URL Filtering

機械学習を活用し、フィッシング、認証情報の不正使用、コマンド アンド コントロールを阻止

悪意のある Web ページにより、フィッシングや認証情報の盗難、マルウェア感染、ランサムウェアなどの危険に従業員がさらされます。攻撃者は自動化を利用して、数千もの悪意のある新しい URL を毎日動的に生成するため、スタンドアロン プロキシや Web フィルタリング ツールなどの従来の保護では、その数に圧倒され、単純に対応しきれなくなっています。悪意のある Web サイトを特定、分類、防御する間に、感染が広く拡散し、組織全体がリスクにさらされる可能性があります。ポイント製品が残りのセキュリティ スタックと統合していない場合、管理すべきポリシー セットが多くなることを意味するため、新しいビジネス アプリケーションの採用が遅れると同時に、維持するためのリソースが余計に必要になる可能性があります。

ビジネス上のメリット

- **セキュリティ サイロを解消し、ユーザーの安全を確保。** 機械学習 (ML) を活用した NGFW のネイティブなコンポーネントとして、URL Filtering はクラス最高の Web セキュリティをキャンパス、支社、モバイル ユーザーに、または所在地に関係なく提供し、管理が難しい従来のソリューションをなくします。
- **運用コストを最小化。** 既存のネットワーク トラフィック ポリシーに直接導入されるため、URL Filtering 機能は、ルール セットを簡素化し、セキュリティ チームの管理を合理化します。
- **新しい悪意のあるサイトをブロック。** URL Filtering は、ネットワークやエンド ユーザーが感染する前に、未知の悪意のある URL を即座に分類し、ブロックします。
- **既知の悪意のある Web サイトを防御。** フィッシング、マルウェア、エクスプロイト キット、コマンド アンド コントロール (C2) などの、既知の Web ベースの脅威から組織を保護します。
- **フィッシングから保護。** リアル タイムで認証情報フィッシングを阻止できるため、防御層が既知や未知のフィッシング サイトから組織を保護します。
- **法令コンプライアンスと利用規定に対応。** 組織が社内、業界、および政府の規制方針を継続的に遵守できるようにします。

統合保護機能を通じた安全な Web アクセス

安全な Web アクセスを実現するには、ML を活用した次世代ファイアウォール (NGFW) ポリシーを拡張するネイティブに統合されたアプローチに加え、脅威を自動的に検出、防御、制御する、設定が容易な Web コントロールが必要です。Web サイトをホワイトリストやブラックリストに単に登録するだけでなく、パロアルトネットワークスの URL Filtering は、機械学習を利用して、新しい未知の攻撃をインラインで特定して防御し、ユーザーがアクセスできるようになる前に脅威をブロックします。

このサービスは URL を分析し、無害なカテゴリと悪意のあるカテゴリに分類するので、ML を活用した NGFW ポリシーに簡単に組み込んで Web トラフィック全体を制御することができます。これらのカテゴリは、ファイアウォール プラットフォーム全体に対して補完機能をもたらすため、対象を絞った SSL 復号化や高度なロギングなどの、追加の防御層が提供されます。独自の分析に加え、URL Filtering では、WildFire® マルウェア防御サービスやその他のソースが共有する脅威情報を使用し、悪意のあるサイトに対する防御を自動的に更新します。

主な機能

機械学習を活用した検出

URL Filtering サブスクリプションは、ユーザーがアクセスできるようになる前に新たな脅威を阻止します。ML を活用した NGFW に機械学習を直接組み込むことで、未知のフィッシングや JavaScript 攻撃をインラインで阻止し、組織に広がるのを防ぎます。悪意のある URL が組織に感染する機会を得る前に、それらを瞬時に特定し、防御します。

Web コンテンツの完全な制御

Web ポリシーは、ファイアウォール ポリシーの単なる拡張です。ML を活用した NGFW は URL Filtering を使用して、URL カテゴリを特定し、リスク レーティングを割り当て、一貫したポリシーを適用します。複数の URL カテゴリとリスク レーティングを微妙に異なるポリシー内で組み合わせることで、正確な例外ベースの適用、管理の簡素化、単一のポリシー テーブルを通じた Web トラフィックのきめ細やかな制御を可能にします。フィッシング攻撃やエクスプロイト キットの配信、C2 に利用される可能性のある、危険なサイトをブロックできます。それでもなお、従業員は、ビジネスの目的のために必要な Web リソースに自由にアクセスすることができます。

選択的な Web トラフィックの復号化

対象を絞った復号化は、リスクの一層の緩和に役立ちます。TLS/SSL で暗号化された Web トラフィックを選択的に復号化するポリシーを確立すると、データ プライバシーに関する法規制に準拠しながら、潜在的な脅威への可視性を最大限に向上させることができます。ソーシャル ネットワーキング、Web ベースの電子メール、コンテンツ配信ネットワークなど、特定の URL カテゴリの復号化を指定しながら、行政機関、金融機関、医療機関向けのサイトなど、その他のタイプのサイトを行き来するトランザクションについては、暗号化を維持するよう指定できます。高または中にリスク レーティングされた、該当のコンテンツ カテゴリに対し、復号化を可能にするシンプルなポリシーを実装できます。選択的な復号化を使用することで、企業ポリシーまたは社外規制で設定した機密トラフィック パラメータを遵守しながら、最適なセキュリティ対策を実現できます。

認証情報フィッシングの防御

ユーザーのログインとパスワードをリアル タイムで保護します。URL Filtering は、認証情報をフィッシングする可能性のあるページを分析し、それらを「フィッシング」の URL カテゴリに照らし合わせることで確実に特定して阻止します。業界初として、URL Filtering は、サイトの URL カテゴリに基づいて、ユーザーが企業の認証情報を送信できるサイトを誤検知なしで制御することにより、進行中のフィッシング攻撃を検出して防御し、認証の盗難を防ぎます。これにより、ユーザーが認証情報を、信頼されていないサイトに送信するのを阻止しながらも、企業のサイトや承認されているサイトに送信できるようになります。

カスタマイズ可能なカテゴリ

カテゴリとポリシーを組織のニーズに合わせてカスタマイズします。URL Filtering は定義された一連のカテゴリを活用しますが、組織によって、リスク許容度やコンプライアンス、規制、利用規定に関するニーズは異なる可能性があります。組織の要件を満たし、セキュリティ ポリシーをきめ細かく調整するため、管理者は、複数の既存のカテゴリを組み合わせて新しいカテゴリを作成することにより、カスタムなカテゴリを確立できます。たとえば、「高リスク」、「金融サービス」、「新しく登録されたドメイン」カテゴリを組み合わせると、強力なカテゴリが新たに生み出され、このような基準に見合うサイトに制定されるポリシーを有効化できます。

キャッシュされた結果の分析と翻訳サイトのフィルタリング

一般的なポリシー回避技法に対して厳密な制御を維持します。キャッシュされた結果や言語翻訳サイトなど、攻撃で一般的な回避技法を使用している場合でも、URL Filtering ポリシーを適用できます。このことを実現するため、以下を実行します。

- **検索エンジンでキャッシュされた結果に対する防御**：エンド ユーザーが Web 検索やインターネット アーカイブのキャッシュ済みの結果を表示しようとした場合に、そのキャッシュ済みの結果に URL Filtering ポリシーが適用されます。
- **翻訳サイト フィルタリング**：Google 翻訳などの言語翻訳 Web サイトでポリシーを迂回するために入力された URL に、URL Filtering ポリシーが適用されます。

セーフ サーチの適用

検索結果を厳格に制御するため、セーフ サーチを適用すると、ユーザーの検索結果に不適切なコンテンツが表示されないようにすることができます。この機能を有効にすると、最も厳格なセーフ サーチ オプションが設定されている Google、Yandex、Yahoo、Bing の検索のみが許可されるようになり、その他の検索をすべてブロックできます。

カスタマイズ可能なエンド ユーザー通知

ユーザーがアクセスしようとしている Web ページが、ポリシーおよび関連付けられた URL Filtering プロファイルに従ってブロックされている場合に、各組織には、そのことをユーザーに通知するためのさまざまな方法があります。管理者は、カスタム ブロック ページを使用して、ユーザーに違反について通知することができます。このページには、ユーザー名と IP アドレス、ユーザーがアクセスしようとしている URL、そのページの URL カテゴリに対する参照情報のほか、管理者からのカスタマイズされたメッセージが記載されます。Web アクティビティに関するある程度の所有権をユーザーに戻すために、管理者は、ユーザーが危険なページにアクセスしようとするときに次の 2 つの制御オプションを利用できます。

- **[Continue (コンティニュー)]** では、[Continue (コンティニュー)] ボタンのある、カスタマイズされた警告ページが表示されます。これにより、要求したサイトのリスクに関してユーザーを啓蒙する機会が開かれます。ユーザーがこのリスクを許容できる場合は、操作の続行を許可します。
- **[Override (オーバーライド)]** では、ポリシーの例外を作成して継続するために、ユーザーによる設定可能なパスワードの入力が必要になります。これにより、ユーザーは、管理者の承認を得て、危険性のあるサイトにアクセスすることができるようになります。

パロアルトネットワークスのセキュリティ サブスクリプションの能力

今日、サイバー攻撃は増加、高度化し、高度なテクニックを利用してネットワーク セキュリティ デバイスやツールを迂回しています。そのため、組織には、セキュリティ チームの負荷を増やすことなく、またはビジネスの生産性を妨げることなく、ネットワークを保護することが課されています。業界初の ML を活用した NGFW プラットフォームとシームレスに統合された、弊社のクラウド提供型のセキュリティ サブスクリプションは、インテリジェンスをまとめ、すべての攻撃ベクトルに対する保護を実現し、クラス最高の機能を提供しながら、さまざまなネットワーク セキュリティ ツールから生じる、それらが網羅する範囲のギャップを解消します。一貫したプラットフォーム体験をもたらす市場をリードする機能を利用して、最も高度で巧妙な脅威に対してさえも、組織を保護します。URL Filtering やその他の弊社のセキュリティ サブスクリプションの利点は、次のとおりです。

- **Threat Prevention**: 従来の侵入防御システム (IPS) ソリューションを超え、シングル パスで、すべてのトラフィックについて既知のすべての脅威を自動的に防御します。
- **WildFire**: 業界をリードするクラウドベースの分析により、未知のマルウェアを自動的に検出し、防御することにより、ファイルの安全性を確保します。
- **DNS セキュリティ**: インフラストラクチャへの変更を必要とせずに、C2 やデータ窃盗に DNS を使用する攻撃を遮断します。
- **IoT セキュリティ**: 業界初のターンキー Internet of Things(IoT) セキュリティ ソリューションを使用して、組織全体の IoT および OT デバイスを保護します。
- エンドポイント向け **GlobalProtect**™ ネットワーク セキュリティ: ML を活用した NGFW 機能をリモート ユーザーに拡張し、環境内のあらゆる場所で一貫したセキュリティを提供します。

運用上のメリット

URL Filtering サブスクリプションでは、以下が可能です。

- **共有インテリジェンスの恩恵を享受**。使用が容易なアプリケーションベースのポリシーとユーザーベースのポリシーを備えたクラス最高の Web セキュリティを利用し、Threat Prevention や WildFire と緊密に統合します。
- **Web トラフィックに対する完全な制御を維持**。URL カテゴリを使用して、疑わしいサイトに対する選択的な TLS/SSL 復号化などの高度なセキュリティ アクションを自動的にトリガーします。
- **セキュリティを自動化**。アナリストの介入を必要とせずに、ポリシーを URL カテゴリに自動的に適用します。
- **ユーザーおよび URL アクティビティに対する洞察を獲得**。IT 部門は、一連の事前定義された URL Filtering レポートまたは完全にカスタマイズされた URL Filtering レポートにより、URL Filtering および関連する Web アクティビティに対する可視性を確保できます。

表 1: URL カテゴリに基づくポリシーの作成 *

ポリシー	説明
選択的な SSL	URL カテゴリに基づき、SSL 復号化を開始
認証情報の盗難	企業の認証情報を受信できるサイトを規定し、ユーザーが未認証のサイトに認証情報を送信するのをブロック、許可、警告
高リスクのファイル タイプをブロック	実行可能ファイルまたは潜在的に危険なファイル タイプのアップロードとダウンロードを阻止
より厳密な IPS プロファイル	特定の URL カテゴリに対して厳格な脆弱性プロファイルとアンチスパイウェア プロファイルを自動的に採用し、フィッシング キット、エクスプロイト キット、サーバ側およびクライアント側の脆弱性をブロック
ユーザー ベースのポリシー	組織内の特定のグループに特定の URL カテゴリへのアクセスを許可しながら、他のグループのそれらのカテゴリへのアクセスをブロック

* 単に有害なサイトをブロックするに留まらず、URL カテゴリは、きめ細かなセキュリティ ポリシーを可能にして、ビジネスを遅延させることなくユーザーを保護するために利用できます。

表 2: プライバシーとライセンスの概要	
URL Filtering サブスクリプションでのプライバシー	
信頼とプライバシー	パロアルトネットワークスでは、厳格なプライバシー制御とセキュリティ制御を適用しており、機密情報や個人を特定できる情報への不正アクセスを防いでいます。セキュリティや機密については、業界標準のベスト プラクティスを適用しています。詳細については、プライバシー データシートを参照してください。
ライセンスと要件	
要件	パロアルトネットワークスの URL Filtering サブスクリプションを使用するには、以下が必要です。 • PAN-OS 8.1 以降を実行しているパロアルトネットワークスの次世代ファイアウォール • パロアルトネットワークスの Threat Prevention ライセンス
推奨環境	フィッシング、認証情報の盗難、C2 などの脅威は外部との接続が必要なため、パロアルトネットワークスの次世代ファイアウォールをインターネットに面する場所に導入します。
URL Filtering ライセンス	URL Filtering には、パロアルトネットワークスの次世代ファイアウォール用のクラウドベースの統合サブスクリプションとして配信される、スタンドアロンのライセンスが必要です。また、パロアルトネットワークスのサブスクリプション ELA、VM-Series ELA、または Prisma Access の一部としても提供されます。

〒 100-0011
東京都千代田区内幸町 2 丁目 1 番 6 号
日比谷パークフロント 15 階
電話番号 : 03-6205-8061
www.paloaltonetworks.jp

url-filtering-ds-061020