格情報の送信を許可することができます。

ウェブサイトに送信されるユーザー名およびパスワードをスキャンし、それらの送信を正当な企業の認証情報と比較することで、認証情報フィッシング防止が行われます。ウェブサイトの URL カテゴリに基づき、企業の認証情報を送信するのを許可あるいはブロックするウェブサイトを選択できます。制限を受けたカテゴリのサイトに資格情報を送信しようとするユーザーを検出すると、ユーザーが資格情報を送信できないようにするブロック応答ページを表示するか、特定のURLカテゴリのサイトに資格情報を送信しないように警告する続行ページを表示します。応答ページをカスタマイズすることで、正規の非フィッシング サイトであっても、企業の認証情報を再利用しないようユーザーを教育できます。

次のトピックでは、認証情報の送信を検知するために使用できる各種の方法、および認証情報フィッシング防止を設定する方法を説明します。

- 企業の認証情報送信をチェックする方式
- Windows ベースの User-ID エージェントを使用する認証情報検知の設定
- 認証情報フィッシング防御を有効にする

企業の認証情報送信をチェックする方式

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

資格情報のフィッシング防止を有効にする前に、有効な企業資格情報がWebページに送信されたかどうかを確認するために使用する方法を決定します。

送信された認証情報をチェックする方式	**User-ID** 設定の要件	この方法では、ユーザーが **Web** サイトに送信する企業のユーザー名および/またはパスワードをどのように検出しますか？
Group Mapping（グループ マッピング）	ファイアウォール上の グループ マッピング設定	ファイアウォールは、制限されているサイトにユーザーが送信するユーザー名が有効な企業ユーザー名と一致するかどうかを判断することを確認します。 これを行うため、ファイアウォールは、送信されるユーザー名をユーザーとグループのマッピング テーブルのユーザー名のリストと照合し、ユーザーが制限されているカテゴリのサイトに企業ユーザー名を送信する時に検出します。 この方法では、LDAP グループ メンバーシップに基づいて企業ユーザー名の送信のみがチェックされるため、設定は簡単ですが、誤検出が多くなる傾向があります。
IPユーザー マッピング	IPユーザマッピングは、認証ポリシーや認証ポータル、GlobalProtectを通じてユーザーマッピングの識	ファイアウォールは、ユーザーが制限されているサイトに送信するユーザー名がログインユーザー名の IP アドレスにマッピングされているかどうかを確認します。 これを行うため、ファイアウォールは、ログイン中のユーザー名およびウェブサイトに送信されたユーザー名を自身の IP アドレス対ユーザーのマッピング テーブルと一致させ、ユーザーが制限されているカテゴリ

送信された認証情報をチェックする方式	User-ID 設定の要件	この方法では、ユーザーが Web サイトに送信する企業のユーザー名および/またはパスワードをどのように検出しますか？
	別が行われます。	のサイトに企業ユーザー名を送信していればそれを検出します。 この方式は、セッションに関連するログイン済みのユーザー名の IP アドレスを IP アドレス対ユーザー名のマッピング テーブルと照合するため、企業のユーザー名の送信を検出するのに適した方式ですが、企業のパスワードの送信を検出することはできません。企業のユーザー名およびパスワードの送信を検出したい場合は、ドメイン認証情報フィルタ方式を使用する必要があります。
ドメイン認証情報フィルタ	User-ID 認証情報サービス アドオンと共に設定された Windows の User-ID エージェント - および - IPユーザマッピングは、認証ポリシーや認証ポータル、GlobalProtectを通じてユーザーマッピングの識別が行われます。	ファイアウォールは、ユーザーが送信するユーザー名とパスワードが、同じユーザーの企業ユーザー名とパスワードと一致するかどうかを判断することを確認します。 これを行うため、ファイアウォールは次のように、送信される認証情報を有効な企業ユーザー名とパスワードと照合し、送信されるユーザー名が、ログインユーザー名の IP アドレスに対応することを確認できる必要があります。 • 企業のユーザー名およびパスワードを検出する–ファイアウォールは User-ID 認証情報サービス アドオンを備えた Windows の User-ID エージェントから、ブルーム フィルタと呼ばれる安全なビットマスクを取得します。このアドオン サービスはディレクトリをスキャンしてユーザー名およびパスワードのハッシュを見つけ、それを安全なビットマスク（ブルーム フィルタ）の形に解体して Windows User-ID エージェントに送付します。ファイアウォールは、Windows User-ID エージェントから定期的にブルームフィルターを取得します。制限されたカテゴリに認証情報を送信しているユーザーを検知した場合は必ず、ブルーム フィルタを再構築し、マッチするユーザー名およびパスワードのハッシュを探します。ファイアウォールは、User-ID 認証情報サービスのアドオンを実行している単体の Windows の User-ID エージェントにのみ接続できます。 • 認証情報がログイン中のユーザー名のものであることを検証する–ファイアウォールは、ログイン中のユーザー名の IP アドレスと、自身の IP アドレス

送信された認証情報をチェックする方式	User-ID 設定の要件	この方法では、ユーザーが Web サイトに送信する企業のユーザー名および/またはパスワードをどのように検出しますか？
		対ユーザー名のマッピング テーブルに含まれる検出されたユーザー名との間のマッピングを探します。 ドメイン資格情報メソッドの詳細については、「Windows ベースのユーザー ID エージェントを使用した資格情報検出の構成」を参照してください。

Windows の User-ID エージェントを使用する認証情報検知の設定

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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

ドメイン認証情報フィルタ検知により、Web ページに送信されたパスワードをファイアウォールが検出できるようになります。この認証情報検知方式には Windows の User-ID エージェントおよび、読み取り専用ドメイン コントローラ（*RODC*） にインストールする User-ID エージェントのアドオンである User-ID 認証情報サービスが必要になります。

ドメイン認証情報フィルタの検出方式は、*Windows* の *User-ID* エージェントでのみサポートされています。*PAN-OS* 統合 *User-ID* エージェントを使用してこの方式の認証情報検知を設定することはできません。

RODC は、ドメイン コントローラがホストするアクティブディレクトリ データベースの読み取り専用のコピーを保持する Microsoft Windows サーバーです。例えば、ドメイン コントローラが企業本部に位置している場合、RODC をリモートネットワークのロケーションにデプロイし、ローカル認証サービスを利用可能にできます。ドメイン コントローラのディレクトリにアクセスするために認証情報検知を有効化する必要がないこと、一部のユーザーを対象にして認証情報検知をサポートできることなど、、User-ID エージェントを RODC 上にインストールすることが役立つ理由はいくつかあります。RODC がホストするディレクトリは読み取り専用であるため、ドメイン コントローラ上でディレクトリ内のコンテンツの安全が確保されます。

証明書の検出のために *RODC* に *Windows* の *User-ID* エージェントをインストールする必要があるため、ベストプラクティスとして別のエージェントを展開してください。*RODC* にインストールされている *User-ID* エージェントを使用して *IP* アドレスをユーザーにマップしないでください。

RODC 上に User-ID エージェントをインストールした後、User-ID 認証情報サービスがバックグラウンドで実行され、ディレクトリをスキャンし、RODC パスワード複製ポリシー（PRP）（このリストに載せるユーザーを定義可能）にリストアップされているグループ メンバーのユーザー名およびパスワードのハッシュを探します。その後、収集されたユーザー名およびパスワードのハッシュを User-ID 認証情報サービスが引き受け、データを解体してブルーム フィルタと呼ばれるビットマスクの携帯にします。コンパクトなデータ構造を持つブルーム フィルタは、エレメント（ユーザー名あるいはパスワードのハッシュ）が一連のエレメント（RODC に対して複製を許可した一連の認証情報）のメンバーであるかどうかを確認する上で、セキュアな方法を提供します。User-ID 認証情報サービスはブルーム フィルタを Windows の User-ID エージェントに転送します。ファイアウォールは定期的に最新のブルーム フィルタを User-ID エージェントから受け取り、送信されたユーザー名およびパスワードのハッシュを検知するためにそれを使用します。設定に応じて、その後ファイアウォールは Web ページに対する有効なパスワード送信をブロック、通知、あるいは許可するか、フィッシングの危険についてユーザーに警告を伝える応答ページを表示しつつ、送信を続行することを許可します。

このプロセス全体を通じて、User-ID エージェントは一切パスワードのハッシュを保存・表示したりせず、またそれをファイアウォールに転送することもありません。ブルーム フィルタの形に解体されたパスワードのハッシュを復元する方法はありません。

STEP 1 | Windows ユーザー ID エージェント を使用してユーザー マッピングを構成します。

> 資格情報の検出を有効にするには、*RODC* に *Windows* の *User-ID* エージェントをインストールする必要があります。サポートされているサーバーのリストについては、Compatibility Matrix（互換性マトリックス）を参照してください。この目的のために別個の *User-ID* エージェントをインストールしてください。

User-ID をセットアップしてドメイン認証情報フィルタ検知を有効化する際に、頭にとどめておくべき重要事項：

- 資格情報フィッシング検出の有効性は、RODCの設定によって異なります。RODC Administration (RODC管理)のベストプラクティスと推奨事項を必ず確認してください。
- User-ID ソフトウェア更新のダウンロード：
  - User-ID エージェント Windows インストーラ–UaInstall-x.x.x-x.msi。
  - User-ID エージェント認証情報サービス Windows インストーラ–UaCredInstall64-x.x.x-x.msi。
- LDAP を介してアクティブディレクトリを読み取る権限を持つアカウントを使用して RODC に User-ID エージェントおよびユーザーエージェント認証情報サービスをインストールします。
  - User-ID エージェント認証情報サービスでは、ローカルシステムのアカウントを使ってログを記録する権限が必要になります。詳細については、User-ID エージェント専用のサービスアカウントを作成を参照してください。
  - サービス アカウントが RODC 上のローカル管理者グループのメンバーでなければなりません。

STEP 2 | （バックグラウンドで稼働して許可された認証情報をスキャンする）User-ID エージェントおよびユーザーエージェント認証情報サービスを有効化し、情報を共有します。

1. RODC サーバーで User-ID エージェントを起動します。
2. **Setup (**セットアップ**)** を選択し、Setup (セットアップ) セクションを編集します。
3. **Credentials (**認証情報**)** タブを選択します。このタブは、User-ID エージェント認証情報サービスをインスール済みである場合のみ表示されます。
4. **Import from User-ID Credential Agent (User-ID** 認証情報エージェントからインポート**)** を選択します。これにより、ユーザーおよび対応するパスワードのハッシュを提供するために User-ID 認証情報エージェントが作成するブルーム フィルタを User-ID エージェントがインポートできるようになります。
5. **OK** をクリックして設定を **Save (**保存**)** し、**Commit (**コミット**)** します。

STEP 3 | RODC ディレクトリにて、認証情報送信検知の対象にしたいユーザーグループを定義します。

- 認証情報送信を適用するグループが Allowed RODC Password Replication Group (許可された RODC パスワード複製グループ) に追加されていることを確認します。
- Allowed RODC Password Replication Group (許可された RODC パスワード複製グループ) に含まれるどのグループも、デフォルトで Denied RODC Password Replication Group 拒

否された RODC パスワード複製グループ) に含まれないことを確認します。両方にリストアップされたグループは、認証情報フィッシング防止の適用対象にはなりません。

STEP 4 | 次のタスクに進みます。

ファイアウォールで資格情報フィッシング防止 を設定します。

認証情報フィッシング防御のセットアップ

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)	❑ Advanced URL Filteringライセンス (またはレガシーURLフィルタリングライセンス) 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

設定するユーザー資格情報検出方法を決定したら、資格情報フィッシング攻撃の成功を防ぐために、次の手順を実行します。

クレデンシャルフィッシング防止を有効にする前に、ファイアウォールで構成するプライマリユーザー名が *samAccountName* 属性を使用していることを確認します。資格情報フィッシング防止機能は代替属性をサポートしていません。

- Strata Cloud Manager
- PAN-OS & Panorama

認証情報フィッシング防御のセットアップ (Strata Cloud Manager)

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

[PAN-OS & Panorama] タブに切り替えて、そこにあるガイダンスに従います。

***Strata Cloud Manager*をお使いの場合は、こちらに進んでください。**

STEP 1 | 使用するユーザ資格情報の検出方法を設定します。

各方法の詳細は、「企業認証情報の提出をチェックする方法」を参照してください。

- IPユーザーマッピングでは、ローカルユーザーとグループ、アイデンティティ再配布、またはプリズマアクセス認証を設定します。
- ドメイン資格情報フィルタを使用するには、アイデンティティの再配布とローカルユーザーとグループまたは認証を設定します。

- グループマッピングを使用するには、ローカルユーザーとグループまたは認証をセットアップします。

STEP 2 | ユーザー資格情報の送信を監視するトラフィックを復号化するための復号化ポリシー ルールを作成します。

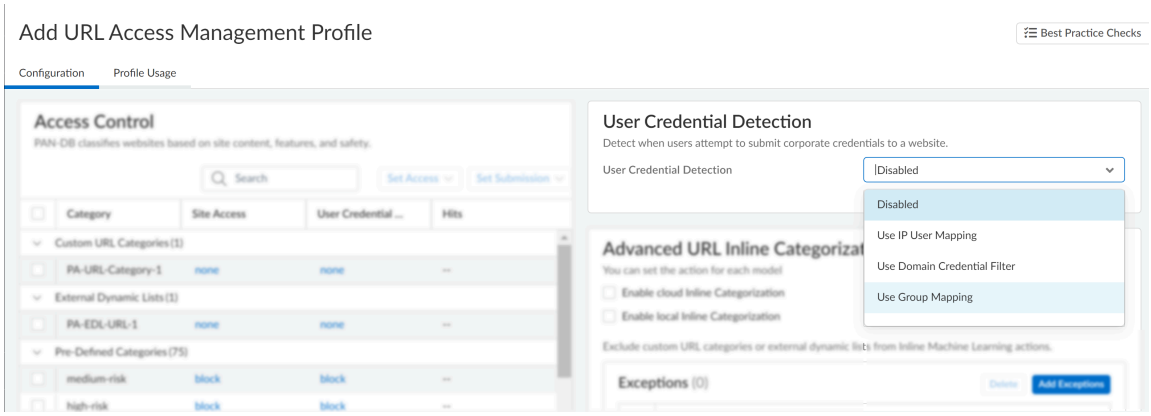
STEP 3 | URLアクセス管理プロファイルを作成または変更します。

1. **[Manage (管理)] > [Configuration (設定)] > [NGFW and Prisma Access] > [Security Services (セキュリティサービス)] > [URL Access Management (URLアクセス管理)]**を順に選択します。
2. [URL Access Management Profiles (URLアクセス管理プロファイル)]で、既存のプロファイルを選択するか、**[Add Profile (プロファイルの追加)]**を選択します。

STEP 4 | ユーザー証明書検出の設定を行います。

1. [User Credential Detection (ユーザー資格情報の検出)]で、**[User Credential Detection (ユーザー資格情報検出)]**方法を選択します。
   - **Use IP User Mapping (IP** ユーザー マッピングの使用)–企業のユーザー名送信が正当なものであり、セッションの送信元 IP アドレスにログイン ユーザー名がマッピングすることが確認されます。そうするために、Prisma Accessは送信されるユーザー名およびセッションの送信元IPアドレスをIPアドレス対ユーザー名のマッピング テーブルと照合します。
   - **Use Domain Credential Filter (**ドメイン認証情報フィルタを使用)–送信される企業ユーザー名とパスワードが正当なものであるか確認し、ユーザー名が、ログイン中のユーザーの IP アドレスに対応することを確認します。
   - グループ マッピングを使用–ユーザーをグループにマップする場合に設定されたユーザーからグループへのマッピング テーブルに基づいて有効なユーザー名の送信をチェックしますディレクトリの任意の部分や、ITなどの機密性の高いアプリケーションにアクセスできる特定のグループに対して資格情報検出を適用できます。

     この方法は、一意に構造化されたユーザ名を持たない環境で誤検出が発生しやすくなります。そのため、この方法は高価値なユーザーアカウントを保護する用途でのみ使用するようにしてください。



2. **[Valid Username Detected Log Severity (有効なユーザ名の検出ログの重大度)]**で、ファイアウォールが企業資格情報の提出を検知したときにログに記録する重大度レベルを選択します。
   - **high**（高）
   - **(デフォルト)中**
   - 低

STEP 5 | ファイアウォールが企業資格情報の提出を検出した場合のアクションを設定します。

1. [Access Control (アクセス制御)]で、**[Site Access (サイトアクセス)]**が[許可]または[警告]に設定されている各URLカテゴリの**[User Credential Submission (ユーザー資格情報送信)]**のアクションを選択します。

   次のアクションから選択できます。
   - （推奨）アラート：ユーザは所定のURLカテゴリのWebサイトにクレデンシャルを送信できますが、これが発生するたびにURLフィルタリング ログが生成されます。
   - （デフォルト）**allow (許可)**–ユーザーが認証情報をWebサイトに送信することを許可します。
   - （推奨）ブロック–ユーザが所定のURLカテゴリのWebサイトにクレデンシャルを送信できないようにします。ユーザーが認証情報を送信しようとする際、ファイアウォールはアンチフィッシングブロックページを表示します。
   - **continue**（続行）–ユーザーが認証情報を送信しようとした際、Anti-Phishing continue Page（アンチフィッシング続行ページ）応答ページをユーザーに表示します。ユーザーがウェブサイトに進むには、応答ページで［続行］を選択する必要があります。
2. プロファイルを保存します。

STEP 6 | URLアクセス管理プロファイルをセキュリティポリシールールに適用します。

1. **[Manage (管理)] [> Configuration (設定)] > [NGFW and Prisma Access] > [Security Services (セキュリティサービス)] > [Security Policy (セキュリティポリシー)]**を順に選択します。
2. [Security Policy Rules (セキュリティポリシー規則)]で、セキュリティポリシー規則を作成または選択します。
3. **[Actions (アクション)] > [Profile Group (プロファイルグループ)]**を選択し、[URLアクセス管理]プロファイルグループを選択します。
4. ルールを保存します。

STEP 7 | **[Push Config (設定をプッシュ)]**をクリックします。

認証情報フィッシング防御のセットアップ (PAN-OS & Panorama)

STEP 1 | ユーザIDを有効化。

メソッドで企業資格情報の送信を確認する方法 には、次の異なる User-ID 構成が必要です。

- グループマッピング–ユーザが有効な企業ユーザ名を送信しているかどうかを検出し、ユーザをグループにマッピングするように要求します。
- IP ユーザ マッピング–ユーザが有効な企業ユーザ名を送信しているかどうか、およびユーザ名がログイン ユーザ名と一致するかどうかを検出します。IP アドレスをユーザにマッピングする必要があります。
- ドメイン資格情報フィルター–ユーザーが有効なユーザー名とパスワードを送信しているかどうか、およびそれらの資格情報がログインユーザーに属しているかどうかを検出します– WindowsベースのUser-IDエージェントでクレデンシャル検出を構成し、IPアドレスをユーザーにマッピングする必要があります。

STEP 2 | 最良の URL フィルタリング プロファイルを設定し、マルウェアあるいは悪意のあるコンテンツをホストしていることが分かっている URL から確実に保護されるようにします。

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. すべての既知の危険なURLカテゴリであるマルウェア、フィッシング、ダイナミックDNS、未知、コマンド& コントロール、エクストリミズム、著作権侵害、プロキシ回避・アノニマイザー、新しく登録されたドメイン、グレイウェアおよびパークドへのアクセスをブロックします。

STEP 3 | ユーザー資格情報の送信を監視するトラフィックを復号化するための復号化ポリシー ルールを作成します。

STEP 4 | 許可されたURLカテゴリにあるウェブサイトへの企業認証情報の提出を検出します。

ファイアウォールは、サイトの*URL*カテゴリのチェックを有効にしても、信頼済みサイトへの認証情報の送信はチェックせず、最高のパフォーマンスが得られます。信頼済みサイトは、*Palo Alto Networks* が悪意のある攻撃やフィッシング攻撃を確認していないサイトを表しています。この信頼済みサイトリストの更新は、アプリケーションおよび脅威コンテンツ更新を通じて配信されます。

1. 変更するURLフィルタリング プロファイル（**Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > URL Filtering (URL**フィルタリング**)**）を選択します。
2. **[User Credential Detection (**ユーザー資格情報検出**)**］を選択し、いずれかのユーザ資格情報検知方式を選択します。

   プライマリ ユーザー名の形式が、*User-ID* ソースが提供するユーザー名の形式と同一であることを確認します。

   - **Use IP User Mapping (IP** ユーザー マッピングの使用**)**–企業のユーザー名送信が正当なものであり、セッションの送信元 IP アドレスにログイン ユーザー名がマッピン

グすることが確認されます。そうするために、ファイアウォールは送信されるユーザー名およびセッションの送信元 IP アドレスを IP アドレス対ユーザー名のマッピング テーブルと照合します。この方法を使用するには、「ユーザーにIPアドレスをユーザーにマップする」で説明されているユーザー マッピング方法のいずれかを設定します。

- **Use Domain Credential Filter**（ドメイン認証情報フィルタを使用）–有効な企業ユーザー名とパスワード送信をチェックし、ユーザー名が、ログイン ユーザーの IP アドレスに対応することを確認します。この方式をセットアップする方法については、WindowsベースのUser-IDエージェントを使用する認証情報検知を設定を参照してください。
- グループ マッピングを使用する] - ユーザーをグループにマップする場合に設定されたユーザーからグループへのマッピング テーブルに基づいて有効なユーザー名の送信をチェックします

  グループ マッピングの場合、ITのような最も重要なアプリケーションにアクセスできる特定のグループのため、あるいはディレクトリのいずれかの部分に認証情報検知を割り当てられます。

  この方法は、ユーザー名が一意な構造でない環境では誤検出が多くなりがちです。そのため、この方法は高価値なユーザーアカウントを保護する用途でのみ使用するようにしてください。

3. ファイアウォールが企業の認証情報送信の検知をロギングするために使用する **Valid Username Detected Log Severity (**有効なユーザー名が検知されたログの重大度**)** を設定します。デフォルト設定では、ファイアウォールはこれらのイベントの重大度を中としてログに記録します。

STEP 5 | 許可されたサイトへの認証情報の送信をブロック（あるいは警告）します。

1. **Categories (**カテゴリ**)** を選択します。
2. **Site Access (**サイト アクセス**)** を許可する各 Category (カテゴリ) について、**User Credential Submissions (**ユーザー証明書送信**)** を扱う方法を選択します。
   - **alert**（アラート） – 認証情報を Web サイトに送信することをユーザーに許可しますが、ユーザーがこのカテゴリのサイトに認証情報を送信するたびに、URL フィルタリング ログを生成します。
   - **allow (**許可**)**–（デフォルト）ユーザーが認証情報を Web サイトに送信することを許可します。
   - **block**（ブロック） – ユーザーが認証情報を Web サイトに送信することをブロックします。ユーザーが認証情報を送信しようとする際、ファイアウォールはアンチフィッシングブロックページを表示し、認証情報の送信を阻止します。
   - **continue (**続行**)**：ユーザーが認証情報を送信しようとした際、Anti-Phishing continueページをユーザーに表示します。ユーザーが送信を続行するためには、応答ページで Continue (続行) を選択する必要があります。
3. **OK** を選択して URL フィルタリング プロファイルを保存します。

STEP 6 | 認証情報検知が設定されたURL フィルタリング プロファイルをセキュリティポリシールールに適用します。

1. **Policies (**ポリシー**) > Security (**セキュリティ**)**を選択し、セキュリティポリシールールを**Add**（追加）または変更します。
2. **Actions** （アクション） タブで **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. 新規あるいは更新された **URL Filtering (URL** フィルタリング**)** プロファイルを選択し、セキュリティポリシー ルールに割り当てます。
4. **OK** をクリックし、セキュリティポリシー ルールを保存します。

STEP 7 | 設定を **Commit**（コミット）します。

STEP 8 | ファイアウォールが検知した認証情報の送信を監視します。

マルウェアおよびフィッシング サイトを訪問したユーザーの数を確認するには、***ACC*** > ***Hosts Visiting Malicious URLs*** (有害な ***URL*** にアクセスしているホスト) を選択します。

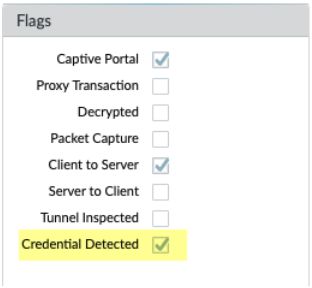
Monitor (監視) > **Logs** (ログ) > **URL Filtering** (**URL** フィルタリング) を選択します。

新たに **Credential Detected** (検出された認証情報) 列には、正当な認証情報を含む HTTP POST リクエストをファイアウォールが検知したイベントが表示されます。

	CATEGORY	APPLICATION	ACTION	CREDENTIAL DETECTED
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes

この列を表示するためには、いずれかの列の見出しにカーソルを合わせ、矢印をクリックして表示したい列を選択します。

ログ エントリの詳細は、認証情報の送信も示唆します。



STEP 9 | 認証情報送信の検知を検証し、トラブルシューティングを行います。

- 次の CLI コマンドを使って認証情報検知の統計情報を表示します。

```
> show user credential-filter statistics
```

このコマンドの出力は、ファイアウォールが認証情報の送信を検知するために設定した方式によって異なります。例えば、Domain Credential Filter (ドメイン認証情報フィルタ) 方法が URL フィルタリング プロファイルで設定されている場合、ブルーム フィルタをファイアウォールに転送した User-ID エージェントのリストが、ブルーム フィルタに含まれている認証情報の数と共に表示されます。

- (Group Mapping メソッドのみ) 次の CLI コマンドを使用して、Group Mapping 資格情報検知が有効になっている URL Filtering プロファイルの数や、制限付きサイトに資格情報を送信しようとしたグループ メンバーのユーザー名など、グループ マッピング情報を表示します。

  ```
  > show user group-mapping statistics
  ```

- (Domain Credential Filter method only) 次の CLI コマンドを使用して、firewall にマッピングを送信しているすべての Windows ベースの User-ID エージェントを表示します:

  ```
  > show user user-id-agent state all
  ```

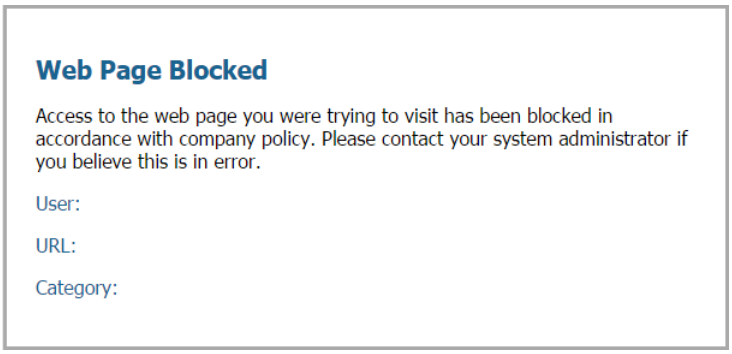
  コマンド出力には、ファイアウォールが各エージェントから受信したブルーム フィルター更新の数、ブルーム フィルターの更新が処理に失敗した場合、および最後のブルーム フィルターの更新から経過した秒数を含むブルーム フィルター数が表示されるようになりました

- （ドメイン認証情報フィルタ方式のみ）Windows ベースの User-ID エージェントが、ファイアウォールへの BF（ブルーム フィルタ）プッシュを参照するログ メッセージを表示します。User-ID エージェント インターフェイスにて、**Monitoring (**モニタリング**) > Logs (**ログ**)**を選択します。

URL フィルタリング応答ページ

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URLフィルタリング応答ページは、リクエストされたURLへのアクセスが制限されたときにユーザーに通知します。ブロック、続行、または上書きアクションが設定されたカテゴリにサイトが属している場合、またはサイトまたはカテゴリへの資格情報の送信がブロックされている場合、アクセスが制限されることがあります。ユーザーが検索エンジンに対して最も厳格なセーフサーチ設定を構成しておらず、セキュリティ ポリシー ルールでセーフサーチが強制されている場合、アクセスも制限されます。5 つの事前定義された応答ページ これらの理由を説明するために存在します。一部の応答ページはアクセスを完全にブロックしますが、他のページは条件付きアクセスを許可します。たとえば、[URL Filtering Continue and Override Page (URLフィルタリングの続行と上書きページ)]または[Phishing Continue Page (フィッシング対策の続行ページ)]が表示された場合、ユーザーは[続行]をクリックしてサイトにアクセスできます (URL管理者の上書きが有効になっている場合を除く)。



一般に、応答ページには、ページにアクセスできない理由が示され、ユーザー、URL、およびURL カテゴリが一覧表示されます。ただし、回答ページの内容や外観はカスタマイズできます。たとえば、通知メッセージを変更したり、利用規定へのリンクを貼ったり、企業ブランドを追加したりできます。

応答ページの外観は、*PAN-OS*ソフトウェアのリリースによって異なる場合があります。ただし、機能は変わらず同じものです。

特定のニーズに合わせて応答ページをカスタマイズできることに留意してください。

SSL/TLSハンドシェイク検査が有効な場合、ブラウザは応答ページを表示しません。

- 事前定義されたURLフィルタリング応答ページ
- URLフィルタリング応答ページのオブジェクト
- URLフィルタリング応答ページのカスタマイズ

事前定義されたURLフィルタリング応答ページ

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

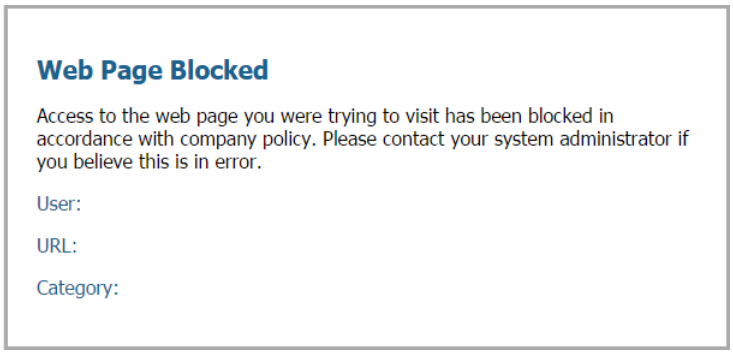
要求されたURLへのアクセスが制限されている場合、URLフィルタリング応答ページがWebブラウザーに表示されます。各応答ページには、ページにアクセスできない理由が説明されており、ほとんどのページには、ユーザー、要求されたURL、およびブロック アクションをトリガーしたURLカテゴリに関する情報がリストされています。

異なる*PAN-OS*ソフトウェア リリース間では、応答ページの外観が異なる場合があります。ただし、機能は変わらず同じものです。

特定のニーズに合わせて応答ページをカスタマイズできることに留意してください。

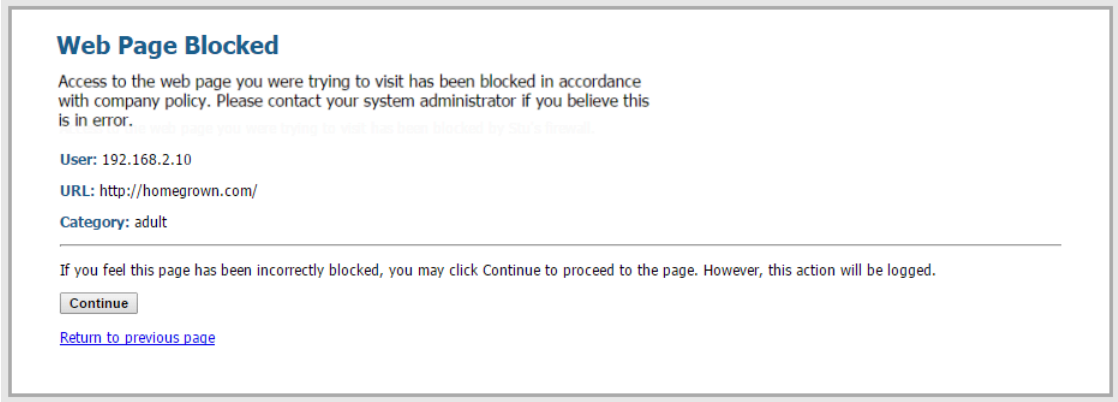
- **URL** フィルタリングおよびカテゴリ一致ブロック ページ

  URL フィルタリング プロファイルによってブロックされたアクセス、または URL カテゴリがセキュリティ ポリシー ルールによってブロックされているため。



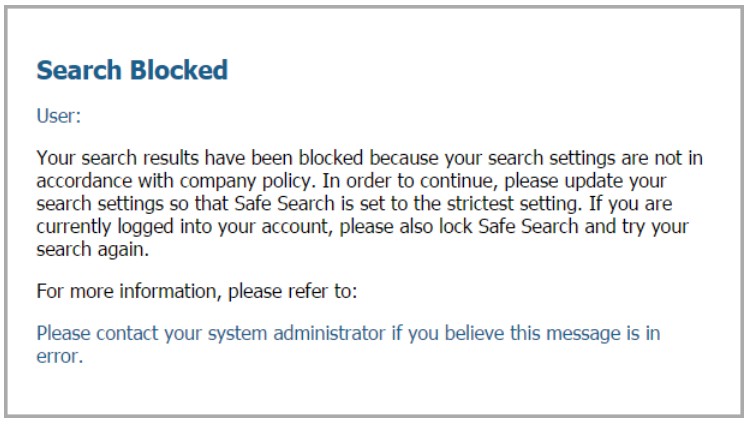
- **URL** フィルタリングの続行とオーバーライド ページ

  Continue (続行**)** をクリックすることでユーザーがブロックをバイパスできる、最初のブロック ポリシーを持つページです。URL 管理の上書きを有効にした (特定のサイトへのパスワードアクセスを許可する)、**Continue** をクリックした後、ユーザーは URL をブロックするポリシーを上書きするためにパスワードを入力する必要があります。



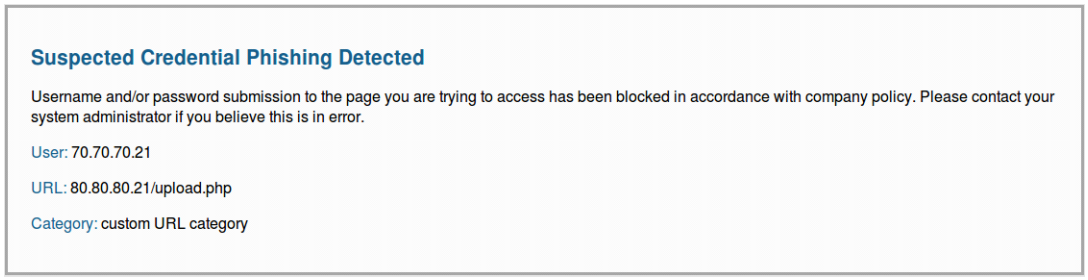
- **URL** フィルタリング セーフ サーチのブロック ページ

  Safe Search Enforcement（セーフ サーチを適用）オプションが有効になっている URL フィルタリング プロファイルを使用したセキュリティ ポリシー ルールによって、アクセスがブロックされたことを示します。(全て見るセーフ サーチの適用)Google、Bing、Yahoo、または Yandex を使用して検索が実行され、ブラウザまたは検索エンジン アカウント設定でセーフ サーチが厳密に設定されていない場合、このページが表示されます。



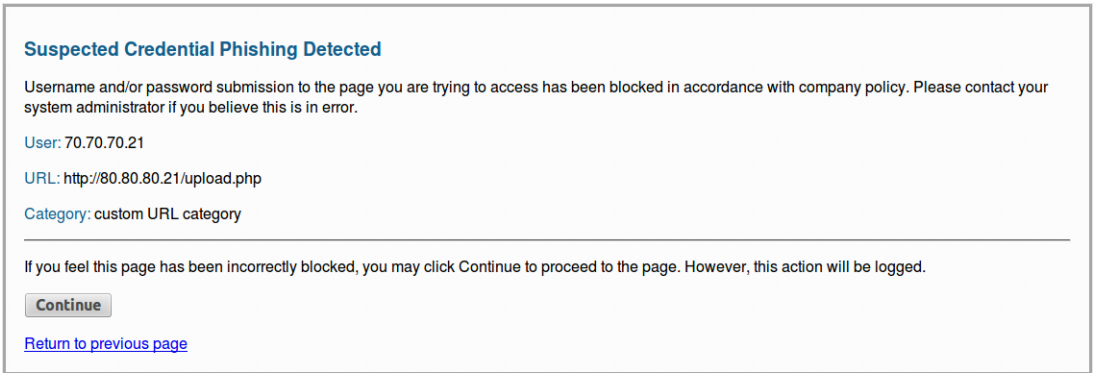
- アンチフィッシング ブロックページ

  このページは、認証情報の送信がブロックされているカテゴリーに属する Web ページで、ユーザーが企業の認証情報（ユーザー名あるいはパスワード）を入力しようとしたときに表示されます。ユーザーは引き続きサイトにアクセスできますが、関連する Web フォームに企業の有効な認証情報を送信することはできません。ユーザーが企業の資格情報を送信できるサイトを制御するには、User-IDを構成し、URLカテゴリに基づいて資格情報のフィッシング防止を有効にする必要があります。



- アンチフィッシング 続行ページ

  このページは、認証情報（ユーザー名とパスワード）を Web サイトに送信することに対してユーザーに警告を表示します。認証情報の送信に対してユーザーに警告を表示することで、企業の認証情報をユーザーが再利用することを阻止できるほか、フィッシングの可能性についてユーザーを教育することができます。サイトで認証を続行するには、ユーザーが Continue (続行) を選択する必要があります。ユーザーが企業の資格情報を送信できるサイトを制御するには、User-IDを構成し、URLカテゴリに基づいて資格情報のフィッシング防止を有効にする必要があります。



URLフィルタリング応答ページのオブジェクト

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注：

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	• レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URLフィルタリング応答ページをカスタマイズするには、次のセクションで説明する変数と参照を使用します。応答ページ変数には、URL要求に関するさまざまな情報が表示されます。例えば、ファイアウォールは応答ページのHTMLコード中の<category/>変数を、リクエストされたURLのURLカテゴリに置き換えます。応答ページ参照を使用すると、外部画像、サウンド、スタイル シート、リンクを追加できます。

応答スページ変数

次の表は、応答ページの変数と、ブロック イベント中にシステムが各変数に置き換える情報またはオブジェクトを示しています。各URLフィルタリング応答ページでは、デフォルトで次の変数が使用されます：user、url、および category。ただし、応答ページはカスタマイズ可能です。たとえば、変数の順序を変更したり、特定のURLカテゴリに異なるメッセージを追加したりできます。

変数	使用率
<user/>	ファイアウォールは、応答ページを表示するときにこの変数をユーザー名（ユーザー ID を介して使用可能な場合）またはユーザーの IP アドレスに置き換えます。
<url/>	ファイアウォールは、応答ページを表示するときにこの変数を、要求された URL に置き換えます。
<category/>	ファイアウォールは、この変数を、ブロックされた要求の URL フィルタリング カテゴリに置き換えます。
<pan_form/>	URL Filtering Continue and Override page [URL フィルタリングの続行とオーバーライド ページ]に **Continue** [続行]ボタンを表示する HTML コード。

ユーザーがアクセスしようとしている URL カテゴリに基づいて異なるメッセージを表示するようにファイアウォールをトリガーするコードを追加することもできます。たとえば、応答ページから以下のコード スニペットを使用して、URL カテゴリが games の場合は Message 1、カテゴリが travel の場合は Message 2、カテゴリが kids の場合は Message 3 を表示するように指定します。

```
var cat = "<category/>"; switch(cat) { case 'games':
 document.getElementById("warningText").innerHTML = "Message 1";
```

```
break; case 'travel':
document.getElementById("warningText").innerHTML = "Message 2";
break; case 'kids': document.getElementById("warningText").innerHTML
= "Message 3"; break; }
```

応答ページのリファレンス

各仮想システムにロードできるのは、ブロック ページのタイプごとに *1* つの *HTML* ページのみです。ただし、イメージ、サウンド、カスケード スタイル シート（*CSS* ファイル）などの他のリソースは、ブラウザに応答ページが表示されるときに他のサーバーからロードできます。すべてのリファレンスに完全修飾 *URL* が含まれている必要があります。

リファレンス タイプ	HTML コードの例
イメージ	`<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">`
サウンド	`<embed src="http://simplythebest.net/sounds/WAV/WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">`
スタイル シート	`<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />`
ハイパーリンク	`<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">企業ポリシーを表示</a>`

URLフィルタリング応答ページのカスタマイズ

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

どこで使用できますか?	何が必要ですか?
	• Prisma AccessライセンスにはAdvanced URL Filtering機能が含まれます。

デフォルトでは、URLフィルタリング応答ページは、要求されたURLにアクセスできない理由を説明し、ユーザーのIPアドレス、要求されたURL、URLカテゴリを表示します。企業のニーズに合わせて応答ページをカスタマイズできます。たとえば、ユーザに表示するメッセージを変更したり、企業ブランディングを追加したり、許容される使用ポリシーにリンクしたりできます。

ページをカスタマイズするには、プラットフォームからエクスポートし、テキストエディタで変更します。提供された応答ページ変数と参照を使用して更新を行うことができます。レスポンスページの変数は、ブロックされた特定のユーザー、URL、およびカテゴリに対応します。レスポンスページ参照は、画像、サウンド、スタイルシート、リンクの使用を可能にします。

Panorama™のWebインターフェイスは、応答ページのエクスポートをサポートしていません。

サポートされている最大サイズを超えるカスタム応答ページは復号化されないか、ユーザーに対して表示されません。*PAN-OS 8.1.2* および古い *PAN-OS 8.1* リリースでは、復号化されているサイトのカスタム応答ページは *8,191* バイトを超えられません。*PAN-OS 8.1.3* 以降のリリースでこの最大サイズが *17,999* バイトです。

- Strata Cloud Manager
- PAN-OS & Panorama

URLフィルタリング応答ページのカスタマイズ (Strata Cloud Manager)

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。

*Strata Cloud Manager*をお使いの場合は、こちらに進んでください。

STEP 1 | カスタマイズしたいデフォルトの回答ページをエクスポートします。

1. **[Manage (管理)] > [Configuration (設定)] > NGFW and Prisma Access > [Security Services (セキュリティサービス)] > [URL Access Management (URLアクセス管理)] > [Settings (設定)]**を順に選択します。
2. 回答ページペインで、編集する各回答ページの**[HTML**テンプレートのエクスポート**]**をクリックします。
3. ファイルをシステムに保存します。

STEP 2 | エクスポートした回答ページを編集します。

1. 任意の HTML テキスト エディタを使用して、ページを編集します。
   - ブロックされた特定のユーザー、URL、またはカテゴリに関するカスタム情報を表示するには、1つ以上の応答ページ変数を追加します。

- カスタム画像、音声、スタイルシート、またはリンクを含めるには、応答ページの参照を1つ以上含めてください。

2. 編集したページを新しいファイル名で保存します。

   ページが *UTF-8* エンコーディングのままであることを確認してください。たとえば、メモ帳の*[名前を付けて保存]*ダイアログで、*[*文字コード*]*ドロップダウンから***[UTF-8]***を選択すします。

STEP 3 | カスタマイズした応答ページをインポートします。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **NGFW and Prisma Access** > **[Security Services (セキュリティサービス)]** > **[URL Access Management (URL**アクセス管理**)]** > **[Settings (設定)]**を順に選択します。
2. 回答ページペインで、カスタマイズした回答ページの種類をクリックします。ファイル選択ダイアログが表示されます。

   たとえば、URLアクセス管理ブロックページをカスタマイズした場合は、**URL**アクセス管理ブロックページをクリックします。
3. **[Choose File (ファイルを選択)]**をクリックし、カスタマイズしたファイルを選択します。
4. **Save**（保存）をクリックします。

STEP 4 | **[Push Config (設定をプッシュ)]**をクリックします。

STEP 5 | カスタマイズされた応答ページが表示されることを確認します。

Webブラウザから、応答ページをトリガーするURLにアクセスします。たとえば、カスタマイズされたURLアクセス管理ブロックページを確認するには、セキュリティポリシールールでブロックされているURLにアクセスします。

ファイアウォールは、次のポートを使用してURLアクセス管理応答ページを表示します。

- **HTTP**—6080
- **Default TLS with firewall certificate (**ファイアウォール証明書を含む デフォルト**TLS)** —6081
- **Custom SSL/TLS profile (**カスタム **SSL/TLS** プロファイル**)** —6082

URLフィルタリング応答ページのカスタマイズ (PAN-OS & Panorama)

STEP 1 | カスタマイズする定義済みの応答ページをエクスポートします。

> *Panorama*の*Web*インターフェイスは、応答ページのエクスポートをサポートしていません。特定のファイアウォールの*Web*インターフェイスから直接応答ページをエクスポートしたり、*Panorama*の*Web*インターフェイスのコンテキストドロップダウンを使用して、管理対象ファイアウォールの*Web*インターフェイスにすばやく切り替えることができます。

1. **Device(デバイス) > Response Pages(応答ページ)** の順に選択します。
2. 編集する応答ページのタイプを選択します。特定の応答ページのダイアログが表示されます。
3. **[Predefined (定義済み)]**を選択し、**[Export (エクスポート)]**を選択します。
4. ダイアログを閉じます。
   （任意）応答ページを追加する場合は、手順2から4を繰り返します。
5. ファイルをシステムに保存します。

STEP 2 | エクスポートしたHTMLレスポンスページをカスタマイズする。

1. ファイルを任意のテキストエディタで開きます。
   - 特定のユーザ、要求された URL、またはブロックされた URL カテゴリに関するカスタム情報を表示するには、応答ページ変数を使用します。
   - カスタム画像、サウンド、スタイルシート、またはリンクを統合するには、応答ページ参照を使用します。
2. 編集したファイルに名前を付けて保存します。

   > ページが *UTF-8* エンコーディングのままであることを確認してください。たとえば、メモ帳の *[*名前を付けて保存*]* ダイアログで、*[*文字コード*]* ドロップダウンから ***[UTF-8]*** を選択すします。

STEP 3 | カスタマイズした応答ページをインポートします。

1. **Device(デバイス) > Response Pages(応答ページ)** の順に選択します。
2. 編集した応答ページのタイプを選択します。特定の応答ページのダイアログが表示されます。
3. **[Predefined (定義済み)]**を選択し、**[Import (インポート)]**を選択します。［ファイルのインポート］ダイアログが表示されます。
   [ファイルのインポート]で、編集した応答ページを参照します。
4. （任意）［宛先］で、応答ページを使用する仮想システムを選択します。すべての仮想システムで使用できるようにする場合は、［共有］を選択します。
5. 「了解」をクリックし、ダイアログを閉じます。

STEP 4 | 変更を **Commit (コミット)** します。

STEP 5 | カスタマイズした応答ページをテストします。

Webブラウザから、特定の応答ページをトリガーするURLにアクセスします。たとえば、URLフィルタリングとカテゴリマッチの応答ページを確認するには、セキュリティポリシールールでブロックされているURLにアクセスします。変更内容が表示されることを確認します。

ファイアウォールは、以下のポートを使用して URLフィルタリング応答ページを表示します:

- **HTTP**—6080
- **Default TLS with firewall certificate (**ファイアウォール証明書を含む デフォルト**TLS)** —6081
- **Custom SSL/TLS profile (**カスタム **SSL/TLS** プロファイル**)** —6082

セーフ サーチの適用

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。 • 透過セーフサーチを使用するには、4.1以上のバージョンを実行するPrisma Accessライセンスが必要です。

多くの検索エンジンでは、検索結果からアダルトコンテンツを除外できる安全な検索設定を提供しています。フィルタ設定には、通常、`[Moderate (モデレート)]`、`[Strict (厳格)]`、`[Off (オフ)]`があります。アダルト画像や動画のみを除外する「中」設定や、明示的なテキストを追加で除外する「厳正」設定を使用できます。教育機関、職場、子供、大人、すべての人がこの安全な検索機能の恩恵を受けています。ただし、ネットワーク内のユーザにセーフサーチの設定を許可しても、必ずしも必要な保護が提供されるとは限りません。

成人向けコンテンツからネットワークを保護するには、現在の個々の設定に関係なく、すべてのエンドユーザーに対して最も厳格な安全な検索設定を適用できます。最も厳格な安全な検索設定により、最も安全なブラウジング体験を提供します。まず、URLフィルタリングプロファイルで**[Safe Search Enforcement (セーフサーチを適用)]**オプションを選択します。次に、信頼ゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティポリシールールにプロファイルを適用します。

検索エンジンプロバイダーも*Palo Alto Networks*も、完全なフィルタリング精度を保証することはできません。検索エンジンは*Web*サイトを安全か安全でないかに分類します。その結果、安全と分類された*Web*サイトには、明示的なコンテンツが含まれている可能性があります。*Palo Alto Networks*は、検索エンジンのフィルタリングメカニズムのみに基づいてフィルタリングを実施します。

ファイアウォールは、ユーザーがBing、Yahoo、Yandex、YouTubeで検索し、これらのエンジンの安全な検索設定を最も厳しいレベルに設定していない場合、次のオプションを強制できます。

- [Block Search Results When Strict Safe Search Is Off (厳密なセーフ検索がオフの場合に検索結果をブロックする)](デフォルト)–ファイアウォールは、セーフ検索設定を使用可能な最も厳格なオプションに設定するまで、エンドユーザーに検索結果を表示しないようにします。このシナリオでは、ブラウザにURLフィルタリングセーフサーチブロックページが表示されま

す。この回答ページでは、エンドユーザーに検索結果がブロックされた理由を知らせ、検索に使用した検索エンジンの検索設定へのリンクを表示します。

> *Palo Alto Networks*は、*Google*セーフサーチの実装の変更により、*Google*セーフサーチが有効かどうかを検出できなくなりました。その結果、*Google*検索ではブロック方式が機能しなくなります。代わりに、検索プロバイダのセーフ サーチ設定で説明されている方法を使用して*Google*セーフサーチを設定できます。

- ［Force Strict Safe Search (厳密なセーフサーチを強制する)］（YahooおよびBing 検索エンジンのみサポート）：ファイアウォールは、最も厳格なセーフ検索設定を自動的かつ透過的に実行します。具体的には、ファイアウォールは検索クエリを厳密にフィルタリングされた検索結果を返すURLにリダイレクトし、使用する検索エンジンの安全な検索プリファレンスを変更します。この機能を有効にするには、URLフィルタリングのセーフサーチブロックページのテキストを、手順で指定したテキストに置き換えます。置換テキストには、検索に使用される検索エンジンの厳密な安全検索パラメータを使用して検索クエリURLを書き換えるJavaScriptコードが含まれています。

  > この方法を使用すると、ブラウザに*URL*フィルタリングのセーフサーチブロックページが表示されません。

- Transparent SafeSearch (透過的セーフサーチ)（Prisma Accessデプロイのみ）：トラフィックを復号化できず（たとえば、ゲストのインターネットアクセスを提供するストアで）、ディスプレイデバイスを含む管理対象外のデバイスを持つユーザが制限付き、不適切、または不快なコンテンツを検索できないようにする場合は、Prisma Accessで透過的セーフサーチを使用できます。透過的セーフサーチは、FQDN-IP マッピングを実行することで、モバイルユーザの検索エンジンクエリをエンジンのSafeSearchポータルに解決します。

サポートされている各検索エンジンの安全な検索設定を確認して、安全な検索の実施を開始してください。次に、コンテキストに最適な適用方法を決定します。

- 検索プロバイダのセーフ サーチ設定
- 厳密なセーフ サーチがオフの場合の検索結果のブロック
- 厳密なセーフサーチを強制する
- Prisma Accessで透過的なセーフサーチを使う

検索プロバイダのセーフ サーチ設定

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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

どこで使用できますか?	何が必要ですか?
	• Prima Accessライセンスには*Advanced URL Filtering*機能が含まれます。

検索プロバイダ毎にセーフ サーチ設定が異なるため、次の設定を確認して理解を深めてください。

検索プロバイダ	セーフ サーチ設定の説明
Google/YouTube	個々のコンピュータまたはネットワーク全体（Google のセーフ サーチ仮想 IP アドレスを使用）でセーフ サーチを提供します。 個々のコンピュータでの **Google** 検索のセーフ サーチの適用 Google の検索の設定 の **Filter explicit results**（不適切な検索結果を除外する） 設定で、セーフ サーチ機能を有効にします。有効にした設定はブラウザの Cookie に FF= として保存され、ユーザーが Google の検索を実行するたびにサーバーに渡されます。 **`safe=active`** を Google の検索クエリ URL に追加して、最も厳密なセーフ サーチ設定を有効にすることもできます。 仮想 **IP** アドレスを使用した **Google** および **YouTube** 検索のセーフ サーチの適用 Googleは、次のようなサーバーを提供しています。Lock SafeSearch (ロックセーフサーチ)(forcesafesearch.google.com)すべてのGoogleおよびYouTube検索の設定。**`forcesafesearch.google.com`** を指し示す CNAME レコードを含む、**`www.google.com`** と **`www.youtube.com`**（および Google や YouTube に関連するその他の国別サブドメイン）の DNS エントリを DNS サーバー設定に追加すると、ネットワーク上のすべてのユーザーが Google または YouTube 検索を実行するときに必ず厳密なセーフ サーチ設定を使用するようになります。ただし、このソリューションには、ファイアウォールの Safe Search Enforcement（セーフ サーチを適用）との互換性はありません。したがって、このオプションを使用して Google で安全な検索を強制する場合、カスタム URL カテゴリを作成して URL フィルタリング プロファイルのブロック リストに追加することで、ファイアウォール上の

検索プロバイダ	セーフ サーチ設定の説明
	他の検索エンジンへのアクセスをブロックすることをお勧めします。 • *PAN-OS* は、*HTTP*ヘッダー挿入による *YouTube* のセーフサーチ適用をサポートします。*HTTP* ヘッダー挿入は現在 *HTTP/2* をサポートしていません。*YouTube*の安全な検索を強制するには、App-IDとHTTP/2インスペクション、*HTTP/2*接続を*HTTP/1.1*にダウングレードするには、ストリップ***ALPN***機能を使用します。 • *Google* のセーフ サーチ ロック ソリューションの使用を計画している場合、*DNS* プロキシ（***Network (***ネットワーク***) > DNS Proxy (DNS*** プロキシ***)***）を設定し、*DHCP* を介してサービス プロバイダからファイアウォールに *DNS* 設定を送信するときに使用するレイヤー *3* インターフェイスとして継承ソースを設定することを検討してください。*forcesafesearch.google.com* サーバーのローカル *IP* アドレスを使用して、*www.google.com* と *www.youtube.com* の *[*スタティック エントリ*]* で *DNS* プロキシを設定します。
Yahoo	個々のコンピュータでのみセーフ サーチを提供します。Yahoo の 検索設定 には3つのセーフサーチ設定があります。**Strict** [強]、**Moderate** [中]、**Off** [オフ]。有効にした設定はブラウザの Cookie に `vm=` として保存され、ユーザーが Yahoo の検索を実行するたびにサーバーに渡されます。

検索プロバイダ	セーフ サーチ設定の説明
	vm=r を Yahoo の検索クエリ URL に追加して、最も厳密なセーフ サーチ設定を有効にすることもできます。 *Yahoo* アカウントでログイン中に *Yahoo Japan*（***yahoo.co.jp***）で検索を実行する場合、エンド ユーザーは *[*チャイルド ロック*]* オプションも有効にする必要があります。
Bing	個々のコンピューターで安全な検索を提供します。Bing の 検索設定 には3つのセーフサーチ設定があります。**Strict** [強]、**Moderate** [中]、**Off** [オフ]。有効にした設定はブラウザの Cookie に adtl= として保存され、ユーザーが Bing の検索を実行するたびにサーバーに渡されます。 **adlt=strict** を Bing の検索クエリ URL に追加して、最も厳密なセーフ サーチ設定を有効にすることもできます。 Bing SSL 検索エンジンでは、セーフ サーチ URL パラメータが適用されないため、完全なセーフ サーチを適用するために SSL 経由の Bing をブロックすることを検討してください。

厳密なセーフ サーチがオフの場合の検索結果のブロック

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

セーフサーチの実施を有効にすると、ファイアウォールのデフォルトの動作では、Bing、Yahoo、Yandex、または Youtube の検索エンジンで検索しているエンドユーザーが

セーフサーチの設定を利用可能な最も厳格なオプションに設定するまで、検索結果をブロックします。デフォルトでは、URLフィルタリングのセーフサーチブロックページがブラウザに表示されます。定義済みブロックページには、使用する検索エンジンの検索設定へのリンクが表示されます。これにより、ユーザーは安全な検索設定を調整できます。セーフサーチブロックページをカスタマイズして、組織の特定のニーズを満たすことができます。

この既定の方法を使用してセーフ サーチを適用する場合は、ポリシーを実装する前にエンドユーザーに通知する必要があります。エンドユーザーの検索クエリURLを完全安全な検索バージョンに自動的にリダイレクトしたい場合は、[strict safe search transparently (透過性の高い厳密な安全検索)]に有効にしてください。

*Palo Alto Networks*は、*Google*の実装の変更により、*Google*セーフサーチがオンになっているかどうかを検出できなくなりました。結果として、ファイアウォールはこの方法で安全な検索を強制できません。セーフサーチを透過的に強制する場合もあります。ただし、*Google*が明示的な画像やコンテンツをフィルタリングして排除することを保証することはできません。

- Strata Cloud Manager
- PAN-OS & Panorama

厳密なセーフ サーチが無効である場合の検索結果のブロック(Strata Cloud Manager)

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。

Strata Cloud Managerをお使いの場合は、こちらに進んでください。

STEP 1 | URLアクセス管理プロファイルで安全な検索の実施を有効にする。

1. **[Manage (管理)] > [Configuration (設定)] > [Security Services (セキュリティサービス)] > [URL Access Management (URL**アクセス管理**)]**を順に選択します。
2. [URLアクセス管理プロファイル]で、既存のプロファイルを選択するか、**[Add Profile (**プロファイルの追加**)]**を選択して新しいプロファイルを作成します。設定オプションが表示されます。
3. **[Settings (**設定**)]**で**[Safe Search Enforcement (**安全な検索の実施**)]**を選択します。
4. プロファイルを保存します。

STEP 2 | （任意）エンドユーザがアクセスできる検索エンジンを制限します。

1. **[Manage (管理)] > [Configuration (設定)] > [Security Services (セキュリティサービス)] > [URL Access Management (URL**アクセス管理**)]**を順に選択します。
2. **[Access Control (**アクセス制御**)]**で、検索エンジンカテゴリを検索( )します。
3. 検索エンジンカテゴリのサイトアクセスをブロックするように設定します。

   後のステップで、許可したい検索エンジンを含むカスタムURLカテゴリ (URLリストタイプ) を作成します。
4. プロファイルを保存します。

STEP 3 | URLアクセス管理プロファイルを、トラストゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティポリシールールに適用します。

URLアクセス管理プロファイル（および任意のセキュリティプロファイル）をアクティブにするには、プロファイルグループに追加し、セキュリティポリシー規則でプロファイルグループを参照します。

STEP 4 | サポートされている検索エンジン用のカスタムURLカテゴリを作成します。

次のステップでは、このカスタムカテゴリへのトラフィックを復号化するようにファイアウォールを設定します。

1. **[Manage (管理)] > [Configuration (設定)] > [Security Services (セキュリティサービス)] > [URL Access Management (URL**アクセス管理**)]**を順に選択します。
2. [**Access Control (**アクセス制御**)]**の[カスタムURLカテゴリ]で、[**Add Category (**カテゴリを追加**)]**を選択します。
3. カテゴリの**Name [**名前**]**（**`SearchEngineDecryption`**など）を入力します。
4. カスタムURLカテゴリの種類で**[URL List (URL**リスト**)]**を選択します。
5. 項目で、URLリストに次のエントリを追加します。
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. カスタムカテゴリを保存します。
7. 新しいカスタムURLカテゴリのサイトアクセスを設定します。
   1. [URLアクセス管理プロファイル]で、先に設定したプロファイルを選択します。
   2. [アクセス制御]で、新しいカスタムURLカテゴリを選択します。「外部動的URLリスト」と「事前定義されたカテゴリ」の上にある「カスタムURLカテゴリ」セクションに表示されます。
   3. **[Site Access (**サイトアクセス**)]**を**[allow (**許可**)]**に設定します。
   4. 変更を保存します。

STEP 5 | SSLフォワードプロキシ復号化を設定します。

ほとんどの検索エンジンは検索結果を暗号化するため、ファイアウォールが検索トラフィックを検査し、安全な検索設定を検出できるように、[SSL Forward Proxyの復号化]を有効にする必要があります。

復号ポリシールールの**[Services and URLs (**サービスと**URL)]**セクションで**[Add URL Categories (URL**カテゴリを追加**)]**をクリックします。次に、先ほど作成したカスタムURLカテゴリを選択します。新しいカスタムカテゴリは、リストの一番上に配置されます。

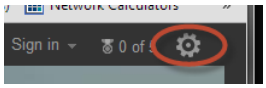
復号化ポリシー ルールの保存

STEP 6 | **[Push Config (**プッシュ設定**)]**を選択して変更を有効にします。

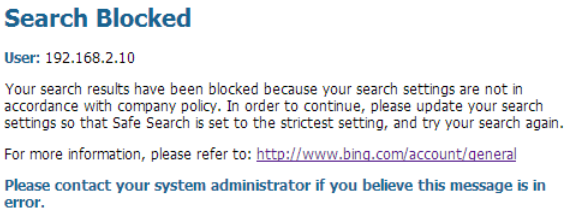
STEP 7 | Safe Search Enforcement （セーフ サーチを適用）設定を確認します。

この確認手順は、ブロック ページを使用してセーフ サーチを適用している場合にのみ機能します。セーフサーチを透過的に有効にすると、別の検証ステップがあります。

1. ファイアウォールの背後にあるコンピュータから、サポートされている検索プロバイダの厳密な検索設定を無効にします。たとえば、bing.com で、Bing メニュー バーの設定アイコンをクリックします。



2. **[SafeSearch (セーフサーチ)]**オプションを**[Moderate (標準)]**または**[Off (オフ)]**に設定し、**[Save (保存)]**をクリックします。
3. Bing 検索 (または別のプロバイダーを使用して検索) を実行して、検索結果の代わりにURLアクセス管理セーフサーチブロックページが表示されるかどうかを確認します。



4. ブロックページのリンクを使用してセーフサーチの設定を最も厳しい設定(Bingの場合は**Strict (厳格)**)に更新し、**[Save (保存)]**をクリックします。
5. Bing から再度検索を実行し、ブロック ページではなく、フィルタリングされた検索結果が表示されることを確認します。

厳密なセーフ サーチがオフの場合の検索結果のブロック (PAN-OS & Panorama)

STEP 1 | URL フィルタリング プロファイルでセーフ サーチの適用を有効にします。

1. **Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > URL Filtering (URL フィルタリング)** の順に選択します。
2. 既存のプロファイルを選択して変更するか、デフォルト プロファイルをコピーして新しいプロファイルを作成します。
3. **[URL Filtering Settings (URL フィルタリング設定)]**タブで、**[Safe Search Enforcement (セーフサーチ強制)]**を選択します。

STEP 2 | (任意) エンドユーザーがアクセスできる検索エンジンを同じURLフィルタリングプロファイルで制限します。

1. [カテゴリ]タブで、検索エンジンのカテゴリを( )検索します。
2. 検索エンジンカテゴリのサイトアクセスをブロックするように設定します。

   後のステップで、許可したい検索エンジンを含むカスタムURLカテゴリ (URLリストタイプ) を作成します。
3. **OK** をクリックしてプロファイルを保存します。

STEP 3 | URLフィルタリングプロファイルを、トラストゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティポリシールールに適用します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。次に、URLフィルタリングプロファイルを適用するルールをクリックします。
2. [アクション]タブで、[プロファイル設定]を探します。[プロファイルタイプ] で [プロファイル] を選択します。プロファイルのリストが表示されます。
3. [**URL**フィルタリングプロファイル] で、前に作成したプロファイルを選択します。
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 4 | サポートされている検索エンジン用のカスタムURLカテゴリを作成します。

次のステップでは、カスタムカテゴリのサイトへのトラフィックを復号化することを指定します。

1. **Objects (**オブジェクト**) > Custom Objects (**カスタム オブジェクト**) > URL Category (URL** カテゴリ**)** を選択してカスタム カテゴリを **Add (**追加**)** します。
2. カテゴリの **Name** [名前]（**`SearchEngineDecryption`**など）を入力します。
3. 以下を**[Sites (**サイト**)]**リストに**[Add (**追加**)]**します。
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com`**。**`*`**
4. 「**OK**」をクリックしてカスタムカテゴリを保存します。
5. 新しいカスタムURLカテゴリのサイトアクセスを設定します。
   1. **[Objects (**オブジェクト**)] > [Security Profiles (**セキュリティプロファイル**)] > URL Filtering ([URL**フィルタリング**)]**に移動し、前に構成したURLフィルタリングプロファイルを選択します。
   2. **[Category (**カテゴリ**)]**タブで、新しいカスタムURLカテゴリを選択します。外部動的URLリストと定義済みカテゴリの上の[カスタムURLカテゴリ]セクションに表示されます。
   3. [**Site Access (**サイトアクセス**)]**を**[allow (**許可**)]**に設定します。
   4. **OK** をクリックして変更内容を保存します。

STEP 5 | SSLフォワードプロキシ復号化を設定します。

ほとんどの検索エンジンは検索結果を暗号化するため、ファイアウォールが検索トラフィックを検査し、安全な検索設定を検出できるように、[SSL Forward Proxyの復号化]を有効にする必要があります。

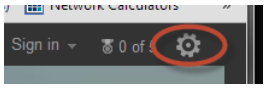
復号化ポリシールールの[サービス**/URL** カテゴリ]タブで、前に作成したカスタムURLカテゴリを追加します。**[OK]**をクリックします。

STEP 6 | 変更を **Commit (**コミット**)** します。

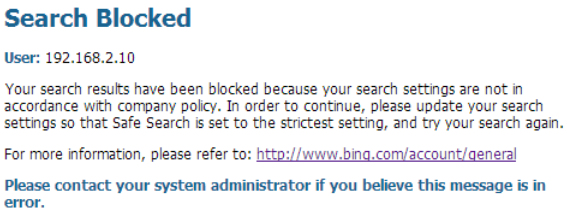
STEP 7 | Safe Search Enforcement （セーフ サーチを適用）設定を確認します。

この確認手順は、ブロック ページを使用してセーフ サーチを適用している場合にのみ機能します。セーフサーチを透過的に有効にする場合は、別の検証手順があります。

1. ファイアウォールの内側にあるコンピューターから、サポートされている検索プロバイダーの厳密な検索設定を無効にします。たとえば、bing.com で、Bing メニュー バーの設定アイコンをクリックします。



2. **[SafeSearch (セーフサーチ)]**オプションを**[Moderate (標準)]**または**[Off (オフ)]**に設定し、**[Save (保存)]**をクリックします。
3. Bing 検索 (または別のプロバイダーを使用して検索) を実行して、検索結果の代わりにURLフィルタリングセーフサーチブロックページが表示されるかどうかを確認します。



4. ブロックページのリンクを使用してセーフサーチの設定を最も厳しい設定(Bingの場合は**Strict (厳格)**)に更新し、**[Save (保存)]**をクリックします。
5. Bing から再度検索を実行し、ブロック ページではなく、フィルタリングされた検索結果が表示されることを確認します。

厳密なセーフサーチを強制する

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

厳密なセーフサーチを透過的に有効にすることで、BingおよびYahooのエンドユーザーに安全でシームレスな検索エクスペリエンスを提供できます。エンドユーザーが厳密なセーフサーチを有効にせずに検索した場合に 検索結果をブロックする 代わりに、ファイアウォールは自動的に厳密なセーフサーチを有効にし、厳密にフィルタリングされた検索結果のみを返します。たとえば、学校や図書館は、一貫した学習体験を保証する自動施行の恩恵を受けることができます。

透過的なセーフ サーチの適用を有効にするには、URLフィルタリング プロファイルでセーフ サーチの適用を有効にし、URLフィルタリングのセーフ サーチ ブロック ページ ファイル内のテキストを次の手順で提供されるテキストに置き換える必要があります。置換テキストには、検索に使用される検索エンジンの厳密なセーフサーチパラメータを含む検索クエリURLを追加するJavaScriptが含まれます。

*URL*フィルタリングのセーフサーチ ブロック ページがブラウザに表示されません。

これらの手順を完了すると、エンドユーザーが検索するたびにファイアウォールがJavaScriptを実行します。たとえば、不適切な結果をもたらす可能性のある概念を学生が調査するときに、Bingセーフサーチ設定がオフに設定されているとします。ファイアウォールはセーフサーチの設定を検出すると、検索クエリURLに`&adlt=strict`を追加します。その後、検索エンジンは適切な結果を表示し、セーフサーチの設定が `[Strict (厳格)]`に変更されます。

- Strata Cloud Manager
- PAN-OS & Panorama

厳密なセーフサーチを強制する (Strata Cloud Manager)

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

[PAN-OS & Panorama] タブに切り替えて、そこにあるガイダンスに従います。

***Strata Cloud Manager*をお使いの場合は、こちらに進んでください。**

STEP 1 | URLアクセス管理プロファイルで安全な検索の実施を有効にする。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[Security Services (セキュリティサービス)]** > **[URL Access Management (URLアクセス管理)]**を順に選択します。
2. [URLアクセス管理プロファイル]で、既存のプロファイルを選択するか、**[Add Profile (プロファイルの追加)]**を選択して新しいプロファイルを作成します。設定オプションが表示されます。
3. **[Settings (設定)]**で**[Safe Search Enforcement (安全な検索の実施)]**を選択します。
4. プロファイルを保存します。

STEP 2 | （任意）エンドユーザがアクセスできる検索エンジンを制限します。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[Security Services (セキュリティサービス)]** > **[URL Access Management (URLアクセス管理)]**を順に選択します。
2. **[Access Control (アクセス制御)]**で、検索エンジンカテゴリを検索( )します。
3. 検索エンジンカテゴリのサイトアクセスをブロックするように設定します。

後のステップで、許可したい検索エンジンを含むカスタムURLカテゴリ (URLリストタイプ) を作成します。

4. プロファイルを保存します。

STEP 3 | URLアクセス管理プロファイルを、トラストゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティポリシールールに適用します。

URLアクセス管理プロファイル（および任意のセキュリティプロファイル）をアクティブにするには、プロファイルグループに追加し、セキュリティポリシー規則でプロファイルグループを参照します。

STEP 4 | URLアクセス管理のセーフ サーチ ブロック ページを編集し、既存のコードをJavaScriptに置き換えて検索クエリURLを書き換えます。

1. **[Manage (管理)] > [Configuration (設定)] > [Security Services (セキュリティサービス)] > [URL Access Management (URLアクセス管理)] > [Response Pages (応答ページ)]**を順に選択します。
2. URL アクセス管理ブロック ページの**HTML** テンプレートをエクスポートします 。
3. HTMLエディターを使用して、既存のブロックページのテキストをすべて次のテキストに置き換えます。次に、ファイルを保存します。

```
<html> <head> <title>検索ブロック</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
 color:#196390; } b { font-weight:normal; color:#196390; }</
style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>検索がブロックされた</h1> <p> <b>ユーザー:</b><user/> </
p> <p>検索設定が会社のポリシーに従っていないため、検索結果がブロック
されました。続行するには、Safe Searchが最も厳しい設定に設定されるよ
うに検索設定を更新してください。現在アカウントにログインしている場合
は、Safe Searchもロックして検索を再試行してください。</p><p> 詳細
については、<a href="<ssurl/>"を参照してください> <ssurl/> </
a> </p> <p id="java_off">お使いのブラウザでJavaScriptを有効に
してください。<br></p><p><b>このメッセージに誤りがあると思われる
場合は、システム管理者に問い合わせてください。</b></p> </div> </
body> <script> // ブラウザにある URL を取得します。var s_u =
 location.href;bing // 先頭のスラッシュ、何でも、次に ".bing." 、次
に何かに一致し、その後に非貪欲なスラッシュが続きます。うまくいけば、最初の
スラッシュ。var b_a = /^.*//(.+.bing..+?)//.exec(s_u);if (b_a)
 { s_u = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML = 'あなた
はより安全な検索にリダイレクトされています!'; } //yahoo // 冒頭
のスラッシュと一致し、次に ".yahoo." 、その後に非貪欲なスラッシュ
が続きます。うまくいけば、最初のスラッシュ。var y_a = /^.*//(.
+.yahoo..+?)//.exec(s_u);if (y_a) { s_u = s_u.replace(/&vm=p/
ig,""); s_u = s_u + "&vm=r"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML
```



```
= 'You are redirected to a safer search!'; }
document.getElementById("java_off").innerHTML = ' ';</script>
</html>
```

STEP 5 | 編集したURLアクセス管理セーフ サーチ ブロック ページをファイアウォールにインポートします。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[Security Services (セキュリティサービス)]** > **[URL Access Management (URLアクセス管理)]** > **[Response Pages (応答ページ)]**を順に選択します。
2. URLアクセス管理セーフ サーチ ブロック ページをクリックします**[Choose File (ファイルの選択)]**オプションを含むダイアログが表示されます。
3. 先ほど編集したセーフサーチブロックページファイルを選択し、[保存]をクリックします。

STEP 6 | サポートされている検索エンジン用のカスタムURLカテゴリを作成します。

次のステップでは、このカスタムカテゴリへのトラフィックを復号化するようにファイアウォールを設定します。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[Security Services (セキュリティサービス)]** > **[URL Access Management (URLアクセス管理)]**を順に選択します。
2. **[Access Control (アクセス制御)]**の[カスタムURLカテゴリ]で、**[Add Category (カテゴリを追加)]**を選択します。
3. カテゴリの**Name** [名前]（**`SearchEngineDecryption`**など）を入力します。
4. カスタムURLカテゴリの種類で**[URL List (URLリスト)]**を選択します。
5. 項目で、URLリストに次のエントリを追加します。
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. カスタムカテゴリを保存します。
7. 新しいカスタムURLカテゴリのサイトアクセスを設定します。
   1. [URLアクセス管理プロファイル]で、先に設定したプロファイルを選択します。
   2. [アクセス制御]で、新しいカスタムURLカテゴリを選択します。「外部動的URLリスト」と「事前定義されたカテゴリ」の上にある「カスタムURLカテゴリ」セクションに表示されます。
   3. **[Site Access (サイトアクセス)]**を**[allow (許可)]**に設定します。
   4. 変更を保存します。

STEP 7 | SSLフォワードプロキシ復号化を設定します。

ほとんどの検索エンジンは検索結果を暗号化するため、ファイアウォールが検索トラフィックを検査し、安全な検索設定を検出できるように、[SSL Forward Proxyの復号化]を有効にする必要があります。

復号ポリシールールの**[Services and URLs (**サービスと**URL)]**セクションで**[Add URL Categories (URL**カテゴリを追加**)]**をクリックします。次に、先ほど作成したカスタムURLカテゴリを選択します。新しいカスタムカテゴリは、リストの一番上に配置されます。

復号化ポリシー ルールの保存

STEP 8 | **[Push Config (**プッシュ設定**)]**を選択して変更を有効にします。

STEP 9 | Safe Search Enforcement （セーフ サーチを適用）設定を確認します。

ファイアウォールの背後にあるコンピューターからブラウザを開き、Bing、Yahoo、またはYandexを使用して検索を実行します。次に、次のいずれかの方法を使用して構成を確認します。

- URLのクエリ文字列を調べて、安全な検索パラメータを確認してください。検索プロバイダのセーフサーチ設定には、各検索クエリURLに追加されたセーフサーチパラメータが一覧表示されます。
- サポートされている検索エンジンのセーフサーチ設定に移動し、選択したセーフサーチ設定が最も厳しいレベル(ほとんどの場合は**[Strict (**厳格**)]**)であることを確認します。

厳密なセーフサーチを強制する (PAN-OS & Panorama)

STEP 1 | ファイアウォールでコンテンツ リリース バージョン 475 以降が実行されていることを確認します。

1. Select **Device (**デバイス**) > Dynamic Updates (**動的アップデート**)**を選択します:
2. **[**アプリケーションおよび脅威**]** セクションを確認し、現在どの更新が実行されているのかを特定します。
3. ファイアウォールで必要なバージョン（またはそれ以降）の更新が実行されていない場合、**Check Now**（今すぐチェック）をクリックし、使用可能な更新のリストを取得します。
4. 必要な更新を見つけて **[**ダウンロード**]** をクリックします。
5. ダウンロードが完了したら、**Install**（インストール）をクリックします。

STEP 2 | URL フィルタリング プロファイルでセーフ サーチの適用を有効にします。

1. **Objects (**オブジェクト**) > Security Profiles (**セキュリティ プロファイル**) > URL Filtering (URL** フィルタリング**)** の順に選択します。
2. 既存のプロファイルを選択して変更するか、デフォルト プロファイルをコピーして新しいプロファイルを作成します。
3. **[URL Filtering Settings (URL** フィルタリング設定**)]**タブで、**[Safe Search Enforcement (**セーフサーチ強制**)]**を選択します。

STEP 3 | (任意) エンドユーザーがアクセスできる検索エンジンを同じURLフィルタリングプロファイルで制限します。

1. [カテゴリ]タブで、検索エンジンのカテゴリを( )検索します。
2. 検索エンジンカテゴリのサイトアクセスをブロックするように設定します。

   後のステップで、許可したい検索エンジンを含むカスタムURLカテゴリ (URLリストタイプ) を作成します。
3. **OK** をクリックしてプロファイルを保存します。

STEP 4 | URLフィルタリングプロファイルを、トラストゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティポリシールールに適用します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。次に、URLフィルタリングプロファイルを適用するルールをクリックします。
2. [アクション]タブで、[プロファイル設定]を探します。[プロファイルタイプ] で [プロファイル] を選択します。プロファイルのリストが表示されます。
3. [**URL**フィルタリングプロファイル] で、前に作成したプロファイルを選択します。
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 5 | URLフィルタリングのセーフサーチブロックページを編集し、検索クエリURLを書き換えるための既存のコードをJavaScriptに置き換えます。

1. **Device (デバイス) > Response Pages (応答ページ) > URL Filtering Safe Search Block Page (URL フィルタリング セーフ サーチのブロック ページ)** を選択します。
2. [事前定義済み] を選択し、[エクスポート] をクリックして、ファイルをローカルに保存します。
3. HTMLエディターを使用して、既存のブロックページのテキストをすべて次のテキストに置き換えます。次に、ファイルを保存します。

```
<html> <head> <title>検索ブロック</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
 color:#196390; } b { font-weight:normal; color:#196390; }</
style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>検索がブロックされた</h1> <p> <b>ユーザー:</b><user/> </
p> <p>検索設定が会社のポリシーに従っていないため、検索結果がブロックされました。続行するには、Safe Searchが最も厳しい設定に設定されるように検索設定を更新してください。現在アカウントにログインしている場合は、Safe Searchもロックして検索を再試行してください。</p><p> 詳細については、<a href="<ssurl/>"を参照してください> <ssurl/> </
a> </p> <p id="java_off">お使いのブラウザでJavaScriptを有効にしてください。<br></p><p><b>このメッセージに誤りがあると思われる場合は、システム管理者に問い合わせてください。</b></p> </div> </
body> <script> // ブラウザにある URL を取得します。var s_u =
 location.href;bing // 先頭のスラッシュ、何でも、次に ".bing." 、次
```



```
に何かに一致し、その後に非貪欲なスラッシュが続きます。うまくいけば、最初のスラッシュ。var b_a = /^.*//(.+.bing..+?)//.exec(s_u);if (b_a) { s_u = s_u + "&adlt=strict"; window.location.replace(s_u); document.getElementById("java_off").innerHTML = 'あなたはより安全な検索にリダイレクトされています!'; } //yahoo // 冒頭のスラッシュと一致し、次に ".yahoo." 、その後に非貪欲なスラッシュが続きます。うまくいけば、最初のスラッシュ。var y_a = /^.*//(.+.yahoo..+?)//.exec(s_u);if (y_a) { s_u = s_u.replace(/&vm=p/ig,""); s_u = s_u + "&vm=r"; window.location.replace(s_u); document.getElementById("java_off").innerHTML = 'You are redirected to a safer search!'; } document.getElementById("java_off").innerHTML = ' ';</script> </html>
```

STEP 6 | 編集した URL フィルタリング セーフ サーチのブロック ページをファイアウォールにインポートします。

1. **Device (デバイス) > Response Pages (応答ページ) > URL Filtering Safe Search Block Page (URL フィルタリング セーフ サーチのブロック ページ)** を選択します。
2. **[インポート]** をクリックします。次に、ブロックページファイルを参照するか、**[Import File (ファイルのインポート)]**フィールドにパスとファイル名を入力します。
3. (オプション)**[Destination (宛先)]**では、ログインページを使用する仮想システム、またはすべての仮想システムで使用できるように共有する仮想システムを選択します。
4. **OK** をクリックしてファイルをインポートします。

STEP 7 | サポートされている検索エンジン用のカスタムURLカテゴリを作成します。

次のステップでは、このカスタムカテゴリへのトラフィックを復号化するようにファイアウォールを設定します。

1. **Objects (オブジェクト) > Custom Objects (カスタム オブジェクト) > URL Category (URL カテゴリ)** を選択してカスタム カテゴリを **Add (追加)** します。
2. カテゴリの **Name [名前]**（**SearchEngineDecryption**など）を入力します。
3. 以下を**[Sites (サイト)]**リストに**[Add (追加)]**します。
   - **www.bing.***
   - **search.yahoo.***
   - **yandex.com.***
4. ［**OK**］をクリックしてカスタムURLカテゴリを保存します。

STEP 8 | SSLフォワードプロキシ復号化を設定します。

ほとんどの検索エンジンは検索結果を暗号化するため、ファイアウォールが検索トラフィックを検査し、安全な検索設定を検出できるように、[SSL Forward Proxyの復号化]を有効にする必要があります。

復号化ポリシールールの[サービス/**URL** カテゴリ]タブで、前に作成したカスタムURLカテゴリを追加します。**[OK]**をクリックします。

STEP 9 | 変更を **Commit (**コミット**)** します。

STEP 10 | Safe Search Enforcement （セーフ サーチを適用）設定を確認します。

ファイアウォールの内側にあるコンピューターからブラウザーを開き、Bing またはYahooを使用して検索を実行します。次に、次のいずれかの方法を使用して、構成が意図したとおりに機能することを確認します。

- URL のクエリ文字列を調べて、安全な検索パラメータを確認してください。検索プロバイダのセーフサーチ設定には、各検索クエリ URL に追加されたセーフサーチパラメータが一覧表示されます。
- 検索エンジンのセーフサーチ設定に移動し、選択したセーフサーチ設定が最も厳しいレベル(Bingの場合は**Strict (**厳格**)**)であることを確認します。

Prisma Accessで透過的なセーフサーチを使う

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) この機能をPrisma Access環境で使用したい場合は、アカウントチームにお問い合わせください。	❑ バージョン4.1以上を実行しているPrisma Access環境 ❑ Prisma Accessライセンス

Prisma Accessでは、FQDNからIPへのマッピングを実行することで、モバイルユーザーの検索エンジンクエリをエンジンのSafeSearchポータルに解決できます。トラフィックを復号化できず（ゲストのインターネットアクセスを提供する店舗など）、ディスプレイデバイスを含む管理対象外のデバイスを持つユーザーが制限付き、不適切、または不快なコンテンツを検索できないようにする場合は、厳密なセーフサーチを実装する代わりに透過的なセーフサーチを使用します。

- Strata Cloud Manager
- Panorama

Prisma Accessで透過的なセーフサーチを使う (Strata Cloud Manager)

Strata Cloud ManagerのPrisma Accessに対する透過的なセーフサーチのサポートを設定するには、以下の手順を実行する。リモートネットワークまたはGlobalProtectモバイルユーザーのいずれかに透過的なセーフサーチを設定できます。

STEP 1 | セーフサーチを設定したいデプロイメント タイプ (モバイルユーザーまたはリモートネットワーク) を選択します。

- モバイルユーザーの場合—GlobalProtectの導入環境では**[Manage (管理)] > [Service Setup (サービスセットアップ)] > [Mobile Users (モバイルユーザー)]**に移動し**[GlobalProtect Setup] > [Infrastructure Settings]**を選択します。

  Strata Cloud Managerを使用している場合は、**[Workflows (ワークフロー)] > [Prisma Access Setup] > [Mobile Users (モバイルユーザー)]**に移動し、**[GlobalProtect Setup] > [Infrastructure Settings (インフラストラクチャ設定)]**を選択します。
- リモートネットワークデプロイメントの場合は、**[Manage (管理)] > [Service Setup (サービスセットアップ)] > [Remote Networks (リモートネットワーク)]**に移動してください。

  Strata Cloud Manager を使用している場合は、**[Workflows (ワークフロー)] > [Prisma Access Setup] > [Remote Networks (リモートネットワーク)]**に移動してください。

STEP 2 | [詳細設定]を選択します。

STEP 3 | 静的エントリを使用してFQDNを特定のIPアドレスに解決します。

STEP 4 | 静的エントリルールには一意の名前、検索エンジンの**FQDN**、FQDNリクエストの送信先となる検索エンジンのセーフサーチIPアドレスを入力します。

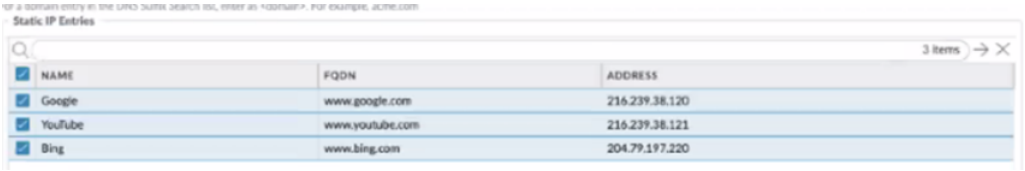
Prisma Accessで透過的なセーフサーチを使う (Panorama)

PanoramaのPrisma Accessに対する透過的なセーフサーチのサポートを設定するには、以下の手順を実行する。リモートネットワークまたはGlobalProtectモバイルユーザーのいずれかに透過的なセーフサーチを設定できます。

STEP 1 | セーフサーチを設定するデプロイメント タイプ(リモートネットワークまたはモバイルユーザ)を選択します。

- モバイルユーザー—GlobalProtectの導入の場合、**[Panorama] > [Cloud Services] > [Configuration (構成)] > [モバイルユーザー—GlobalProtect]**に移動し、**[Onboarding (オンボーディング)]**領域で**[Configure (構成)]**を選択してから、**[Network Services (ネットワークサービス)]**を選択します。
- リモートネットワークの導入の場合、**[Panorama] > [Cloud Services (クラウドサービス)] > [Configuration (構成)] > [Remote Networks (リモートネットワーク)]**に移動し、歯車をクリックして**[Settings (設定)]**を編集し、**[DNSプロキシ]**を選択します。

STEP 2 | 静的エントリルールの一意の名前、検索エンジンの**FQDN**、およびFQDN要求を誘導する検索エンジンのセーフサーチIPアドレスを入力して、**Static IP Entries (**静的**IP**エントリ**)**を入力します。



サードパーティのリモートブラウザ分離プロバイダと統合する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ 高度なURLフィルタリングライセンス 注:Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

最も安全なアクションですが、未知の危険なサイトをブロックすると、ユーザーのエクスペリエンスと生産性が損なわれる可能性があります。リモートブラウザ隔離（RBI）は、未知のサイトやリスクの高いサイトから、RBIプロバイダがホストする隔離環境にユーザーをリダイレクトします。ウェブサイトはユーザー向けにレンダリングされ、エンドポイントから未知のサイトやリスクの高いサイトに直接アクセスすることなく、必要なリソースを表示できます。

Prisma Accessは、この種のブラウザリダイレクトのためにRBIプロバイダーと簡単に統合できます。わずか1、2ステップで連携するRBIプロバイダーを選択し、次にRBIプロバイダーのホスト環境に誘導するURLカテゴリを選択できます。

サードパーティの*RBI*プロバイダーに加えて、パロアルトネットワークスのリモートブラウザアイソレーション（RBI）も利用でき、*Prisma Access*とネイティブに統合できます。他の分離ソリューションとは異なり、*RBI* は次世代の分離技術を使用して、セキュリティに妥協することなく、ウェブサイトにアクセスするユーザーにネイティブに近いエクスペリエンスを提供します。

Prisma Accessが統合するRBIプロバイダーは次のとおりです。プロバイダーによっては、統合を設定するためにRBI環境の詳細（バニティURLやテナントIDなど）をStrata Cloud Managerに追加する必要がある場合があります。

- **Palo Alto Networks**による**RBI**

  *Palo Alto Networks*の*RBI*と統合するには、リモートブラウザ分離を設定する必要があります。
- **Authentic8**

  *Authentic8*と統合するには、*Authentic8 RBI*環境のバニティ*URL*を手元に用意します。
- **Proofpoint**

  *Proofpoint*と統合するには、*RPI*に*Proofpoint*本番環境または*PoC*環境のどちらを使用するかを選択する準備をしてください。
- **Ericom**

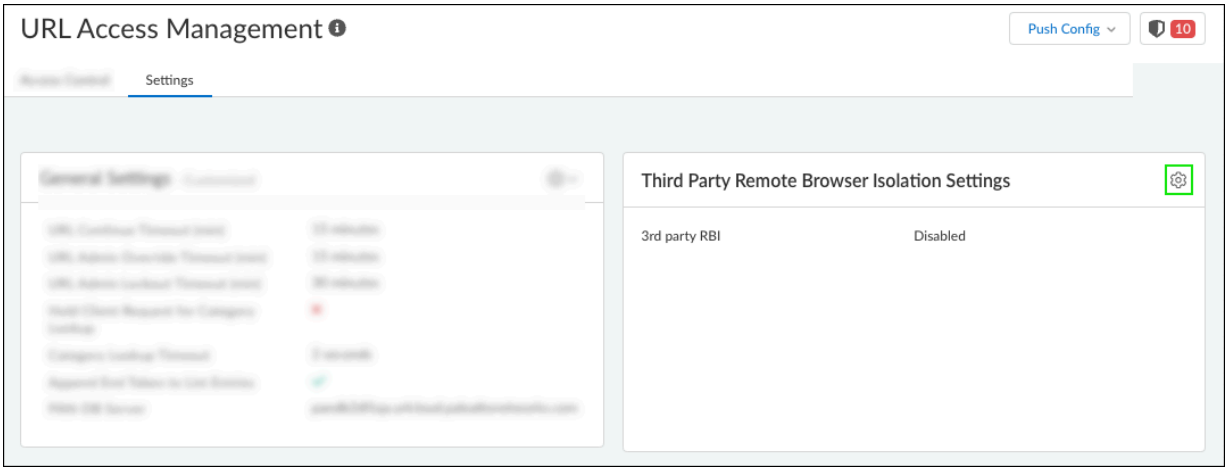
  *Ericom*と統合するには、*Ericom RBI*環境のテナント*ID*を手元に用意します。
- **Menlo Security**

  *Menlo Security RBI*環境の設定は必要ありません。連携を有効にするだけです。

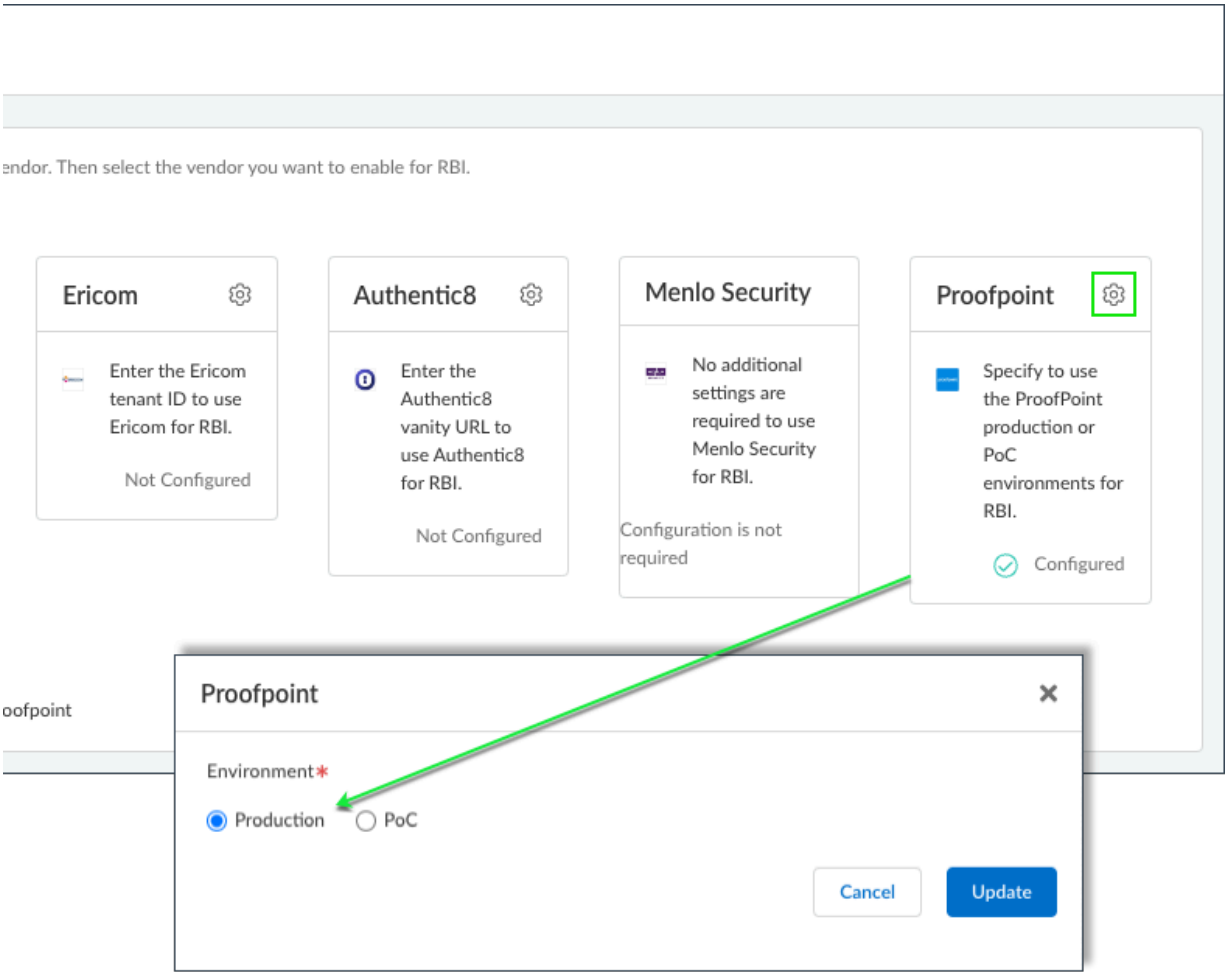
ここでは、サードパーティのRBIプロバイダーをStrata Cloud Managerに追加し、ユーザーをRBI環境にリダイレクトするURLカテゴリを指定する方法を説明します。

STEP 1 | リモートブラウザ分離（RBI）を設定する。

- **[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)]** > **[URL Access Management (URLアクセス管理)]** > **[Settings (設定)]**へと順に移動し、次に**[Third Party Remote Browser Isolation Settings (サードパーティーリモートブラウザ分離の設定)]**を順に開きます。
- ウェブセキュリティ管理者の場合：**[Manage (管理)]** > **[Configuration (設定)]** > **[Web Security (Webセキュリティ)]** > **[Threat Management (脅威管理)]**へと順に移動し、次に**[Third Party Remote Browser Isolation Settings (サードパーティーリモートブラウザ分離の設定)]**を順に開きます。

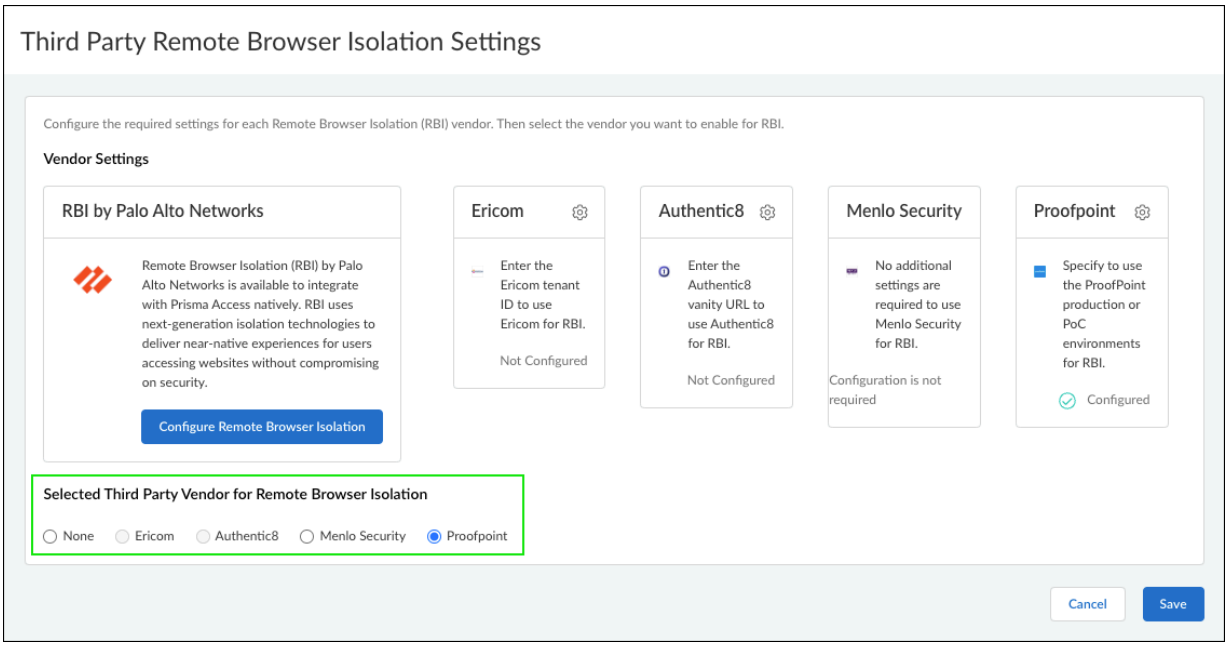


STEP 2 | 使用するRBI環境の指定がRBIで必要かどうかをチェックします。指定する場合は、必要な設定を入力します。



STEP 3 | 次に、有効にするサードパーティのRBIプロバイダーを選択して保存します。以上です!次に［**Push Config (設定をプッシュ)**］を実行すると、RBIプロバイダーがPrisma Accessと統合されます。

また、Palo Alto NetworksによるRBIのライセンスをすでに購入してアクティブにしている場合は、リモートブラウザ分離を設定することもできます。ただし、*Palo Alto NetworksのRBI*とサードパーティの*RBI*ベンダーの両方を使用して分離することはできません。*Palo Alto NetworksのRBI*を使用する場合は、*[なし]* を選択します。それ以外の場合は、***[Selected Third Party Vendor for Remote Browser Isolation (リモートブラウザ分離用のサードパーティベンダーを選択)]*** からサードパーティの*RBI*ベンダーを選択します。

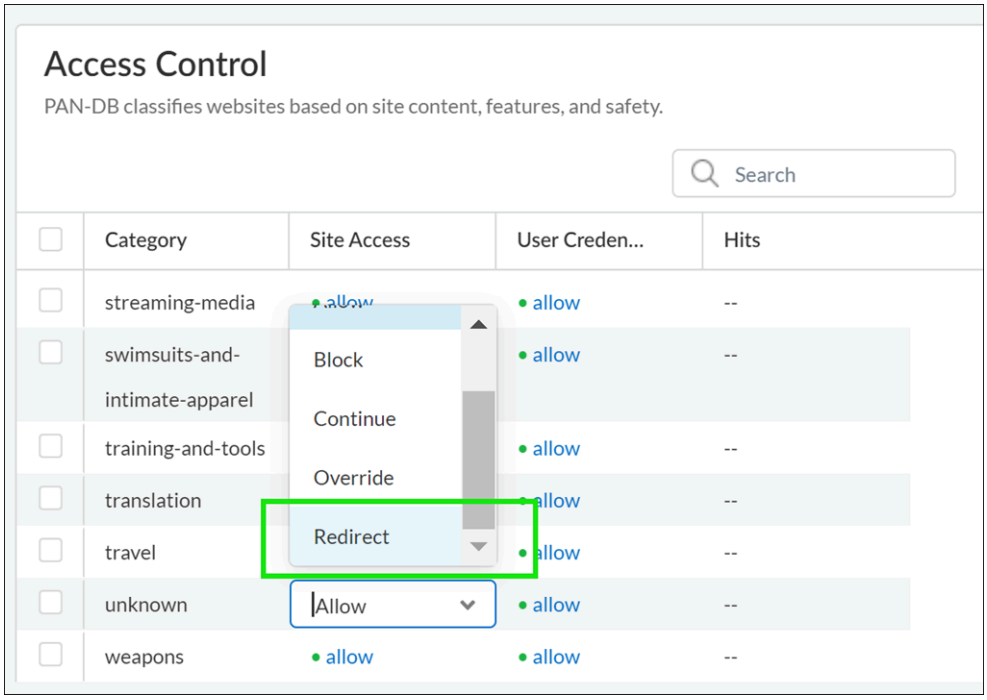


STEP 4 | ここで、ユーザーをRBI環境にリダイレクトするURLカテゴリを指定します。

[URL Access Management (URLアクセス管理)] > [Access Control (アクセス制御)]を選択し、**[URL Access Management Profile (URLアクセス管理プロファイル)]**を追加または編集します。

[Access Control (アクセス制御)]の設定で、**[Site Access (サイトアクセス)]**を**[Redirect (リダイレクト)]**に更新します。

新しい **[Redirect (リダイレクト)]** アクションは、ブロックページを表示する代わりに、ユーザをRBI環境にリダイレクトします。



モニタリング

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

ネットワーク上のWebアクティビティを監視することは、組織を保護し、URLフィルタリングポリシーの有効性を確保するために不可欠です。Palo Alto Networksのプラットフォームは、ダッシュボードやレポートのソースとして機能する詳細なログを生成します。特定の監視およびレポートのニーズに合わせて、ログ、ダッシュボード、レポートをカスタマイズできます。必要に応じて、URLフィルタリング ログからURLカテゴリの変更をリクエストできます。監視ツールが提供する洞察を活用して、Webアクセス ポリシー ルールを微調整し、疑わしいアクティビティを分析して対処します。

HTTPヘッダー ログ記録とログコンテナー ページの機能のみで、ログの詳細とボリュームを制御できます。HTTPヘッダー ログ記録により、ログの粒度が向上します。ユーザーがアクセスするメイン ページのみをログに記録すると、生成されるログの数が減ります。

Webアクティビティ監視ツールと機能の詳細については、次のトピックを参照してください。

- ウェブアクティビティの監視
- ユーザーがアクセスしたページのみを記録
- HTTP ヘッダのロギング
- URL のカテゴリを変更するためのリクエスト

ウェブ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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

さまざまなダッシュボード、レポート、ログを表示して、ネットワーク上のWebアクティビティを確認および分析できます。たとえば、PAN-OS次世代ファイアウォールのApplication Command Center（ACC）では、URLフィルタリングのログとレポートは、警告、ブロック、継続、または上書きに設定されているURLカテゴリのすべてのユーザーのWebアクティビティを表示します。以下のツールでユーザーアクティビティを監視することで、ユーザーベースのウェブアクティビティをよりよく把握し、適切なウェブアクセスポリシールールを決定することができます。

プラットフォーム	ユーザーのウェブアクティビティを表示する方法
PAN-OS & Panorama	• アプリケーションコマンドセンター(ACC) • ネットワークアクティビティウィジェット • URLフィルタリング ログ • URLフィルタリングレポート
Prisma Access	• ログ • インサイト（知見） • 自律型 DEM • アクティビティ

- Strata Cloud Manager
- PAN-OS & Panorama

Webアクティビティのモニタリング(Strata Cloud Manager)

のアクティビティペインは、Prisma Accessの管理に使用しているインターフェイス（PanoramaまたStrata Cloud Managerは）に関係なく、ネットワークで何が起きているかを総合的にStrata Cloud Manager 表示します。さまざまなダッシュボードがアクティビティペインを構成します。アクティビティペインは、Strata Cloud Managerおよび[Device Insights (デバイスインサイト)]アプリケーションで使用できます。アクティビティデータを組織内の他のユーザーと共有することもできます。

次のインタラクティブなダッシュボードは、ネットワーク上のWebアクティビティを監視および分析するのに役立ちます。

- **Threat Insights (脅威インサイト)**：高度なURLフィルタリングやその他のPalo Alto Networksのセキュリティサービスがネットワーク内で検出し、ブロックしたすべての脅威の総合的なビュー。脅威の傾向、影響を受けるアプリケーション、ユーザー、および脅威を許可またはブロックしているセキュリティポリシールールを表示できます。
- **Log Viewer (ログビューア)**：ログは、システム、設定、およびネットワークイベントの監査証跡を提供します。アクティビティダッシュボードからログにジャンプして詳細を取得し、調査結果を調査できます。
- **Application Usage (アプリケーション使用状況)**：ネットワーク上のアプリケーションの概要です。リスク、許可状況、帯域幅使用量、これらのアプリケーションを最もよく使用しているユーザーなどの情報を確認できます。
- **Executive Summary (エグゼクティブサマリー)**（**URL**フィルタリング）：ネットワーク内で最もWebアクティビティが多いURLカテゴリ、悪意のあるURLトップ10、およびリスクの高いURLトップ10を確認できます。
- **User Activity (ユーザーアクティビティ)**：個別ユーザーのブラウジングパターン（特に頻繁にアクセスするサイト、データをやり取りするサイト、リスクが高いサイトへのアクセス試行など）を表示します。URLフィルタリングログとCloud Identity Engineのデータにより、この可視化が可能になります。

  - ユーザーのアクティビティデータにアクセスし、レポートを簡単かつ安全に共有するために、クラウドアイデンティティエンジンをアクティブ化して構成することをお勧めします。

その他の可視性と監視方法：

- ［Reports (レポート)］ペインには、レポート配信のスケジュールを設定したり、レポートをオフラインで表示できるようにいつでもダウンロードして共有したりするためのオプションがあります。
- また、ネットワークとグローバル脅威インテリジェンスの両方の調査結果から導き出された、そのアーティファクトのためだけにデータを操作するセキュリティアーティファクト（IPアドレス、ドメイン、URL、またはファイルハッシュ）を検索することもできます。

[Activity (アクティビティ)]ダッシュボードを開きます。

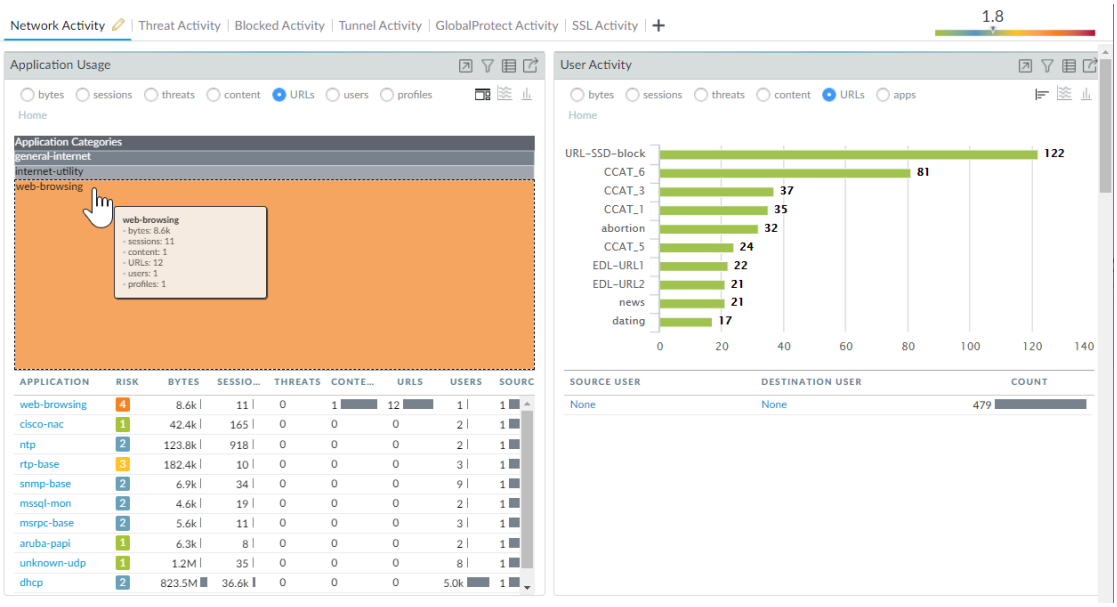
- [アクティビティ] > [脅威インサイト]｜[アプリケーションの使用状況]｜[ユーザーアクティビティ]｜[エグゼクティブサマリー]を選択します。

  URLフィルタリングのエグゼクティブサマリーを表示するには、ダッシュボードにランディングしたときに［URLフィルタリング］タブをクリックする必要があります。
- ログビューアにアクセスするには、[アクティビティ] > [ログ] > [ログビューア]を選択します。

アクティビティレポートのダウンロード、共有、スケジュール設定が可能です。

Webアクティビティのモニタリング(PAN-OS & Panorama)

使用する環境でユーザーが最もよくアクセスしているカテゴリをすばやく把握するには、**ACC** ウィジットを確認します。大抵の **Network Activity (**ネットワーク アクティビティ**)** ウィジェットは、URL で並び替えられるようになっています。たとえば、Application Usage （アプリケーション使用率）ウィジットの場合、最もアクセスされているカテゴリは networking カテゴリで、その次に encrypted tunnel と ssl が続きます。**Threat Activity** [脅威アクティビティ]と **Blocked Activity** [ブロックされたアクティビティ]のリストも URL でソートして表示できます。



ログを表示してログ オプションを設定します：

ACC から直にログ（）にジャンプするか、**Monitor (監視) > Logs (ログ) > URL Filtering (URL フィルタリング)** を選択できます。

各エントリのログ アクションは、該当するカテゴリ用に定義したサイト アクセス設定によって異なります。

- アラート ログ–この例では、computer-and-internet-info カテゴリがアラートに設定されています。

	RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/16 14:10:53	computer-and-internet-info	outlook.office36...	pm wifi	UNTRUST	[redacted]	[redacted]	[redacted]	outlook-web-online	alert

- ブロック ログ–この例では、insufficient-content カテゴリが続行するよう設定されています。そうではなくブロックするようにカテゴリが設定されていた場合、ログの Action (アクション) は block-url になります。

	RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/08 18:47:49	insufficient-content	munchkin.mark...	pm wifi	UNTRUST	[redacted]	[redacted]	[redacted]	ssl	block-continue

- 暗号化されたウェブサイトでアラート ログ–この例では、カテゴリは private-ip-addresses であり、アプリケーションは web-browsing です。このログは、ファイアウォールがトラフィックを復号化したことも示します。

	RECEIVE TIME	CATEGORY	URL	DECRYPTED	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/09 14:11:29	private-ip-addresses	[redacted]/Updates/Updat...	yes	TRUST	UNTRUST	192.168.58.3	[redacted]	[redacted]	web-browsing	alert

「 [local] Inline ML verdict 」 （ PAN-OS 10.0/10.1）と 「 [local and cloud] Inline Categorization verdict 」 （ PAN-OS 10.2以降）は、インラインMLベースのアナライザーによって決定される評決を示します。

- Inline ML verdictは、PAN-OS 10.0/10.1でローカルに運用されているURL Filtering Inline MLを使用して分類されたURLに適用されます。

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE ML VERDICT	ACTION	URL
	10/11 17:32:10	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
	10/11 14:15:14	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
	04/30 15:19:30	medium-risk	medium-risk,unknown	malicious-javascript	block	130.127.24.16/0x39814f84/448d21c8e396e8f4e0eb75de69d6473e033422b...

以下の評決がある。

- フィッシング–ローカルインラインMLによって検出されたフィッシング攻撃コンテンツ。
- **Malicious-javascript**：ローカルのインラインMLによって検出された悪意のあるjavascriptの内容。
- 不明：URLが分類され、コンテンツが良性であると判断されました。

- インライン分類の評決は、ローカルで運用されるURLフィルタリングインラインML（PAN-OS 10.2でローカルインライン分類に改名）と、クラウドインライン分類の

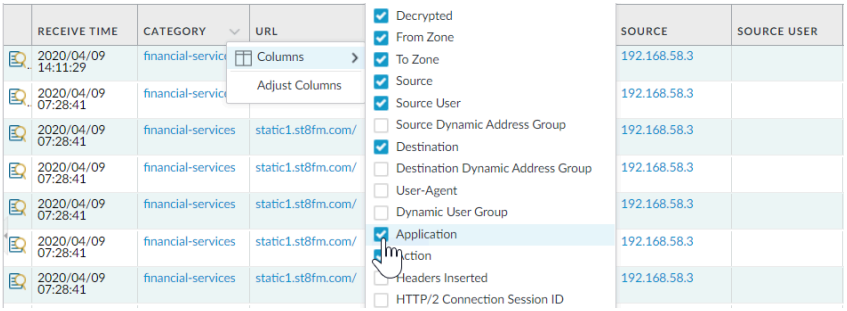
両方を使用して分類されたURLに適用され、高度なURL フィルタリングのクラウドで運用されます。具体的な攻撃の種類は、ログのカテゴリ欄に明記されています。

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE CATEGORIZATI... VERDICT	ACTION	URL
	08/16 15:16:58	computer-and-internet-info	computer-and-internet-info,high-risk	N/A	alert	mlav.testpanw.com/js.html
	08/16 15:16:58	phishing	computer-and-internet-info,high-risk	local	block	mlav.testpanw.com/phishing.html
	08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
	08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com:80/test-inline-content-analysis-phishing

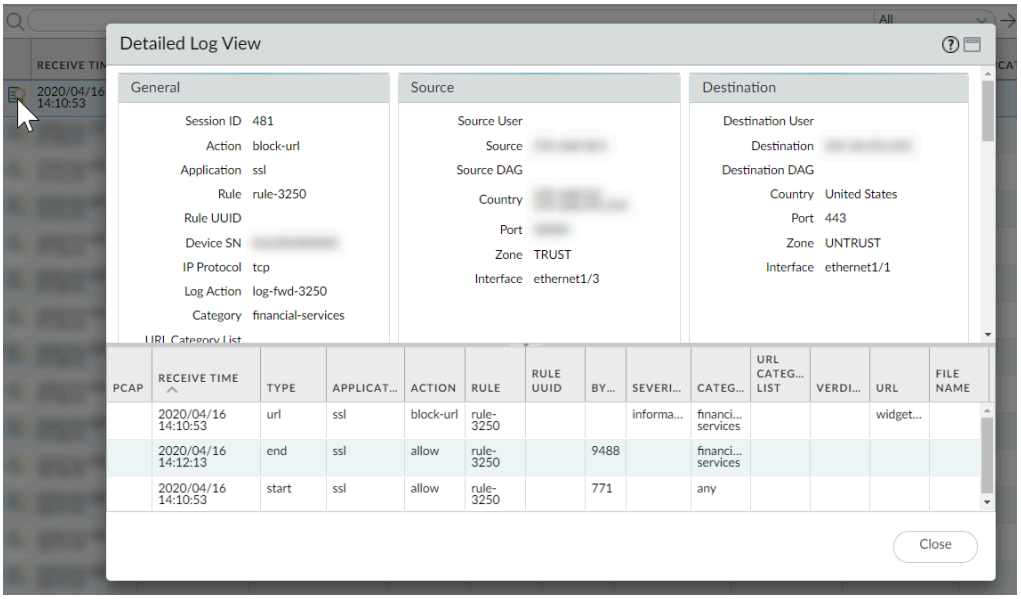
以下の評決がある。

- ローカル–ローカルインライン分類を使用して検出された悪意のあるコンテンツ。
- クラウド–高度なURLフィルタリングクラウドにあるクラウドインライン分類エンジンを使用して、悪意のあるコンテンツを検出します。
- 該当なし–URLはローカルまたはクラウドのインライン分類エンジンで分析されませんでした。

また、送信元ゾーンと宛先ゾーン、コンテンツ タイプ、およびパケット キャプチャを実行するかどうかなどの複数の列を URL フィルタリングのログ ビューに追加することもできます。表示する列を変更するには、任意の列の下向き矢印をクリックし、表示する属性を選択します。

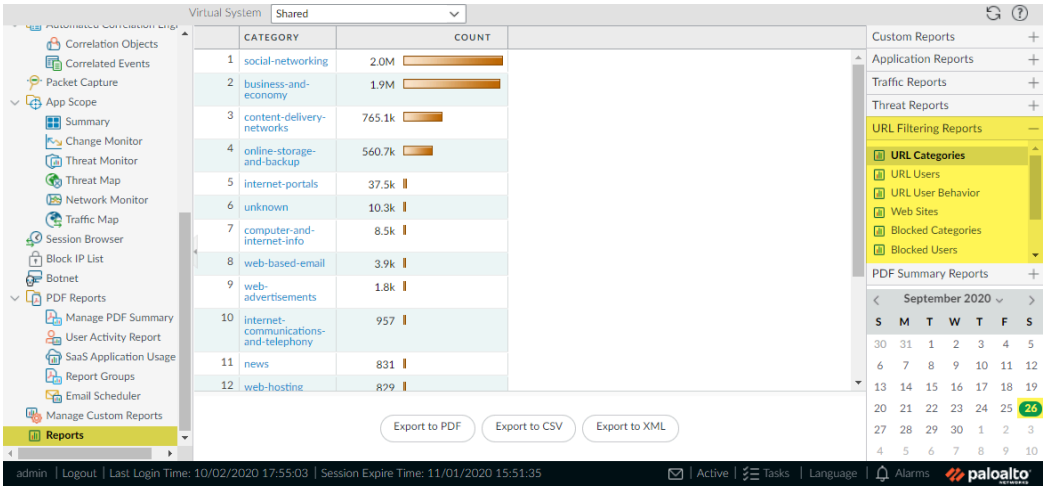


アクセスした特定の URL の完全なログの詳細またはカテゴリの変更要求、あるいはその両方を表示するには、ログの最初の列のログ詳細アイコンをクリックします。



URL カテゴリ、URL ユーザー、アクセスされたウェブサイト、ブロックするカテゴリなどに関する事前定義済みの URL フィルタリング レポートを生成します。

Monitor (監視) > Reports (レポート) を選択し、**URL Filtering Reports (URL** フィルタリング レポート**)** セクションでいずれかのレポートを選択します。レポートには、カレンダーで選択した日付の 24 時間分のデータが含まれます。レポートを PDF、CSV、または XML にエクスポートすることもできます。



ユーザー アクティビティ レポートの表示

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

このレポートでは、ユーザー アクティビティ、グループ アクティビティを迅速に表示し、閲覧時のアクティビティを表示するオプションを提供します。

- Strata Cloud Manager
- PAN-OS & Panorama

ユーザー アクティビティ レポートの表示 (Strata Cloud Manager)

PanoramaまたはStrata Cloud Managerを使用してPrisma Accessを管理している場合でも、Strata Cloud Managerアプリに移動してユーザーアクティビティレポートを生成できます。アプリ内で、アクティビティに移動し、ユーザーアクティビティレポートダッシュボードを見つけます。ユーザーアクティビティデータにアクセスするには、アクティブなCloud Identity Engineテナントが必要です。

STEP 1 | Cloud Identity Engineをアクティベートする。

STEP 2 | Cloud Identity Engineをセットアップする。

STEP 3 | ユーザー アクティビティ レポートを設定します。

1. ［**Activity (アクティビティ)**] > **[User Activity (ユーザー アクティビティ)**］を選択します。
2. ユーザー名を入力すると、1人分のレポートが作成されます。
3. 次の中からレポートの **Type (タイプ)** を選択します。
   - 一人分のレポートを生成するには、**User (ユーザー)** を選択します。
   - 複数のユーザーを対象にする場合は **Group (グループ)** を選択します。

   ユーザー名またはグループ名を選択するには、*User-ID* を にする必要があります。*User-ID* が設定されていない場合は、*[ユーザー]* タイプを選択して、ユーザーのコンピュータの *IP* アドレスを入力します。
4. ユーザー レポートの**Username/IP Address (ユーザー名/IP** アドレス)を入力するか、ユーザー グループ レポートのグループ名を入力します。
5. 期間を選択します。既存の期間または、[カスタム] を選択できます。
6. 閲覧情報をレポートに表示できるように **[Include Detailed Browsing]** チェックボックスをオンにします。

STEP 4 | レポートを実行します。

1. **[今すぐ実行]** をクリックします。
2. ファイアウォールがレポートの生成を完了させたら、いずれかのリンクをクリックしてそれをダウンロードします。
   - **Download User Activity Report (ユーザー アクティビティ レポートをダウンロード)** をクリックすると、PDF 版のレポートをダウンロードできます。
   - 対応するログ エントリの CSV ファイルをダウンロードするには、**Download URL Logs (URL** ログをダウンロード**)** をクリックします。
3. レポートをダウンロードした後、**Cancel (キャンセル)** をクリックします。
4. ユーザー アクティビティ レポートの設定を保存し、同じレポートを後で実行できるようにしたい場合は **OK** をクリックします。そうでない場合は **Cancel (キャンセル)** をクリックします。

STEP 5 | ダウンロードしたファイルを開いて、ユーザー アクティビティ レポートを確認します。PDF 版のレポートには、レポートの基準にしたユーザーあるいはグループ、レポート期間、目次が記載されています。

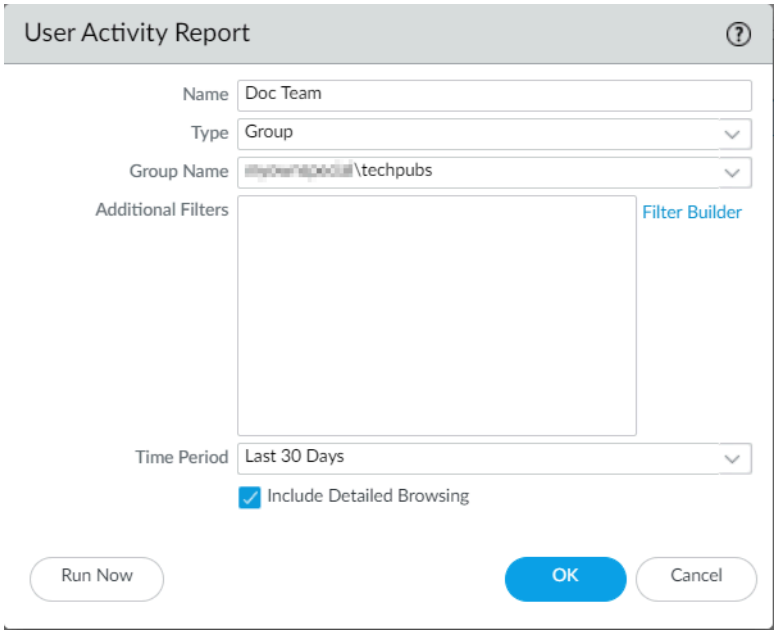
STEP 6 | 目次の項目をクリックして、レポートの詳細を表示します。たとえば、**Traffic Summary by URL Category** （**URL** カテゴリ別トラフィックサマリー）をクリックして、選択されたユーザーまたはグループの統計情報を表示します。

ユーザー アクティビティ レポートの表示 (PAN-OS & Panorama)

STEP 1 | ユーザー アクティビティ レポートを設定します。

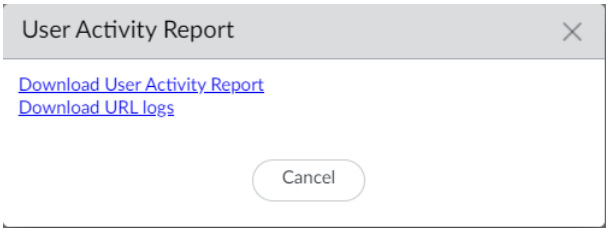
1. **Monitor (監視) > PDF Reports (PDF レポート) > User Activity Report (ユーザー アクティビティ レポート)** の順に選択します。
2. レポートを **Add (追加)** してその **Name (名前)** を入力します。
3. 次の中からレポートの **Type (タイプ)** を選択します。
   - 一人分のレポートを生成するには、**User (ユーザー)** を選択します。
   - 複数のユーザーを対象にする場合は **Group (グループ)** を選択します。

   ユーザー名またはグループ名を選択できるようにするには、User-ID を有効にする必要があります。*User-ID* が設定されていない場合は、*[ユーザー]* タイプを選択して、ユーザーのコンピュータの *IP* アドレスを入力します。
4. ユーザー レポートの**Username/IP Address (ユーザー名/IP アドレス)**を入力するか、ユーザー グループ レポートのグループ名を入力します。
5. 期間を選択します。既存の期間または、[カスタム] を選択できます。
6. 閲覧情報をレポートに表示できるように **[Include Detailed Browsing]** チェックボックスをオンにします。



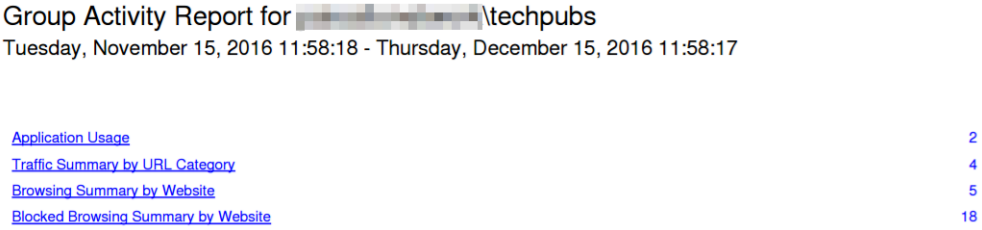
STEP 2 | レポートを実行します。

1. [今すぐ実行] をクリックします。
2. ファイアウォールがレポートの生成を完了させたら、いずれかのリンクをクリックしてそれをダウンロードします。
   - **Download User Activity Report (**ユーザー アクティビティ レポートをダウンロード**)** をクリックすると、PDF 版のレポートをダウンロードできます。
   - 対応するログ エントリの CSV ファイルをダウンロードするには、**Download URL Logs (URL** ログをダウンロード**)** をクリックします。

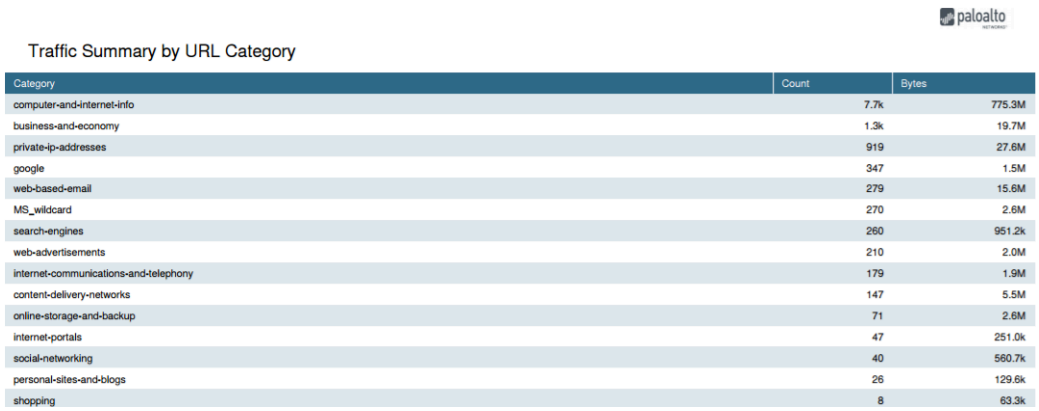


3. レポートをダウンロードした後、**Cancel (**キャンセル**)** をクリックします。
4. ユーザーアクティビティレポートの設定を保存して後で同じレポートを再実行する場合は、**[OK]**をクリックします。それ以外の場合は、**[Cancel (**キャンセル**)]**をクリックします。

STEP 3 | ダウンロードしたファイルを開いて、ユーザー アクティビティ レポートを確認します。PDF 版のレポートには、レポートの基準にしたユーザーあるいはグループ、レポート期間、目次が記載されています。



STEP 4 | 目次の項目をクリックして、レポートの詳細を表示します。たとえば、**Traffic Summary by URL Category** （**URL** カテゴリ別トラフィックサマリー）をクリックして、選択されたユーザーまたはグループの統計情報を表示します。



Category	Count	Bytes
computer-and-internet-info	7.7k	775.3M
business-and-economy	1.3k	19.7M
private-ip-addresses	919	27.6M
google	347	1.5M
web-based-email	279	15.6M
MS_wildcard	270	2.6M
search-engines	260	951.2k
web-advertisements	210	2.0M
internet-communications-and-telephony	179	1.9M
content-delivery-networks	147	5.5M
online-storage-and-backup	71	2.6M
internet-portals	47	251.0k
social-networking	40	560.7k
personal-sites-and-blogs	26	129.6k
shopping	8	63.3k

URLフィルタリングレポートのスケジュールと共有

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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

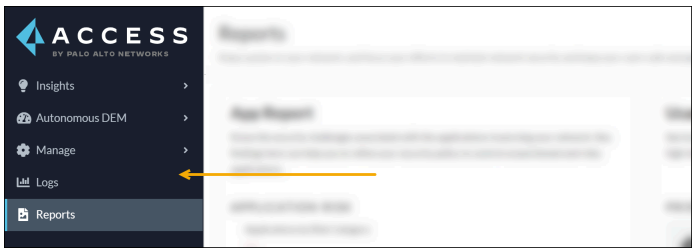
URLフィルタリングやWebアクティビティに関連するさまざまなレポートをスケジュール、生成、共有できます。

- Strata Cloud Manager
- PAN-OS & Panorama

URLフィルタリングレポートのスケジュールと共有(Strata Cloud Manager)

PanoramaまたはStrata Cloud Managerを使用してPrisma Accessを管理している場合でも、URLフィルタリングレポートにStrata Cloud Managerを使用できます。Strata Cloud Managerで、［アクティビティ］に移動して、インタラクティブなURLフィルタリングのデータとレポートを参照します。アクティビティレポートを組織内で共有し、定期的な更新のためにスケジュールすることもできます。URLフィルタリングを活用し、最も関連性の高いPrisma Accessダッシュボードとツールを次に示します。

- エグゼクティブサマリー –ネットワーク内で最もWebアクティビティが多いURLカテゴリ、悪意のあるURLトップ10、高リスクURLトップ10を確認できます。
- ユーザーアクティビティ–個別ユーザーのブラウジングパターン（特に頻繁にアクセスするサイト、データをやり取りするサイト、リスクが高いサイトへのアクセス試行など）を表示します。URLフィルタリングログとCloud Identity Engineのデータにより、この可視化が可能になります。
- ネットワークとグローバル脅威インテリジェンスの両方の調査結果から導き出された、そのアーティファクトのためだけにデータを操作するセキュリティアーティファクト（IPアドレス、ドメイン、URL、またはファイルハッシュ）を検索することができます。



ユーザーのアクティビティデータにアクセスし、レポートを簡単かつ安全に共有するために、クラウドアイデンティティエンジンをアクティブ化して構成することをお勧めします。

STEP 1 | アクティビティレポートのダウンロード、共有、スケジュール設定が可能です。

STEP 2 | URLフィルタリングのエグゼクティブサマリーにアクセスします。

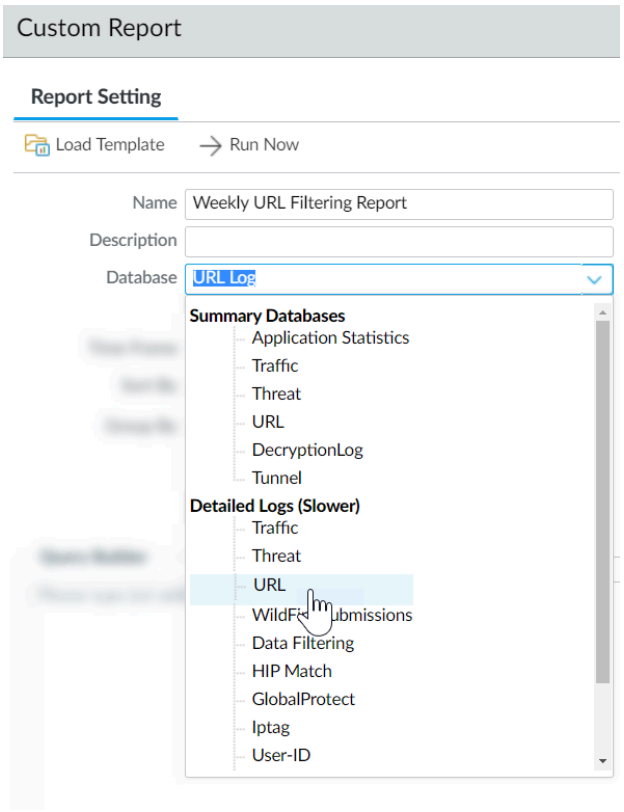
[Activity (アクティビティ)] > [Executive Summary (エグゼクティブサマリー)]を選択し、[URL Filtering (URLフィルタリング)]タブをクリックします。

STEP 3 | セキュリティ アーティファクトの検索。

URLフィルタリングレポートのスケジュールと共有(PAN-OS & Panorama)

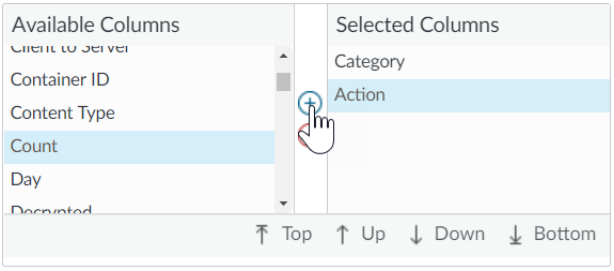
STEP 1 | 新しいカスタム レポートを追加します。

1. **Monitor (監視) > Manage Custom Reports (カスタム レポートの管理)** を選択してレポートを **Add (追加)** します。
2. レポートに一意の **Name (名前)** を付け、任意で **Description (説明)** を加えます。
3. レポートを生成するために使用する **Database (データベース)** を選択します。詳細な URL フィルタリング レポートを生成するためには、Detailed Logs (詳細ログ) セクションで **URL** を選択します。

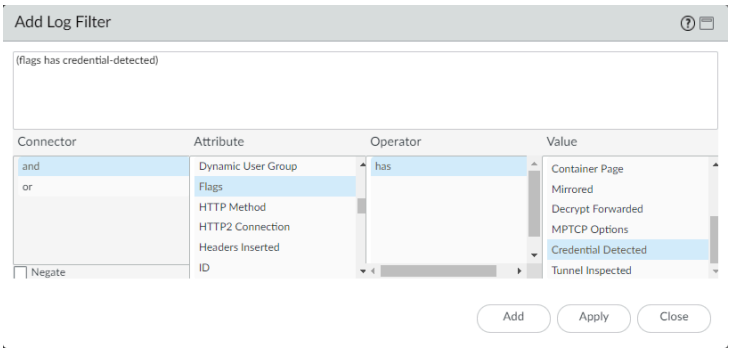


STEP 2 | レポート オプションを設定します。

1. 定義済みの **Time Frame (期間)** あるいは **Custom (カスタム)** を選択します。
2. Available Columns (利用可能な列) リストから、レポートに含めるログの列を選択し、それらを Selected Columns (選択済みの列) に追加します（⊕）。例えば、URL Filtering (URL フィルタリング) レポートについては、次のような選択を行う可能性があります。
   - Action（アクション）
   - アプリケーション カテゴリ
   - カテゴリ
   - 宛先国
   - Source User （送信元ユーザー）
   - URL

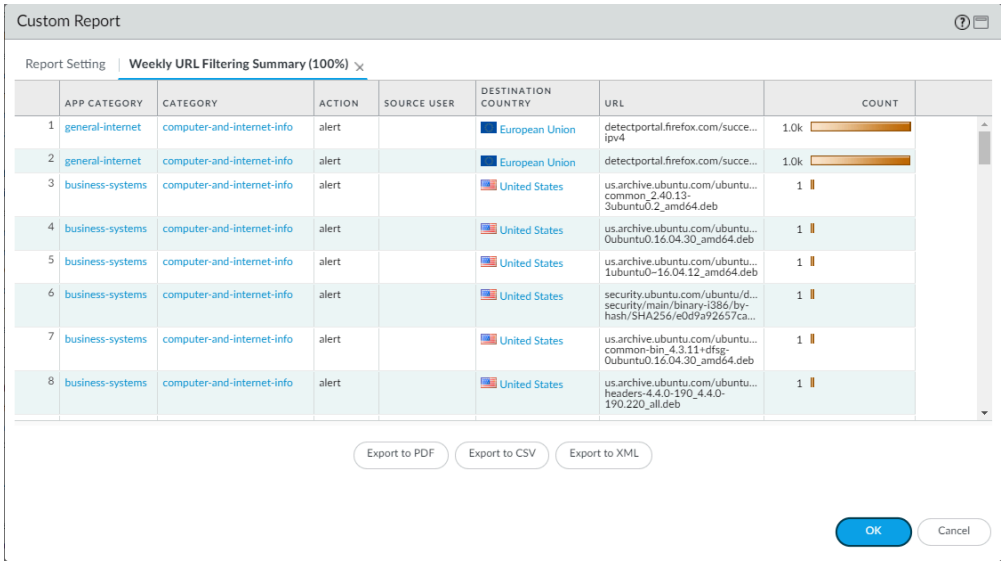


3. ファイアウォールが に対して に設定されている場合は、属性 フラグ 、オペレーター が 、値 の資格情報が検出された を選択して、ユーザーが有効な企業資格情報をサイトに送信したときに記録されるイベントをレポートに含めます。



4. （任意）**Sort By (ソート基準)**オプションを選択し、レポートの詳細を集約するために使用する属性を設定します。ソート基準にする属性を選択しないと、レポートには集約情報なしで最初の N 件の結果が返されます。データのグループ化時にアンカーとして使用する **Group By (グループ化基準)** 属性を選択します。次の例は、**Group By (グルー**

プ化基準) を **App Category** (アプリ カテゴリ) に、**Sort By** (ソート基準) を **Top 5** (トップ 5) の **Count** (カウント) に設定したレポートの例です。



STEP 3 | レポートを実行します。

1. 新しいタブに表示されるレポートをすぐに生成するには、**Run Now** (今すぐ実行) アイコンをクリックします。
2. レポートのレビューが完了したら **Report Setting** (レポート設定) タブに戻り、設定を調整するか、再びレポートを実行するか、次のステップに進んでレポートのスケジュール設定を行います。
3. **Schedule** (スケジュール) チェックボックスを選択し、1 日に一度レポートを実行します。直近の 24 時間の Web アクティビティの詳細に関する日次レポートが作成されます。

STEP 4 | 設定を **Commit**（コミット）します。

STEP 5 | カスタム レポートを表示します。

1. **Monitor** (監視) > **Logs** (ログ)を選択します。
2. 右の列にある **Custom Reports** (カスタム レポート) ペインを開き、表示したいレポートを選択します。最新のレポートが自動的に表示されます。
3. 以前の日付のレポートを表示するためには、カレンダーからその日付を選択します。レポートを PDF、CSV、または XML にエクスポートすることもできます。

ユーザーがアクセスしたページのみを記録

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

コンテナ ページは、Web サイトを訪れるときにユーザーがアクセスするメインのページです。ただし、メインのページと共に追加のページがロードされる場合があります。URL フィルタリング プロファイルで の [ログ コンテナー ページのみ] オプションが有効になっている場合 (Prisma AccessのURLアクセス管理プロファイル)、メイン コンテナ ページのみがログに記録され、コンテナ ページ内に読み込まれる後続のページはログに記録されません。URL フィルタリングではログ エントリが多数生成される可能性があるため、要求されたページ ファイル名が特定の MIME タイプに一致する URI のみがログ エントリに格納されるように、このオプションを有効にすることをお勧めします。デフォルトのセットには、以下の MIME タイプが含まれています。

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml

Log コンテナ ページのみ オプションを有効にすると、ウイルス対策または脆弱性の保護によって検出された脅威に対して、関連する *URL* ログ エントリが常に存在するとは限りません。

- Strata Cloud Manager
- PAN-OS & Panorama

ユーザーがアクセスしたページのみを記録 (Strata Cloud Manager)

> ***Panorama***を使用して***Prisma Access***を管理している場合**:**
>
> *[**PAN-OS & Panorama**]* タブに切り替えて、そこにあるガイダンスに従います。
>
> ***Strata Cloud Manager***をお使いの場合は、こちらに進んでください。

STEP 1 | URLアクセス管理プロファイルで、**[Log Container Page Only (ログコンテナページのみ)]**を選択します。

STEP 2 | URLアクセス管理プロファイルをセキュリティポリシールールに適用します。

URLアクセス管理プロファイルは、セキュリティポリシー規則が参照するプロファイルグループに含まれている場合にのみアクティブになります。

手順に従って、URLアクセス管理プロファイル（および任意のセキュリティプロファイル）をアクティブにします。必ず**[Push Config (設定のプッシュ)]**を行ってください

ユーザーがアクセスしたページのみを記録 (PAN-OS & Panorama)

STEP 1 | 変更するURLフィルタリングプロファイルを作成または選択します。

[Objects (オブジェクト)] > **[Security Profiles (セキュリティ プロファイル)]** > **[URL Filtering (URLフィルタリング)]**の順に選択します。

STEP 2 | コンテナ ページのみログを記録

STEP 3 | **OK** をクリックしてプロファイルを保存します。

STEP 4 | 変更を **Commit (コミット)** します。

HTTP ヘッダのロギング

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URLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

URL フィルタリングでは、ネットワーク上の Web トラフィックを可視化および制御できます。Web コンテンツの可視化を向上させるために、Web 要求に含まれる HTTP ヘッダー属性をログに記録するように URL フィルタリング プロファイルを設定できます。クライアントが Web ページを要求すると、ユーザー エージェント、Referer、x-forwarded-for フィールドが属性-値ペアとして HTTP ヘッダーに格納され、Web サーバーに転送されます。ファイアウォールで HTTP ヘッダーのロギングが有効になっている場合、以下の属性-値ペアが URL フィルタリング ログに記録されます。

HTTP ヘッダーを使用して、*SaaS* アプリケーションへのアクセスを管理することもできます。これを行うために *URL* フィルタリング ライセンスは必要ありませんが、この機能をオンにするには *URL* フィルタリング プロファイルを使用する必要があります。

属性	説明
ユーザーエージェント	ユーザーが URL へのアクセスに使用した Web ブラウザ（Internet Explorer など）。この情報は、HTTP 要求でサーバーに送信されます。 HTTP ヘッダーには、ユーザー エージェントの完全な文字列が含まれていません。ヘッダー・エンドを含むパケットより前のパケットからの最大ログ・バイト数は 36 バイトです。
リファラー	ユーザーを別の Web ページにリンクした Web ページの URL。要求された Web ページにユーザーをリダイレクト（参照）した送信元です。
X-Forwarded-For （XFF）	Web ページを要求したユーザーの IP アドレスを保持する HTTP 要求のヘッダー フィールドのオプション。ネットワー

属性	説明
	クにプロキシ サーバーがある場合、XFF により、Web ページを要求した送信元 IP アドレスとしてプロキシ サーバーの IP アドレスを記録するだけではなく、コンテンツを要求したユーザーの IP アドレスを識別できます。
挿入されたヘッダー	ファイアウォールが挿入するヘッダーのタイプとヘッダーのテキスト。

URLのカテゴリを変更するリクエスト

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) • NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注： • レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。 • Prisma Accessライセンスには*Advanced URL Filtering*機能が含まれます。

ドメインまたはURLが誤って分類されていると思われる場合は、ファイアウォールまたはTest A Site（URLカテゴリ検索ツール）を通じて再分類リクエストを送信できます。Test A Siteから一括再分類リクエストを送信することもできます。どちらの方法でも、レビューしたいURLに対して少なくとも1つの新しいカテゴリを提案する必要があります。

*URL*のリスクカテゴリの変更、またはコンテンツが不十分な*URL*や新規登録されたドメインの変更を要求することはできません。

ファイアウォールでは、URLフィルタリングログエントリの詳細ログビューからURLカテゴリの変更を要求できます。Test A Siteで、PAN-DB分類を表示するには、再分類するウェブサイトを入力する必要があります。リクエストフォームのリンクは検索結果の後に続きます。同様に、Strata Cloud Managerでは、URLアクセス管理のプロファイルを編集するときに利用できる内部テストAサイトツールへのクエリの結果とともに、Test A Siteフォームへのリンクが表示されます。を使用する必要がありますか。一括変更リクエストフォームにアクセスするには、Test A Siteにログインする必要があります。ログインすると、ウェブページに一括依頼フォームへのリンクが表示されます。

誰かが変更リクエストを送信した直後に、自動クローラーがURLを分析します。クローラーがカテゴリ提案を検証した場合、Palo Alto Networksはリクエストを承認し、PAN-DBを新しいカテゴリで即座に更新します。そうでない場合は、パロアルトネットワークスの脅威調査チームとデータサイエンスチームの人間の編集者がリクエストを確認します。元のカテゴリを維持するか、提案されたカテゴリに同意するか、カテゴリを変更するか（元のカテゴリと提案されたカテゴリの両方に同意しない場合）を決定する場合があります。

変更申請後、確認のメールが届きます。調査が完了すると、結果を記載した2通目のメールが届きます。

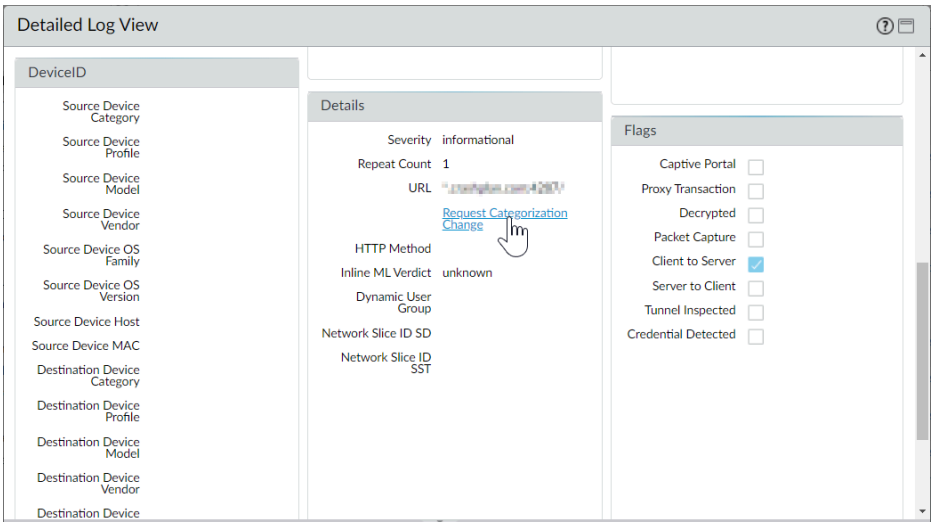
- PAN-OS & Panorama
- Test A Site

URLのカテゴリを変更するリクエスト(PAN-OS & Panorama)

STEP 1 | URLフィルタリングログにアクセスします(**Monitor (監視) > Logs (ログ) > URL Filtering (URL**フィルタリング**)**)。

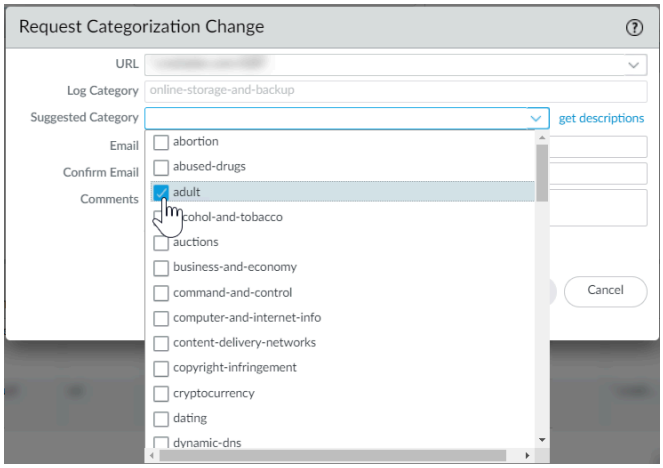
STEP 2 | URL分類を変更したいURLフィルタリングログエントリの［Detailed Log View (詳細ログビュー)］を開きます。

1. ログエントリに対応するスパイグラス（ ）をクリックします。詳細ログビューが表示されます。



STEP 3 | [詳細]で、**[Request Categorization Change (**分類変更を要求**)]**をクリックします。

STEP 4 | リクエストフォームに必要事項を入力し送信します。



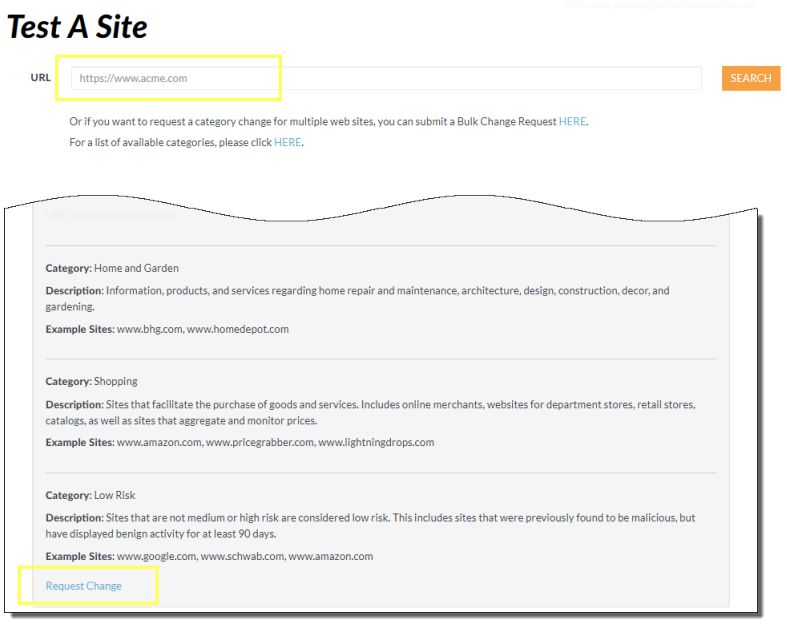
URLのカテゴリ変更リクエスト (Test A Site)

STEP 1 | Test A Site(サイトのテスト)に移動します。

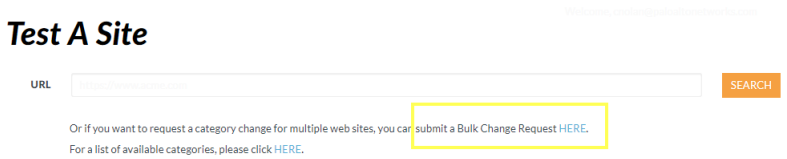
CAPTCHA テストを完了したり、変更リクエスト フォームにメール アドレスを入力したりするのを避けるには、ログインしてください。一括変更リクエスト フォームにアクセスするには、ログインするしかないことに注意してください。

STEP 2 | 完了する変更リクエスト フォームを選択します。

- 単一の**URL**の変更リクエスト- 再分類する**URL**を入力し、**[Search (検索)]**をクリックします。URLカテゴリの結果の下にある**[Request Change (変更をリクエスト)]**をクリックします。



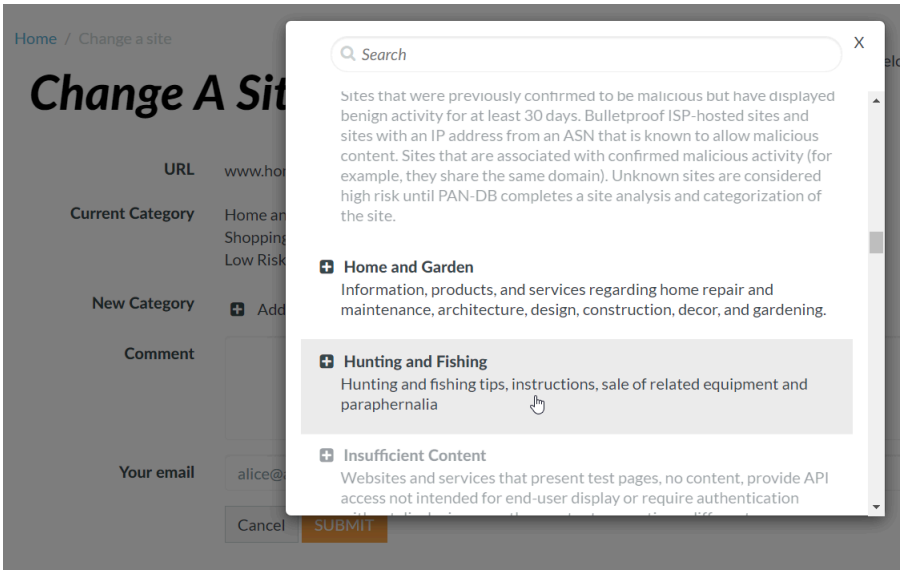
- 一括変更リクエスト- サイトをテストするにはログインしてください。次に、一括変更リクエストを送信をクリックします。ここをクリックしてください。



STEP 3 | 変更リクエストフォームに記入してください。

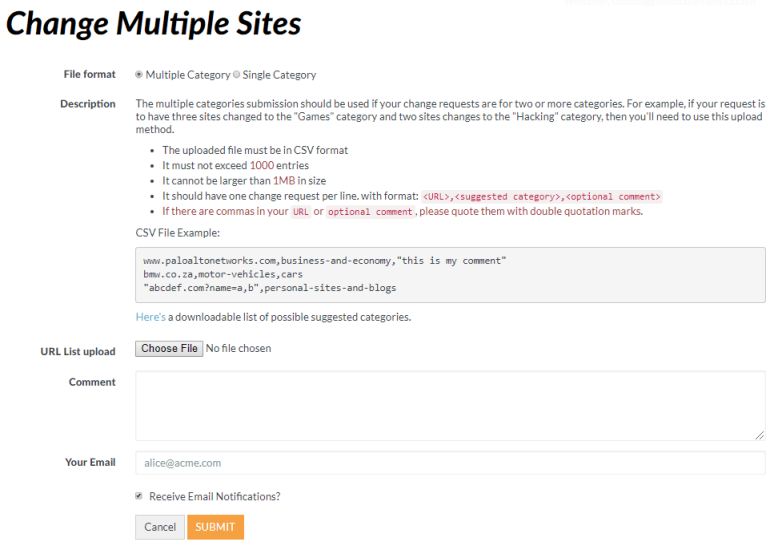
- 単一の**URL**の変更リクエスト- URLに対して最大2つの新しいカテゴリを提案します。**[カテゴリを選択 (リストから)]**をクリックし、一度に1つのカテゴリを選択します。必要に

応じて、リクエストに関するコメントを残します。たとえば、自分の提案がなぜ適切であるかを説明することができます。



- 一括変更リクエスト-ファイル形式を選択します。変更リクエストに2つ以上のカテゴリが含まれる場合は、[Multiple Category (複数のカテゴリ)]を選択します。たとえば、リスト内のURLの半分を`business-and-economy`に再分類し、残りの半分を`personal-sites-and-blogs`に再分類するとします。

  次に、**[Choose File (ファイルを選択)]**をクリックし、アップロードするCSVファイルを選択します。ファイルには、次の形式で1行につき1つの変更要求が含まれている必要があります。`<URL>`、`<first suggested category>`、`<second suggested category>`、`<(optional) comment>`。ファイルは1000エントリを超えることはできず、サイズも1MBを超えることはできません。必要に応じて、リクエストに関するコメントを残します。



STEP 4 | フォームの **Submit**（送信）をクリックします。

トラブルシューティング

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

この章では、Palo Alto Networksの次世代ファイアウォールの一般的なURLフィルタリングの問題を診断および解決するためのタスクについて説明します。これらの問題に関してPalo Alto Networksサポートに連絡する前に、関連するタスクの手順を完了してください。それでもサポートに問い合わせる必要がある場合は、トラブルシューティング タスクの実行から得たすべての情報を必ず含めてください。

多くの場合、*Web*アクティビティのトラブルシューティングとモニタリングは同時に行われます。この章で明示的に説明されていない問題を特定し、トラブルシューティングするには、モニタリングおよびログ記録ツールを頻繁に活用してください。Monitoring (モニタリング)の章でモニタリング ツールとタスクについて詳しく理解してください。

- 高度なURLフィルタリングのアクティブ化に関する問題
- PAN-DB クラウド接続の問題
- Not-Resolved に分類された URL
- 誤った分類
- ウェブサイトへのアクセスに関する問題のトラブルシューティング
- URLフィルタリングの応答ページ表示に関する問題のトラブルシューティング

高度なURLフィルタリングのアクティブ化に関する問題

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

次のワークフローを使用して、高度なURLフィルタリングのアクティブ化の問題をトラブルシューティングします。

STEP 1 | PAN-OS CLI にアクセスします。

STEP 2 | 次のコマンドを実行して、高度なURLフィルタリングがアクティブ化されているかどうかを確認します。

```
show system setting url-database
```

応答が `paloaltonetworks`の場合、PAN-DB（Palo Alto Networks URLフィルタリングデータベース）がアクティブなベンダーです。

STEP 3 | ファイアウォールに有効な高度なURLフィルタリングのライセンスがあることを確認します。

`request license info`CLIコマンドを実行します。

次のライセンス エントリ機能を確認してください。高度な URL フィルタリングライセンスがインストールされていない場合は、ライセンスを取得しインストールする必要があります。URL フィルタリングの設定を参照してください。

STEP 4 | PAN-DB クラウド接続ステータスを確認してください。

PAN-DB クラウド接続の問題

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

*PAN-DB*クラウドへの接続を確実にするために、専用のセキュリティポリシー ルールを作成し、すべての*Palo Alto Management Service*トラフィックを許可します。これにより、管理トラフィックが *`not-resolveed`* として分類されるのを防ぎ、データプレーンを経由する際にトラフィックがブロックされることを防ぐことができます。

firewall と PAN-DB クラウド間の接続を確認するには:

```
show url-cloud status
```

クラウドにアクセスできる場合は、以下のような応答が予測されます。

```
show url-cloud status PAN-DB URL Filtering License : valid Current
 cloud server : serverlist.urlcloud.paloaltonetworks.com Cloud
 connection : connected Cloud mode : public URL database version -
 device :20200624.20296 URL database version - cloud :20200624.20296
 ( last update time 2020/06/24 12:39:19 ) URL database status : good
 URL protocol version - device : pan/2.0.0 URL protocol version -
 cloud : pan/2.0.0 Protocol compatibility status : compatible
```

クラウドにアクセスできない場合は、以下のような応答が予測されます。

```
show url-cloud status PAN-DB URL Filtering License : valid
 Cloud connection : not connected URL database version -
 device :0000.00.00.000 URL protocol version - device : pan/0.0.2
```

次のチェックリストを使用し、接続の問題を特定して解決します。

- ☐ PAN-DB URL フィルタリング ライセンスのフィールドに invalid と表示されていますか？有効な PAN-DB ライセンスを取得してインストールします。
- ☐ URL プロトコルのバージョンが not compatible と表示されていますか？PAN-OS を最新バージョンにアップグレードします。

- ファイアウォールから PAN-DB クラウド サーバーに ping を行えますか？次のコマンドを実行してチェックします。

  ```
  ping source <ip-address> host
   serverlist.urlcloud.paloaltonetworks.com <
  ```

  たとえば、管理インターフェイス IP アドレスが 10.1.1.5 の場合、以下のコマンドを実行します。

  ```
  ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
  ```

- ファイアウォールは HA 構成ですか？ファイアウォールの HA 状態が active、active-primary、あるいは active-secondary 状態であることを確認します。ファイアウォールが他の状態である場合、PAN-DB クラウドへのアクセスがブロックされます。ペアになっている各ファイアウォールに対して次のコマンドを実行し、状態を確認します。

  ```
  show high-availability state
  ```

ファイアウォールおよび PAN-DB クラウド間の接続にまだ問題がある場合は、Palo Alto Networks のサポートにお問い合わせください。

Not-Resolved に分類された URL

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

URLは、ファイアウォールがPAN-DB URLフィルタリング クラウドサービスに接続してルックアップを実行できない場合や、PAN-DBがURLクエリへの応答に時間がかかりすぎる場合、未解決に分類されます。クラウド接続の状態と URL の分類は、有効期限が切れたサブスクリプション ライセンスまたはライセンスのないユーザーには適用されません。URL分類プロセスの詳細については、「URLフィルタリングの仕組み」を参照してください。

次の流れで、PAN-DB で識別される一部またはすべての URL が Not-resolved に分類される問題を解決します。

STEP 1 | **`show url-cloud status`** CLIコマンドを実行して、PAN-DBクラウド接続を確認します。

`Cloud connection:` フィールドに`[connected (接続済)]`と表示されます。`connected (接続済)`以外が表示されている場合、管理プレーン キャッシュに存在しないすべてのURLは、`not-resolved (未解決)`に分類されます。この問題を解決する方法は、PAN-DB クラウド接続の問題を参照してください。

STEP 2 | クラウド接続の状態が `connected` と表示されている場合、ファイアウォールの現在の使用率を確認します。

ファイアウォールの使用状況がスパイク状態である場合、URL 要求はドロップ（管理プレーンに到達することができない）され、`not-resolved`として分類されます。

システムリソースを表示するには、**`show system resources`** CLIコマンドを実行します。次に、%CPU列と%MEM列を表示します。

また、Web インターフェイスの**Dashboard (ダッシュボード)** にある System Resources (システム リソース) ウィジェットでシステム リソースを表示することもできます。

STEP 3 | カテゴリ検索タイムアウト(秒)の値を大きくすることを検討してください。

カテゴリ検索タイムアウト値を大きくすると、URLカテゴリが解決される可能性が高まり、ログで未解決のURLが表示される頻度が減ります。

1. **[Device (デバイス)] > [Setup (セットアップ)] > [Content-ID]**を選択し、URLフィルタリングの設定を編集します。
2. **OK** をクリックし、変更を **Commit (コミット)** します。

   `set deviceconfig setting ctd url-wait-timeout`CLIコマンドを使用して値を更新することもできます。

STEP 4 | 問題が解決しない場合は、Palo Alto Networks サポートにお問い合わせください。

誤った分類

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

時々、カテゴリ分けが間違っていると思われる URL に遭遇することもあるでしょう。次の作業を行うことで、サイトの URL カテゴリを判断し、必要に応じてカテゴリの変更をリクエストできます。

STEP 1 | 以下のコマンドを実行して、データプレーンのカテゴリを確認します。

```
show running url <URL>
```

たとえば、Palo Alto Networks Web サイトのカテゴリを表示するには、以下のコマンドを実行します。

```
show running url paloaltonetworks.com
```

データプレーン キャッシュに保存されている URL のカテゴリが正しい場合（この例では、computer-and-internet-info）、分類は正しく、さらに対策を実行する必要はありません。カテゴリが正しくない場合は、以下の手順に進みます。

STEP 2 | 以下のコマンドを実行して、管理プレーンのカテゴリを確認します

```
test url-info-host <URL>
```

以下に例を示します。

```
test url-info-host paloaltonetworks.com
```

管理プレーン キャッシュに保存されている URL のカテゴリが正しい場合、以下のコマンドを実行して、データプレーン キャッシュから URL を削除します。

```
clear url-cache url <URL>
```

次回、この URL のカテゴリをファイアウォールが要求すると、要求は管理プレーンに転送されます。この処理により問題は解決し、さらに対策を実行する必要はありません。この処理

で問題が解決しない場合は、以下の手順に進み、クラウド システムの URL カテゴリを確認します。

STEP 3 | 以下のコマンドを実行して、クラウドのカテゴリを確認します。

```
test url-info-cloud <URL>
```

STEP 4 | クラウドに保存されている URL のカテゴリが正しい場合、データプレーンおよび管理プレーン キャッシュから URL を削除します。

データプレーン キャッシュから URL を削除するには、以下のコマンドを実行します。

```
clear url-cache url <URL>
```

管理プレーン キャッシュから URL を削除するには、以下のコマンドを実行します。

```
delete url-database url <URL>
```

次回、所定の URL のカテゴリをファイアウォールがクエリすると、要求は管理プレーンに転送され、さらに、クラウドに転送されます。これで、カテゴリ検索に関する問題は解決します。問題が解決しない場合は、以下の手順を参照して、分類の変更要求を提出します。

STEP 5 | Web インターフェイスから変更要求を提出するには、URL ログに移動して、変更する URL のログ エントリを選択します。

STEP 6 | [分類の変更要求] リンクをクリックして、以下の手順を実行します。URLを検索し、変更要求アイコンをクリックして、Palo Alto NetworksのTest A SiteWebサイトからカテゴリ変更を要求することもできます。各カテゴリの説明については、[定義済みURLカテゴリ]を参照してください。

変更要求が承認されると、電子メール通知が送信されます。その後、2 つの方法で、ファイアウォールで URL カテゴリが更新されたことを確認できます。

- キャッシュ内の URL の有効期限が切れるまで待機します。次回ユーザーが URL にアクセスするときに、新しい分類の更新がキャッシュに配置されます。
- 以下のコマンドを実行して、キャッシュの更新を強制的に行います。

```
request url-filtering update url <URL>
```

ウェブサイトへのアクセスに関する問題のトラブルシューティング

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

エンドユーザーは、URLフィルタリングライセンスの欠落、ポリシールールの設定ミス、PAN-DB接続の問題、Webサイトの誤分類など、さまざまな理由でWebサイトへのアクセスに問題に遭遇する可能性があります。次の手順を使用して、Web サイトへのアクセスに関する問題を診断し、解決します。

問題が*URL*フィルタリングに関連していない可能性があります。このタスクのステップに続く*[What to do next (次に行うこと)]*セクションには、トラブルシューティングの焦点を絞る追加の領域がリストされています。

STEP 1 | アクティブな高度なURLフィルタリング ライセンスまたは従来のURLフィルタリング ライセンスがあることを確認します。

次世代のファイアウォールが*Web*サイトやアプリケーションを正確に分類するには、アクティブな*URL*フィルタリングライセンスが必要です。*URL*フィルタリングライセンスがない場合、*Web*サイトへのアクセスの問題は*URL*フィルタリングとは無関係です。

[Device (デバイス)] > **[Licenses (ライセンス)]** をクリックし、高度なURLフィルタリング(またはPAN-DB URLフィルタリング)ライセンスを探します。アクティブなライセンスには、現在の日付より後の有効期限が表示されます。

または、ライセンス情報をリクエストするCLIコマンドを使用します。ライセンスがアクティブな場合、インターフェイスには有効期限ステータスなどのライセンス情報が表示されます。有効期限切れ： なし。

STEP 2 | PAN-DB クラウド接続ステータスの確認をCLIで実施します。

`Cloud connection:` フィールドに`[connected (接続済)]`と表示されます。それ以外の場合、管理プレーン(MP)キャッシュに存在しないURLは未解決に分類されます。また、セキュリティポリシールールのURLフィルタリングプロファイル設定によってブロックされる場合があります。

STEP 3 | 特定のURLのMPおよびデータプレーン(DP)キャッシュをクリアします。

キャッシュのクリアは、リソースを大量に消費する可能性があります。メンテナンス期間中にキャッシュをクリアすることを検討してください。

1. MP キャッシュをクリアするには、**`delete url-database url <affected url>`** CLI Iコマンドを使用します。
2. DP キャッシュをクリアするには、**`clear url-cache url <affected url>`** CLI コマンドを使用します。

STEP 4 | URLフィルタリング ログを確認して、Web サイトが属するURLカテゴリがブロックされているかどうかを確認します。

1. モニター > **URL**フィルタリング を選択します。
2. 影響を受けるURLを検索し、最新のログ エントリを選択します。
3. [Category (カテゴリ)]列と[Action (アクション)]列を確認します。

   URLは正しく分類されていますか?以下を使用してカテゴリを確認します：Test A Site (サイトのテスト)、パロアルトネットワークスのURLカテゴリ検索ツール。それでも分類が間違っていると思われる場合は、変更リクエストを送信する。

   ブロックURLが表示されている場合、ログ・エントリーに関連付けられたセキュリティー・ポリシー・ルールの名前をメモします。

STEP 5 | セキュリティ ポリシー ルールを確認し、必要に応じて更新します。

1. **[ポリシー (Policies)]** > **[セキュリティ (Security)]**し、前のステップでメモした名前のポリシールールを選択します。
2. セキュリティ ポリシー ルールで、要求されたURLまたはそのURLカテゴリへのアクセスが許可されていることを確認します。

   次の2つの構成のいずれかを探します:

   - 一致条件としての**URL**カテゴリ:**[Service/URL Category (サービス/URL カテゴリ)]**の場合、指定されたカテゴリの1つに要求されたURLが含まれています。**[Actions (アクション)]**の場合、[Action Setting (アクション設定)]は許可に設定します。
   - **URL**フィルタリング プロファイル:**[Actions (アクション)]**の場合、[プロファイル設定]は、要求されたURLへのアクセスを許可するURLフィルタリング プロファイルに設定されます。

STEP 6 | セキュリティポリシールールをテストします。

上記の手順で問題が強調表示または解決されない場合は、問題をさらに切り分けるために追加のトラブルシューティングが必要になる場合があります。重点分野には以下を含める必要があります。

- 基本的な P アドレス接続
- ルーティング設定
- DNS解決

- プロキシの構成
- パケット パス内のアップストリーム ファイアウォールまたは検査デバイス

断続的または複雑な問題については、パロアルトネットワークスのサポートにお問い合わせください。

URLフィルタリングの応答ページ表示に関する問題のトラブルシューティング

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

URLフィルタリングの応答ページは、次のようなさまざまな理由で表示されない場合があります。

- SSL/TLSハンドシェイク検査は有効になっています。
- SSL/TLSハンドシェイクの検査中にウェブサイトがブロックされた。この場合、ファイアウォールがHTTPS接続をリセットするため、URLフィルタリングの応答ページは表示されません。
- ウェブサイトはHTTPSプロトコルを使用しているか、HTTPSで配信されるコンテンツ（広告など）が含まれているが、ウェブサイトまたはURLカテゴリが復号化されていない。
- カスタム応答ページが、サポートされる最大サイズを超えています。

URLフィルタリングの応答ページが表示されない場合のトラブルシューティングの出発点として、次の手順を使用してください。問題が解決しない場合は、Palo Alto Networks サポートにお問い合わせください。

STEP 1 | 問題の範囲を決定します。

問題は特定のウェブサイトに固有のものか、Webページのサブセットに固有のものか。Webサイトの別のページにアクセスしたときに、応答ページが表示されるかどうかを確認します。

STEP 2 | Webサイトのプロトコル（HTTPまたはHTTPS）を識別する。

この区別は、問題のさらなる切り分けと診断に役立ちます。

STEP 3 | （HTTPSサイトまたはHTTPSコンテンツを持つHTTPサイト）SSL/TLS復号化ポリシールールが、ウェブサイトまたはURLカテゴリへのトラフィックを復号化することを確認します。

一般的に、ファイアウォールは*HTTPS*ウェブサイトの応答ページを配信できません。

ウェブサイトによっては、*HTTP*でプライマリページを提供するが、*HTTPS*で広告やその他のコンテンツを提供する場合があります。これらのウェブサイトも、応答ページの表示を保証するために復号化する必要があります。

1. Web インターフェイスにログインします。
2. **[ポリシー (Policies)]** > **[復号化 (Decryption)]**を選択し、関連するルールが特定のWebサイトまたはURLカテゴリへのトラフィックを復号化することを確認します。

   そうでない場合は、復号化ポリシールールを更新して、ウェブサイトまたはURLカテゴリを復号化します。

- SSL/TLS復号化が有効になっていても応答ページが表示されない場合は、SSL/TLSハンドシェイクの検査を有効にします。
- SSL/TLS復号化を有効にせずにHTTPSセッションでURLフィルタリング応答ページを提供するには、次の手順に従います。

STEP 4 | Webサイトが属するURLカテゴリがブロックされていることを確認します。

セキュリティポリシー規則に適用されたURLフィルタリングプロファイル、または特定のURLカテゴリを一致基準とするセキュリティポリシー規則によってカテゴリがブロックされている場合、特定のエントリの ［アクション］ カラムの値に`block-url` (ブロックURL) が表示されます。

1. **[Monitor (監視)]** > **[URL Filtering (URLフィルタリング)]**を選択します。
2. 影響を受けるウェブサイトを検索し、最新のログエントリを選択します。
3. カテゴリ列とアクション列を調べます。

   ウェブサイトに割り当てられたカテゴリは正確ですか？以下を使用してカテゴリを確認します：Test A Site (サイトのテスト)、パロアルトネットワークスのURLカテゴリ検索ツール。それでもウェブサイトが正しく分類されていないと思われる場合は、変更リクエストを送信します。

   Action (アクション)の値は`block-url`ですか？更新されていない場合は、URLフィルタリングプロファイルまたはセキュリティポリシールールを更新します。
4. 今後の参照のために、このログエントリに関連付けられた規則を書き留めておきます。

STEP 5 | カスタム応答ページがこの問題の原因であるかどうかを判断します。

1. **[Device (デバイス)]** > **[Response Pages (応答ページ)]**の順に選択します。
2. **[Predefined (事前定義)]**のみが選択されていることを確認します。

   カスタム応答ページは、共有が（**Predefined (事前定義)**に加えて）次のいずれかの場所にリストされている場合にアクティブになります。

   - **[Device (デバイス)]** > **[Response Pages (応答ページ)]**の順に選択します。所定の応答ページに対応する[Location (ロケーション)]列の下。
   - **[Device (デバイス)]** > **[Response Pages (応答ページ)]** > ***[Type (種類)]***の順に選択します。ユーザーロケーション。
3. （**[Shared (共有済)]**がリストされている場合）カスタムページをデフォルトの状態に戻して、カスタム応答ページが問題であることを確認します。

   1. カスタムページを削除します。
   2. 変更を **Commit (コミット)** します。
   3. 影響を受けるWebサイトにアクセスして、デフォルトの応答ページが表示されるかどうかを確認します。

   問題が解決しない場合は、サポートに連絡して詳細を調査してください。

上記の手順で問題を解決できない場合は、Palo Alto Networksのサポートにお問い合わせください。問題を特定するには、追加のトラブルシューティングが必要になる場合があります。たとえば、サポートと並行してパケットキャプチャ（pcap）ツールを介してトラフィックを分析することは、応答ページが一部のウェブページでは機能しないが、別のウェブページでは機能する場合に役立ちます。

PAN-DB 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)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

PAN-DBプライベート クラウドは、パブリック クラウド サービスの使用を制限する組織向けのオンプレミス ソリューションです。特にファイアウォールは、PAN-DBパブリッククラウドサーバではなく、URLルックアップ中にPAN-DBプライベートクラウドサーバにクエリを実行します。このソリューションを実装するには、ネットワークまたはデータセンター内に1台以上のM-600またはM-700アプライアンスをPAN-DB サーバーとしてデプロイする必要があります。PAN-DBプライベートクラウドと通信できるのは、PAN-OS 9.1以降のバージョンを実行しているファイアウォールのみです。を表すように修正されたら、xrefを「deploy (デプロイ)」に追加

*PAN-DB*プライベートクラウドの導入では、*Advanced URL Filtering*サブスクリプションのクラウドベースの*URL*分析機能はサポートされていません。

PAN-DBパブリッククラウドとPAN-DBプライベートクラウドの違いを次の表に示します。

表 **1 : PAN-DB** パブリック クラウドと **PAN-DB** プライベート クラウドの差異

差異	PAN-DB パブリック クラウド	PAN-DB プライベート クラウド
コンテンツ更新およびデータベース更新	コンテンツ（定期および重要）更新と完全なURLデータベース更新は、1日に複数回公開されます。PAN-DBパブリッククラウドは、マルウェアおよびフィッシングのURLカテゴリを5分毎に更新します。ファイアウォールは、URL検索のためにクラウド サーバーをクエリするたびに、重要な更新がないかチェックします。	コンテンツ更新と完全な URL データベース更新は、営業日に 1 日に 1 回提供されます。
URL 分類の要求	URL分類変更は、次の方法でリクエストできます。	URL分類の変更は、Palo Alto NetworksのTest A SiteWebサイトからリクエストできます。

差異	PAN-DB パブリック クラウド	PAN-DB プライベート クラウド
	• Palo Alto Networks Test A Site Web サイト。 • URLフィルタリング プロファイル。 • URLフィルタリング ログ。	
未解決の **URL** クエリ	ファイアウォールがURLクエリを解決できない場合、要求はパブリック クラウドのサーバーに送信されます。	ファイアウォールがクエリを解決できない場合、要求はPAN-DBプライベート クラウドのアプライアンスに送信されます。URLの一致がない場合、PAN-DBプライベート クラウドはカテゴリ「未知」応答をファイアウォールに送信します。アプライアンスにPAN-DB パブリック クラウドへのアクセスを設定していない限り、要求がパブリック クラウドに送信されることはありません。 PAN-DBプライベートクラウド内のアプライアンスが完全にオフラインで動作する場合、ファイアウォールはパブリッククラウドにデータや分析を送信しません。

- PAN-DBプライベートクラウドの仕組み
- PAN-DBプライベートクラウドアプライアンス
- PAN-DBプライベートクラウドのセットアップ

PAN-DBプライベートクラウドの仕組み

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

PAN-DBプライベートクラウドをセットアップすると、M-600またはM-700アプライアンスがインターネットに直接アクセスできるように設定したり、オフラインのままにしたりできます。アプライアンスでは、URLルックアップを実行するためにデータベースとコンテンツの更新が必要です。アプライアンスがアクティブなインターネット接続を持っていない場合、ネットワーク上のサーバーに手動でアップデートをダウンロードし、SCPを使用してPAN-DBプライベートクラウド内の各M-600またはM-700アプライアンスにアップデートをインポートする必要があります。またアプライアンスはシード データベースと、サービスを提供するファイアウォール用のその他の定期更新コンテンツ更新または重要なコンテンツ更新を入手できる状態でなければなりません。

URLルックアッププロセスは、プライベートクラウドとパブリッククラウドの両方の展開でファイアウォールで同じです。ただし、プライベートクラウドの導入では、ファイアウォールはPAN-DBプライベートクラウド内のサーバにクエリを実行します。ファイアウォールにプライベートクラウドサーバーへのアクセスを許可するには、問い合わせ可能な各M-600またはM-700サーバーのIPアドレスまたはFQDNを指定する必要があります。

M-600およびM-700アプライアンスは、PAN-DBプライベートクラウドに接続するファイアウォールの認証に、パッケージ化されたサーバ証明書を使用します。認証に別のサーバー証明書をインポートまたは使用することができません。アプライアンスのホスト名を変更する場合、アプライアンスはファイアウォールを認証するための新しい証明書のセットを自動的に生成します。

PAN-DBプライベートクラウドアプライアンス

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

PAN-DBプライベート クラウドをデプロイするには、1台以上のM-600またはM-700 アプライアンスが必要です。どちらのアプライアンスもパノラマモードで出荷されますが、PAN-DBプライベートクラウドとして導入するには、PAN-URL-DBモードで動作するように設定する必要があります。PAN-URL-DB モードでは、このアプライアンスは PAN-DB パブリック クラウドを使用しない企業向けに URL 分類サービスを提供します。

PAN-DBプライベート クラウドとしてデプロイされたM-600またはM-700アプライアンスは、MGT（Eth0）とEth1の2つのポートを使用します。Eth2 は使用できません。管理ポートは、アプライアンスへの管理アクセスや、最新のコンテンツ更新を PAN-DB パブリック クラウドまたはネットワーク上のサーバーから入手するときに使用します。PAN-DB プライベート クラウドとネットワーク上のファイアウォール間の通信には、MGT ポートまたは Eth1 を使用できます。

M-200 アプライアンスは *PAN-DB* プライベート クラウドとしてデプロイできません。

PAN-URL-DBモードのM-600およびM-700アプライアンスには、以下の留意事項があります。

- Web インターフェイスを持たない場合は、コマンド ライン インターフェイス(CLI)のみをサポートします。
- Panorama による管理はできません。
- 高可用性ペアでのデプロイはできません。
- URL フィルタリング ライセンスは必要ありません。ファイアウォールが PAN-DB プライベート クラウドに接続してクエリするには、有効なPAN-DB URL Filtering ライセンスが必要です。
- 出荷時に、PAN-DB プライベート クラウドに接続するファイアウォールを認証するために使用するデフォルトのサーバー証明書のセットが付属します。ファイアウォールの認証に別のサーバー証明書をインポートまたは使用することができません。アプライアンスのホスト名を変更すると、アプライアンスは、サービス提供先のファイアウォールを認証するための新しい証明書のセットを自動的に生成します。
- Panorama モードへのリセットしかできません。アプライアンスを専用ログコレクターとしてデプロイする場合は、Panoramaモードに切り替えてから、Log Collectorモードに設定します。

PAN-DBプライベートクラウドのセットアップ

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

ネットワークまたはデータセンター内に1台以上のM-600またはM-700アプライアンスをPAN-DBプライベート クラウドとしてデプロイするためには、次のタスクを完了させる必要があります。

- PAN-DBプライベートクラウドの設定
- PAN-DBプライベート クラウドにアクセスするためのファイアウォールの設定
- PAN-DB プライベート クラウド上のカスタム証明書による認証の設定

PAN-DB プライベート クラウドの設定

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

STEP 1 | M-600またはM-700アプライアンスをラックマウントします。

関連するハードウェア リファレンスガイドのラック設置手順を参照してください。

STEP 2 | アプライアンスを登録します。

STEP 3 | アプライアンスの初期設定を実行します。

PAN-DB モードの *M-600*および*M-700*アプライアンスは、*MGT*（*Eth0*）と*Eth1*の*2*つのポートを使用します。*Eth2*は*PAN-DB*モードでは使用しません。管理ポートは、アプライアンスへの管理アクセスと、*PAN-DB* パブリック クラウドから最新のコンテンツ更新を取得するために使用します。アプライアンス（*PAN-DB* サーバー）とネットワーク上のファイアウォール間の通信には、*MGT* ポートまたは *Eth1* を使用できます。

1. 以下のいずれかの方法でアプライアンスに接続します。
   - コンピュータからアプライアンスのコンソール ポートにシリアル ケーブルを接続し、ターミナル エミュレーション ソフトウェア（9600-8-N-1）を使用して接続します。
   - コンピュータからアプライアンスのMGTポートにRJ-45イーサネット ケーブルを接続します。ブラウザで、https://192.168.1.1 に移動します。この URL にアクセスできるようにするには、コンピュータの IP アドレスを、192.168.1.0 ネットワークでのアドレス（192.168.1.2 など）に変更しなければならない場合があります。
2. ログインを促されたら、アプライアンスにログインします。デフォルトのユーザー名とパスワード（admin/admin）を使用してログインします。アプライアンスの初期化が開始されます。
3. IP アドレスなど、MGT インターフェイスのネットワーク アクセス設定を行います。

   次のCLIコマンドを使用します。**set deviceconfig system ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***。

   変数の説明：
   - *<server-IP>*はサーバの管理インターフェイスに割り当てたいIPアドレスを示します
   - *<netmask>*はサブネットマスクを示します
   - *<gateway-IP>*はネットワークゲートウェイのIPアドレス、*<DNS-IP>*はプライマリDNSサーバのIPアドレスをそれぞれ示します
   - *<DNS-IP>*はDNSサーバのIPアドレスを示します
4. IPアドレスなど、Eth1インターフェイスのネットワーク アクセス設定を行います。

   次のコマンドを使用します。**set deviceconfig system eth1 ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***。
5. 変更を PAN-DB サーバーに保存します。

   commitコマンドを使用します。

STEP 4 | PAN-DB プライベート クラウド モードに切り替えます。

Panorama モードから *PAN-DB* モード（およびその逆）、Panorama モードから ログ コレクタ モード（およびその逆）に切り替えることができます。*PAN-DB* モードからログ コレクタ モード（またはその逆）への直接の切り替えはサポートされていません。操作モードを切り替えると、データがリセットされます。管理アクセスの設定を除き、再起動時に既存の設定とログはすべて削除されます。

1. PAN-DB モードに切り替えるには、**request system system-mode pan-url-db**コマンドを使用します。
2. モードスイッチを確認するには、**show system info**コマンドを使用します。

   PAN-DBプライベートクラウドモードへの切り替えに成功すると、システムモードフィールドにPAN-URL-DBと表示されます。

```
admin@M-600> システム情報を表示 ホスト名:M-600 ip-address:1.2.3.4
 public-ip-address: netmask:255.255.255.0 default-
gateway:1.2.3.1 ipv6-address: unknown ipv6-link-
local-address: fe80:00/64 ipv6-default-gateway: mac-
address:00:56:90:e7:f6:8e time:Mon Apr 27 13:43:59
 2015 uptime:10 days, 1:51:28 family: m model:M-600
 serial:0073010000xxx sw-version:7.0.0 app-version:492-2638
 app-release-date:2015/03/19 20:05:33 av-version:0 av-release-
date: unknown wf-private-version:0 wf-private-release-date:
 unknown wildfire-version:0 wildfire-release-date: logdb-
version:7.0.9 platform-family: m pan-url-db:20150417-220
 system-mode:Pan-URL-DB operational-mode: normal licensed-
device-capacity:0デバイス証明書のステータス：なし
```

3. アプライアンスのクラウドデータベースのバージョンを確認するには、**show pan-url-cloud-status**コマンドを使用します。

   system-info 表示の*pan-url-db*フィールドにも同じ情報が含まれています。

STEP 5 | コンテンツおよびデータベース更新をインストールします。

アプライアンスには、コンテンツの現在実行中のバージョンと*1*つ前のバージョンのみが保存されます。

次のいずれかのインストール方法を選択します。

- PAN-DB サーバーがインターネットに直接アクセスできる場合は、以下のコマンドを使用します。
  - 新しいバージョンが発行されているかどうかを確認するには：**request pan-url-db upgrade check**
  - 現在サーバにインストールされているバージョンを確認するには：**request pan-url-db upgrade info**。
  - 最新バージョンをダウンロードするには：**request pan-url-db upgrade download latest**。

    最新バージョンをインストールするには：**request pan-url-db upgrade install <*version latest | file*>**。
  - アップデートを自動的にチェックするようにアプライアンスをスケジュールするには：**set deviceconfig system update-schedule pan-url-db recurring weekly action download-and-install day-of-week <*day of week*> at <*hr:min*>**。
- PAN-DBサーバーがオフラインの場合は、Palo Alto Networksカスタマーサポートウェブサイトにアクセスして、コンテンツ更新をダウンロードし、ネットワークのSCPサーバーに保存します。その後で、以下のコマンドを使用して更新をインポートおよびインストールできます。
  - **scp import pan-url-db remote-port <*port-number*> from username@host:path**
  - **request pan-url-db upgrade install file <*filename*>**

STEP 6 | PAN-DB プライベート クラウドへの管理アクセスをセットアップします。

アプライアンスにはデフォルトの ***admin*** アカウントがあります。追加の管理ユーザーを作成して、フル アクセス権または読み取り専用アクセス権を持つスーパーユーザーにすることができます。

PAN-DB プライベート クラウドは、*RADIUS VSA* の使用をサポートしていません。*VSA* がファイアウォールまたは *Panorama* で *PAN-DB* プライベート クラウドへのアクセスを有効にするために使用されると、認証エラーが発生します。

- PAN-DBサーバにローカル管理ユーザを設定するには、次のコマンドを使用します。
  1. 設定する
  2. **set mgt-config users <*username*> permissions role-based <superreader | superuser> yes**
  3. **set mgt-config users <*username*> password**
  4. パスワードを以下の通り入力します：**xxxxx**
  5. パスワードを確認：**xxxxx**
  6. **commit**
- RADIUS認証を使用する管理ユーザを設定するには、次のコマンドを使用します。
  1. RADIUS サーバ プロファイルを作成する場合：**set shared server-profile radius <*server_profile_name*> server <*server_name*> ip-address <*ip_address*> port <*port_no*> secret <*shared_password*>**。
  2. 認証プロファイルを作成する場合：**set shared authentication-profile <*auth_profile_name*> user-domain <*domain_name_for_authentication*> allow-list <all> method radius server-profile <*server_profile_name*>**.
  3. 認証プロファイルをユーザにアタッチする場合：**set mgt-config users <*username*> authentication-profile <*auth_profile_name*>**。
  4. 変更をコミットする場合： **commit**。
- ユーザのリストを表示するには、 **show mgt-config users** コマンドを使用します。

STEP 7 | PAN-DB プライベート クラウド にアクセスするようにファイアウォールを設定します。

PAN-DBプライベート クラウドにアクセスするためのファイアウォールの設定

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス）

どこで使用できますか?	何が必要ですか?
	注: レガシーURLフィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

PAN-DB パブリック クラウドを使用するとき、各ファイアウォールは AWS クラウドの PAN-DB サーバーにアクセスし、URL 検索のために接続可能な適格なサーバーのリストをダウンロードします。PAN-DB プライベート クラウドでは、URL 検索に使用する PAN-DB プライベート クラウド サーバーの（スタティック）リストを使用してファイアウォールを設定する必要があります。リストには最大 20 個のエントリを含めることができます。IPv4 アドレス、IPv6 アドレス、および FQDN がサポートされています。リストの各エントリ（IP アドレスまたは FQDN）は、PAN-DB サーバーの管理ポートまたはeth1に割り当てる必要があります。

STEP 1 | PAN-OS CLI から、URL ルックアップに使用される静的 PAN-DB プライベート クラウド サーバのリストを追加します。

- プライベートPAN-DBサーバーの IP アドレスを追加するには、次のCLIコマンドを使用します。

```
> configure
```

```
# set deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

または、各ファイアウォールのWebインターフェイスで、**[Device (デバイス)]** > **[Setup (設定)]** > **[Content-ID (コンテンツID)]**を選択し、[URL Filtering (URLフィルタリング)] セクションを編集して、PAN-DBサーバーのIPアドレスまたはFQDNを入力します。リストはカンマで区切る必要があります。

- プライベート PAN-DB サーバのエントリを削除するには、次のCLIコマンドを使用します。

```
# delete deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

プライベートPAN-DBサーバーのリストを削除すると、ファイアウォールで再選択プロセスがトリガーされます。ファイアウォールは最初に PAN-DB プライベート クラウド サーバーのリストがあるかチェックし、リストがない場合は、AWS クラウドの PAN-DB サーバーにアクセスして接続可能な適格なサーバーのリストをダウンロードします。

STEP 2 | **#** コミット を入力して、変更を保存します。

STEP 3 | 変更が有効になっていることを確認するには、ファイアウォールで以下の CLI コマンドを使用します。

```
> show url-cloud status Cloud status:Up URL database
 version:20150417-220
```


PAN-DB プライベート クラウド上のカスタム証明書による認証の設定

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama)	☐ 高度なURLフィルタリングライセンス（またはレガシーURLフィルタリングライセンス） 注: レガシー*URL*フィルタリングライセンスは廃止されましたが、アクティブなレガシーライセンスは引き続きサポートされます。

デフォルトでは、PAN-DBサーバーは管理アクセスおよびデバイス間通信に使用されるSSL接続を確立するための相互認証に事前定義済みの証明書を使用します。ただし、代わりにカスタム証明書を使用して認証を設定することもできます。カスタム証明書を使用すると、PAN-DBサーバーとファイアウォール間の相互認証を確実にするための信頼関係を確立することができます。PAN-DB プライベート クラウドの場合、ファイアウォールはクライアントとして動作し、PAN-DB サーバーは該当のサーバーとして動作します。

STEP 1 | PAN-DB サーバーとファイアウォールのキーペアと認証局（CA）証明書を取得します。

STEP 2 | CA 証明書をインポートして、ファイアウォールの証明書を検証します。

1. PAN-DB サーバー上で CLI にログインし、設定モードを開始します。

```
admin@M-600> configure
```

2. TFTP または SCP を使用して CA 証明書をインポートします。

```
admin@M-600# {tftp | scp} import certificate from <value>
 file <value> remote-port <1-65535> source-ip <ip/netmask>
 certificate-name <value> passphrase <value> format {pkcs12 |
 pem}
```

STEP 3 | TFTPまたはSCPを使用して、プライベートクラウド アプライアンスのサーバー証明書と秘密鍵を含むキーペアをインポートします。

```
admin@M-600# {tftp | scp} import keypair from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```

STEP 4 | ルート CA および中間 CA が含まれる証明書プロファイルを設定します。この証明書プロファイルは、PAN-DB サーバーとファイアウォール間のデバイス認証を定義します。

1. PAN-DB サーバーの CLI で、設定モードを開始します。

```
admin@M-600> configure
```

2. 証明書プロファイルに名前を付けます。

```
admin@M-600# set shared certificate-profile <name>
```

3. （省略可能）ユーザー ドメインを設定します。

```
admin@M-600# set shared certificate-profile <name>
 domain <value>
```

4. CA を設定します。

   Default-ocsp-url と ***ocsp-verify-cert*** は任意のパラメータです。

admin@M-600# **set shared certificate-profile <*name*> CA <*name*>**

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [default-ocsp-url <value>]
```

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [ocsp-verify-cert <value>]
```

STEP 5 | アプライアンスのSSL/TLSサービスプロファイルを設定します。このプロファイルは、PAN-DB およびクライアント デバイスが SSL/TLS サービスに使用する証明書およびプロトコルの範囲を定義します。

1. SSL/TLSサービスプロファイルを指定します。

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. 証明書を選択します。

```
admin@M-600# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. SSL/TLS 範囲を定義します。

   *PAN-OS 8.0*以降のリリースでは、*TLSv1.2* 以降の*TLS*バージョンのみがサポートされています。最大バージョンを ***TLS 1.2*** または ***max***（最大）に設定する必要があります。

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 | max
```

STEP 6 | PAN-DB 上の安全なサーバー通信を設定します。

1. SSL/TLSサービスプロファイルを設定します。このプロファイルは、PAN-DBとファイアウォール間のすべてのSSL接続に適用されます。

```
admin@M-600# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. 証明書プロファイルを設定します。

```
admin@M-600# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

3. [Disconnect Wait Time（切断待機時間）]を設定します。PAN-DBがファイアウォールとの接続を切断して再確立するまでの待機時間（分単位）です（範囲は0～44,640）。

```
admin@M-600# set deviceconfig setting management secure-conn-
server disconnect-wait-time <0-44640>
```

STEP 7 | CA証明書をインポートしてアプライアンスの証明書を検証します。

1. ファイアウォール インターフェイスにログインします。
2. 証明書をインポートします。

STEP 8 | ファイアウォールのローカル証明書または SCEP 証明書を設定します。

1. ローカル証明書を設定している場合は、ファイアウォールのキーペアをインポートします。
2. SCEP証明書を設定する場合は、SCEPプロファイルを設定します。

STEP 9 | ファイアウォールの証明書プロファイルを設定します。これを各ファイアウォールで個別に設定することも、Panorama の設定をテンプレートの一部としてファイアウォールにプッシュすることもできます。

1. ファイアウォールの場合は **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）を選択し、また、Panorama の場合は **Panorama** > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）を選択します。
2. 証明書プロファイルの設定を行います。

STEP 10 | 各ファイアウォールにカスタム証明書をデプロイします。Panorama から一元的に証明書をデプロイすることも、各ファイアウォールに手動で証明書を設定することもできます。

1. ファイアウォール インターフェイスにログインします。
2. ファイアウォールの場合は **Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理）を、Panorama の場合は **Panorama** > **Setup**（セットアップ） > **Management**（管理）を選択し、セキュア通信設定を **Edit**（編集）します。
3. **Certificate Type**（証明書タイプ）、**Certificate**（証明書）、および **Certificate Profile**（証明書プロファイル）をそれぞれのドロップダウンリストから選択します。
4. 通信のカスタマイズ設定内で、**PAN-DB Communication**（**PAN-DB** 通信）を選択します。
5. **OK** をクリックします。
6. 変更を **Commit (コミット)** します。

   変更をコミットした後、ファイアウォールは、**[Disconnect Wait Time**（切断待ち時間）]の経過後までPAN-DB サーバーとの現在のセッションを終了しません。次のステップでカスタム証明書の使用を強制すると、切断待機時間がカウントダウンを開始します。

STEP 11 | カスタム証明書認証を適用します。

1. PAN-DB サーバー上で CLI にログインし、設定モードを開始します。

   ```
   admin@M-600> configure
   ```

2. カスタム証明書の使用を適用します。

   ```
   admin@M-600# set deviceconfig setting management secure-conn-
   server disable-pre-defined-cert yes
   ```

この変更のコミット後は、切断待機時間のカウントダウンが開始します（PAN-DBの設定で構成した場合)。待機時間が終了すると、PAN-DB とそのファイアウォールは、設定された証明書だけを使用して接続します。

STEP 12 | 新しいファイアウォールまたは Panorama を PAN-DB プライベート クラウドのでプロイに追加する場合は、2 つの選択肢があります。

- **Custom Certificates Only**（カスタム証明書のみ）を有効にしていない場合は、新しいファイアウォールをPAN-DBプライベート クラウドに追加し、カスタム証明書をデプロイできます。
- PAN-DBプライベート クラウドで**[Custom Certificate Only**（カスタム証明書のみ）**]**を有効にした場合、カスタム証明書をPAN-DBプライベート クラウドに接続する前に、ファイアウォールにカスタム証明書をデプロイする必要があります。

