H3C SecPath ファイアウォール製品
技術紹介

文書バージョン:6W402-20220223

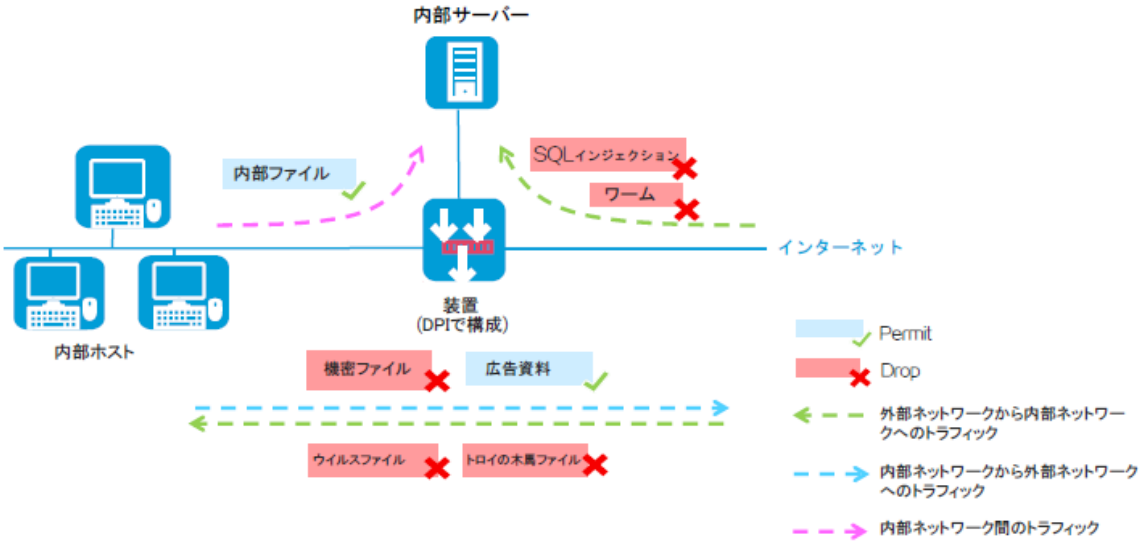
空白ページ

技術紹介

Deep Packet Inspection (DPI) 概要

DPIについて

ディープパケットインスペクション（DPI）は、アプリケーション層のトラフィックを検査および制御します。ウイルス対策、アプリケーションの監査と管理、およびその他のサービスをサポートして、外部からの攻撃をブロックし、内部データの漏洩を防ぎ、ユーザーのオンライン動作を規制し、ネットワークセキュリティを大幅に向上させます。

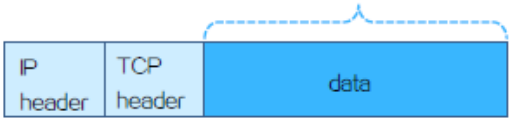


利点

通常の4層検査では、レイヤ2からレイヤ4までのパケットの内容のみが識別されますが、DPIは、レイヤ2からレイヤ4までのパケットの内容と、アプリケーション層のパケットの内容（HTTPデータなど）を識別します。したがって、DPIの結果はより具体的かつ正確になり、ユーザーのニーズをより適切に満たすことができます。

通常の4層検査

アプリケーション層の情報を識別できません。



検査結果：

Protocol: TCP
Port number: 80

DPI

アプリケーション層の情報を識別できます。

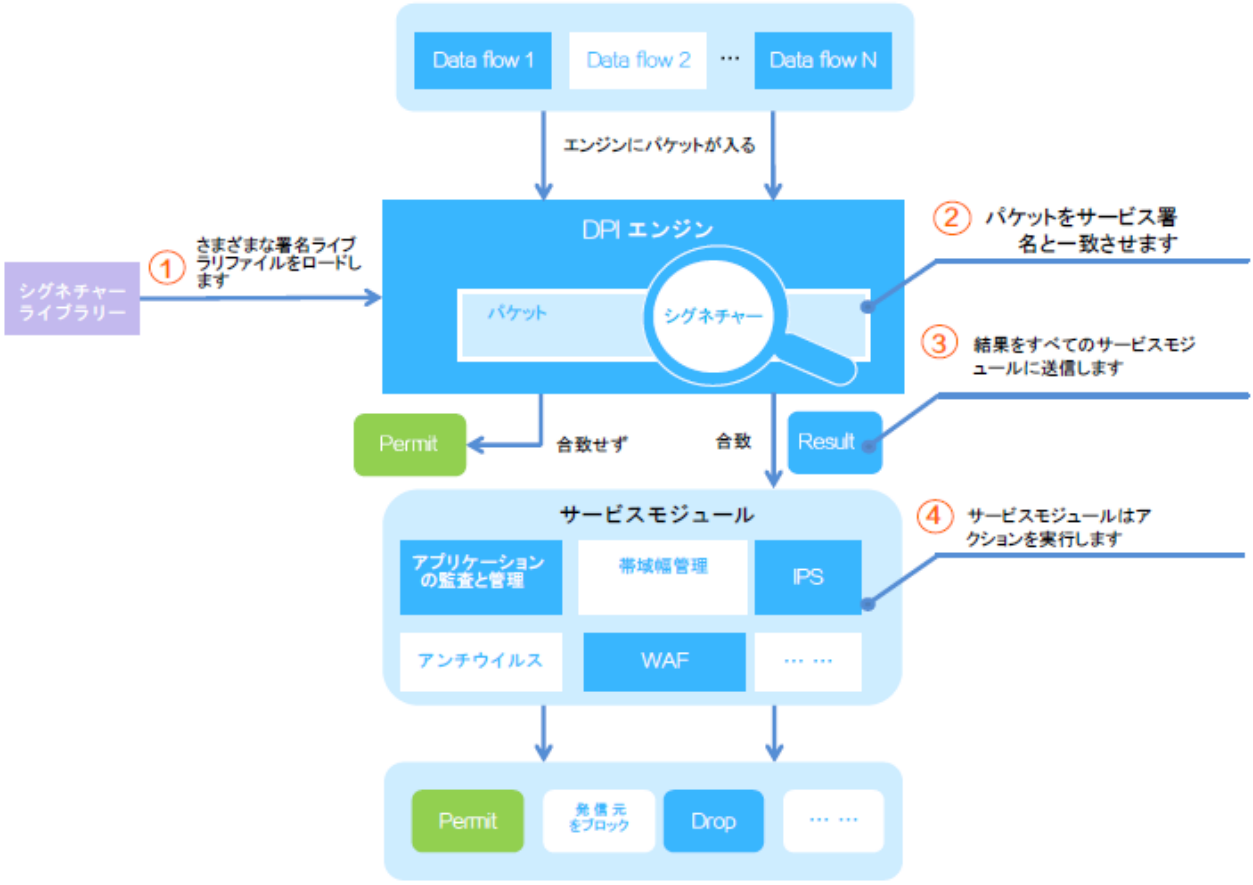
検査結果：

Protocol: TCP
Port number: 80
Application: Baidu
Behavior: Search
Behavior contents: Web games

仕組み

DPIは、DPIエンジンを使用してパケットシグニチャを識別します。

- DPIのコア処理ユニットとして、DPIエンジンはパケットプロトコルを解析し、パケットシグネチャを照合し、DPI結果をすべてのDPIサービスモジュールに送信します。
- プロの攻撃防御チームは、すべてのサービスパケットを分析して、サービス識別用の特定の形式でシグネチャを取得します。
- シグニチャライブラリは、サービスシグニチャのコレクションです。DPIエンジンでさまざまなサービスの署名ライブラリを簡単に使用するには、公式パスから署名ライブラリを取得して、デバイスにロードします。



DPI は以下のように動作します:

① このデバイスは、アンチウイルス署名ライブラリやIPS署名ライブラリなどのさまざまなサービスの署名ライブラリファイルをロードして、エンジンに豊富な署名を提供します。

② エンジンは、パケットをシグニチャと比較して、パケットの内容を識別します。

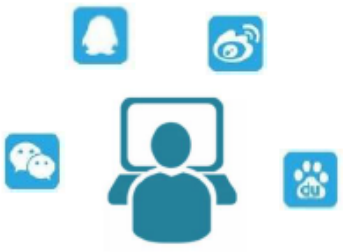
③ エンジンは検査結果を処理します。パケットが署名と一致する場合、デバイスは結果を対応するDPIサービスモジュールに送信します。パケットがどの署名とも一致しない場合、デバイスはDPI処理なしでパケットの通過を許可します。

④ 各サービスモジュールは、エンジンの検査結果に従ってパケットを処理します。

DPIサービス

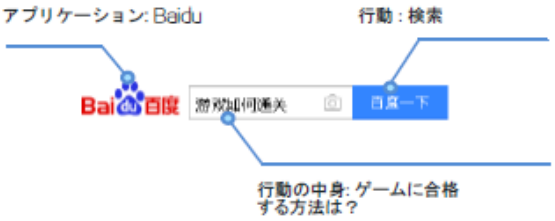
アプリケーションの認識

基本的なDPIサービスとして、アプリケーション認識（APR）は、署名を通じてアプリケーションを認識します。他のサービスは、APRの結果を使用してさらに処理することができます。



アプリケーションの監査と管理

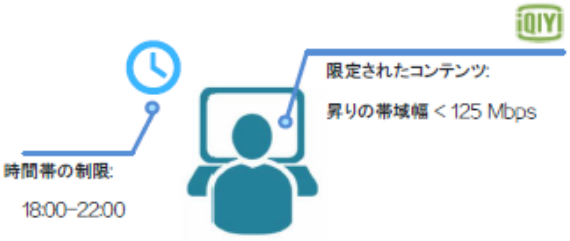
APRに基づいて、アプリケーションの監査と管理は、アプリケーションの動作と動作の内容を識別します。したがって、デバイスはユーザーのインターネットアクセス動作を監査および記録できます。



帯域幅管理

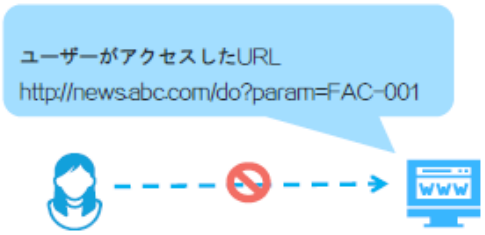
帯域幅管理は、次の情報を使用して、デバイスを流れるトラフィックをきめ細かく制御します：

セキュリティゾーン、ユーザー、APRによって認識されたアプリケーション、および時間範囲。



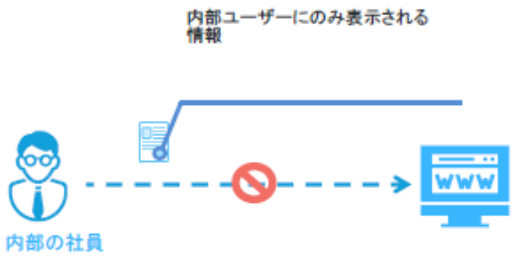
URLフィルタリング

URLフィルタリングは、ユーザーがアクセスするURLをフィルタリングすることにより、Webリソースへのアクセスを制御します。



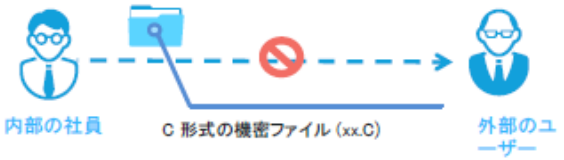
Data フィルタリング

データフィルタリングは、アプリケーション層の情報に基づいてパケットをフィルタリングします。データフィルタリングを使用して、企業の機密情報の漏洩を防ぎ、違法で機密性の高い情報の拡散を防ぐことができます。



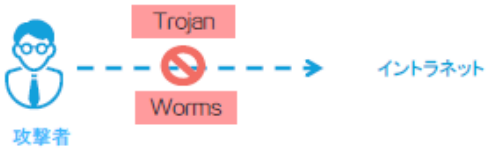
ファイルフィルタリング

ファイルフィルタリングは、ファイル拡張子に基づいてファイルをフィルタリングします。
ファイル拡張子に基づいてファイルに対してアクションを実行するようにファイルフィルタリングを構成できます。



IPS

侵入防止システム(IPS)は、デバイスがネットワークトラフィックの悪意のあるアクティビティを監視し、予防措置を講じることを可能にするセキュリティ機能です。



WAF

Webアプリケーションファイアウォール(WAF)は、Webサーバーを攻撃から保護します。デバイスは、Webアクセス要求を受信した後、要求されたコンテンツのセキュリティと合法性を検査および検証し、Webサーバーを効果的に保護するために、違法な要求をリアルタイムでブロックします。

アンチウィルス

アンチウイルスは、最新のウイルス署名ライブラリに基づいてパケットのアプリケーション層でウイルスを識別し、ネットワークが感染するのを防ぐためのアクションを実行します。 この機能は通常、内部ネットワークをウイルスから保護し、内部データを保護するためにゲートウェイに展開されます。

技術紹介

Deep Packet Inspection アンチウイルス

アンチウイルスについて

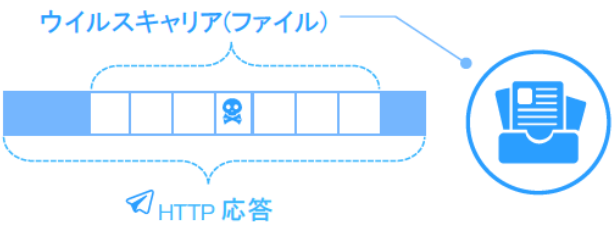
アンチウイルスは、パケットのアプリケーション層でウイルスを識別し、ネットワークが感染するのを防ぐためのアクションを実行します。このセキュリティメカニズムは通常、ウイルスの侵入を防ぎ、データのセキュリティを提供するために、企業ネットワークの境界に展開されます。

仕組み

アンチウイルスは、DPIエンジンとクラウドクエリを使用してファイル内のウイルスを検出し、アンチウイルスポリシーに従ってウイルスに感染したパケットに対してアクションを実行します。

ウイルスキャリアの識別

DPIエンジンは、最初にパケット内のウイルスに感染したファイルを識別します。通常、ウイルスは電子メールまたはファイル共有プロトコルを介して拡散します。パケットのアプリケーション層プロトコルを認識した後、DPIエンジンはさらにパケットを解析、デコード、およびセグメント化して、パケット内のファイルを識別します。たとえば、DPIエンジンは、ダウンロード用のHTTPパケット内のEXEファイルを識別できます。



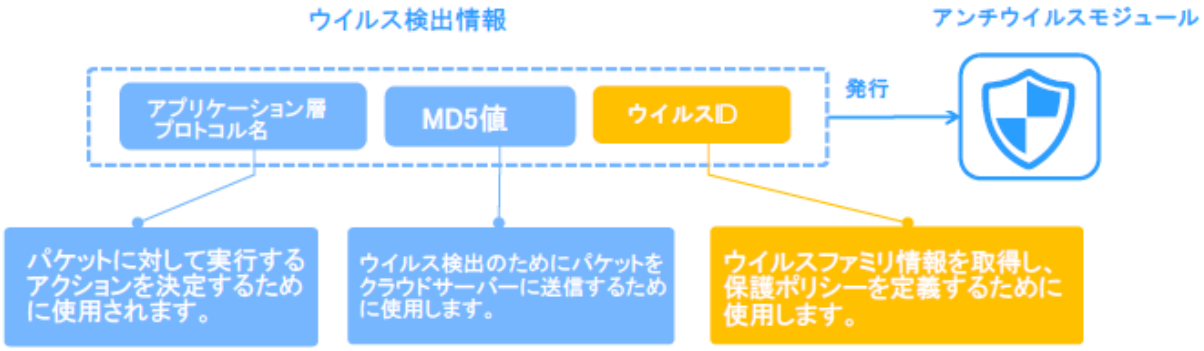
サポートされているプロトコルと検知方向		
プロトコルタイプ	プロトコル	検知方向
ファイル転送プロトコル	HTTP	Upload, download
	FTP	Upload, download
Emailプロトコル	SMTP	Upload
	POP3	Download
	IMAP	Upload, download
ファイル共有プロトコル	NFS	Upload, download
	SMB	Upload, download

ウイルス検知

ウイルスに感染したファイルを識別した後、DPIエンジンは、ファイルをウイルスシグネチャおよびウイルスシグネチャライブラリ内のMD5ルールと照合します。 ウイルスIDは、ウイルス署名またはMD5ルールを一意に識別します。 一致するものが見つかった場合、DPIエンジンはウイルスが検出されたと判断します。

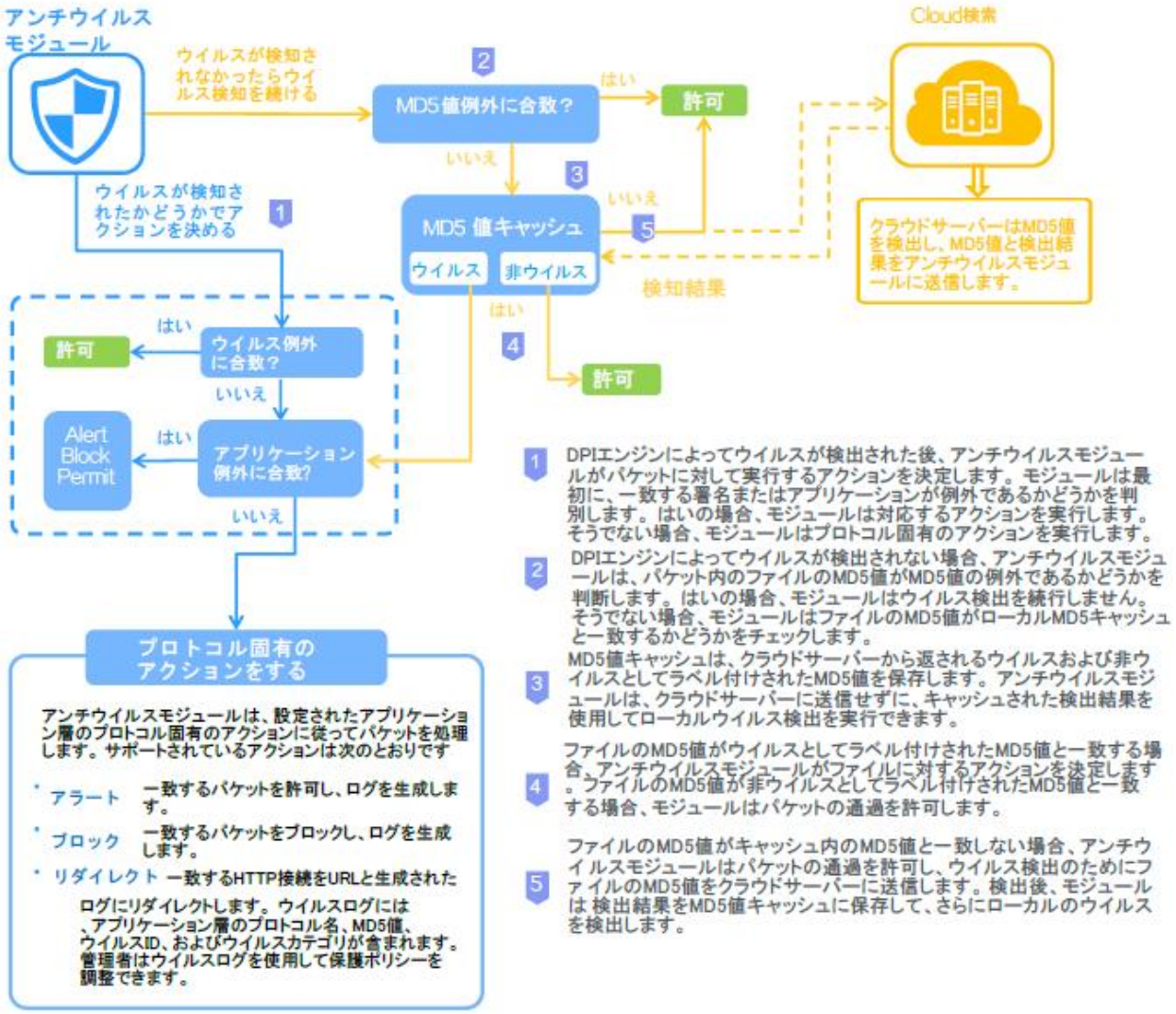
ウイルス検出情報の発行

ローカルウイルス検出が完了すると、DPIエンジンは検出情報をアンチウイルスモジュールに発行します。ウイルスが見つかった場合、DPIエンジンは、アプリケーション層のプロトコル名、MD5値、およびファイルのウイルスIDをアンチウイルスモジュールに発行します。ウイルスが見つからない場合、DPIエンジンは、ファイルのアプリケーション層プロトコル名とMD5値をアンチウイルスモジュールに発行して、ウイルスの検出とパケット処理をさらに進めます。



パケット処理

アンチウイルスモジュールは、DPIエンジンによって発行されたウイルス検出情報と、クラウドサーバーから返された検出結果に従ってパケットを処理します。ウイルスが見つかった場合、モジュールはパケットに対して実行するアクションを決定します。ウイルスが見つからない場合、モジュールはMD5値キャッシュを使用してウイルス検出を続行し、パケットに対して実行するアクションを決定します。



1 DPIエンジンによってウイルスが検出された後、アンチウイルスモジュールがパケットに対して実行するアクションを決定します。モジュールは最初に、一致する署名またはアプリケーションが例外であるかどうかを判別します。はいの場合、モジュールは対応するアクションを実行します。そうでない場合、モジュールはプロトコル固有のアクションを実行します。

2 DPIエンジンによってウイルスが検出されない場合、アンチウイルスモジュールは、パケット内のファイルのMD5値がMD5値の例外であるかどうかを判断します。はいの場合、モジュールはウイルス検出を続行しません。そうでない場合、モジュールはファイルのMD5値がローカルMD5キャッシュと一致するかどうかをチェックします。

3 MD5値キャッシュは、クラウドサーバーから返されるウイルスおよび非ウイルスとしてラベル付けされたMD5値を保存します。アンチウイルスモジュールは、クラウドサーバーに送信せずに、キャッシュされた検出結果を使用してローカルウイルス検出を実行できます。

4 ファイルのMD5値がウイルスとしてラベル付けされたMD5値と一致する場合、アンチウイルスモジュールがファイルに対するアクションを決定します。ファイルのMD5値が非ウイルスとしてラベル付けされたMD5値と一致する場合、モジュールはパケットの通過を許可します。

5 ファイルのMD5値がキャッシュ内のMD5値と一致しない場合、アンチウイルスモジュールはパケットの通過を許可し、ウイルス検出のためにファイルのMD5値をクラウドサーバーに送信します。検出後、モジュールは検出結果をMD5値キャッシュに保存して、さらにローカルのウイルスを検出します。

例外

ウイルス例外: ウイルスの誤警報であることが判明した場合、管理者はウイルス署名を特異な例外として設定できます。署名例外に一致するパケットの通過が許可されます。

アプリケーション例外: アプリケーションに対して別のアクションを実行するために、管理者はアプリケーションを例外として設定し、

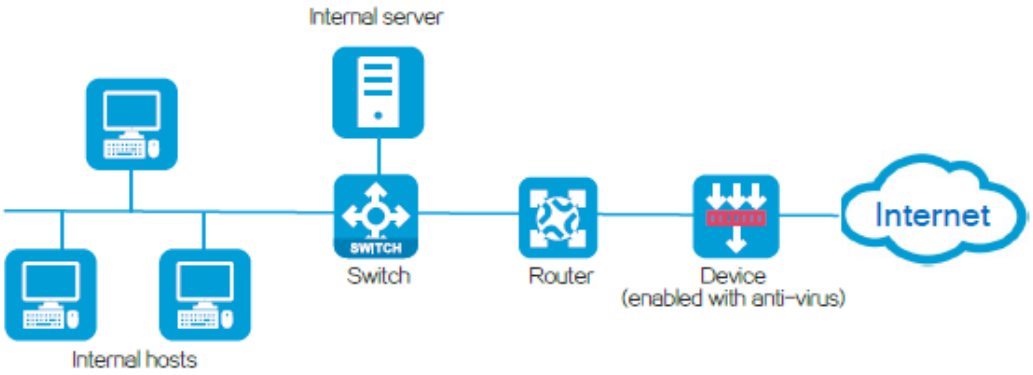
アプリケーションに対して別のアンチウイルスアクションを指定できます。アプリケーション例外はアプリケーション固有のアクションを使用し、他のアプリケーションはプロトコル固有のアクションを使用します。たとえば、HTTPのアンチウイルスアクションはアラートです。HTTPによって運ばれるゲームをブロックするには、ゲームをアプリケーションの受信として設定し、それらのブロックアクションを指定します。

MD5値例外: ウイルスの誤検知が発生した場合は、ウイルスのMD5値をMD5例外に設定できます。デバイスは、MD5値の例外に一致する後続のパケットの通過を許可します。

該当するシナリオ

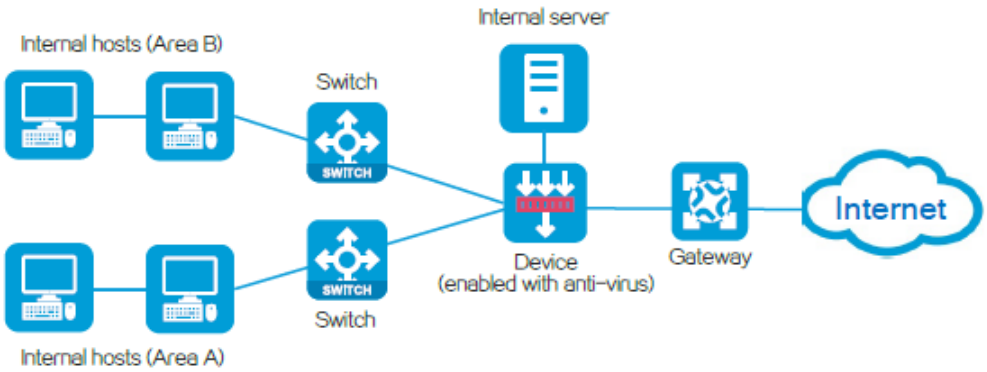
ウイルスの侵入を防ぐために境界に配備する

ネットワーク出力にデバイスを展開して、外部ネットワークからダウンロードされたファイルと内部サーバーにアップロードされたファイルをリアルタイムで検出します。したがって、デバイスは内部サーバーと内部ホストをウイルスから保護できます。



イントラネットに展開して、ウイルスの拡散を防ぎます

内部ネットワークのさまざまな領域の境界にデバイスを配置して、内部ホスト間または内部ホストと内部サーバー間で送信されるファイルをリアルタイムで検出します。したがって、デバイスはウイルスが内部ネットワークに広がるのを防ぐことができます。



ライセンス要件

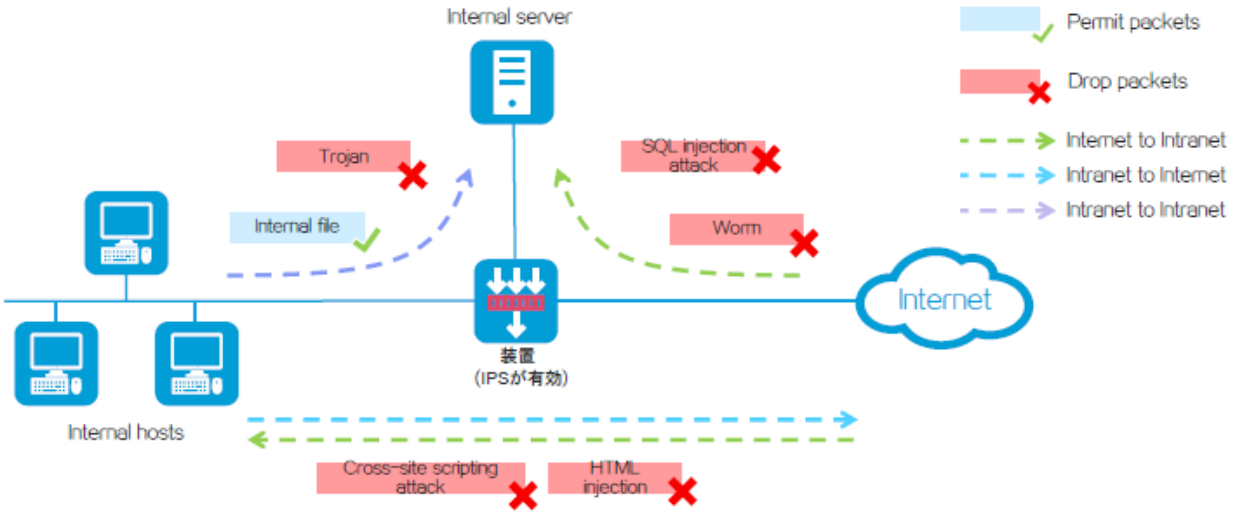
ウイルス対策機能を使用する前に、デバイスにライセンスを購入して正しくインストールしてください。ライセンスの有効期限が切れても、ウイルス対策機能は引き続き利用できますが、デバイスのウイルス署名ライブラリを更新することはできなくなります。

技術紹介

Deep Packet Inspection IPS

IPSについて

侵入防止システム(IPS)は、デバイスがネットワークトラフィックの悪意のあるアクティビティを監視し、予防措置を講じることを可能にするセキュリティ機能です。



IPSの仕組み

IPSは、DPIエンジンを使用して、アプリケーション層のトラフィックをリアルタイムで検査し、攻撃を検出して防止します。IPSは、IPSポリシーに基づいて実装されます。IPSポリシーには、パケットを照合するための一連のIPSシグニチャとパケットのアクションが含まれています。

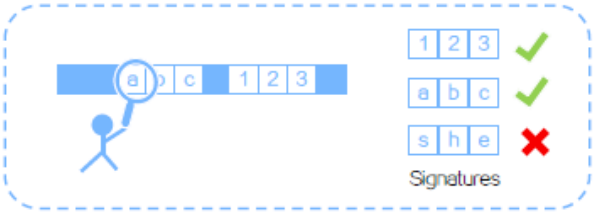
① IPSシグネチャーのロード

IPSシグニチャをデバイスにロードして、デバイスのIPSシグニチャを強化できます。デバイスは、次のタイプのIPSシグニチャをサポートします:

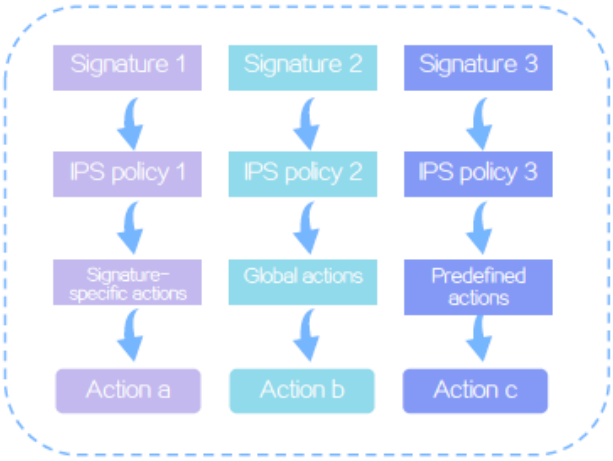
- 事前定義されたIPS署名：公式Webサイトから取得した署名ファイルをロードすることで更新できます。IPSシグニチャライブラリの自動更新をスケジュールしたり、IPSシグニチャの即時更新をトリガーしたり、IPSシグニチャの手動更新を実行したりできます。
- ユーザー定義のIPSシグニチャ：Snortファイルからインポートされたシグニチャと、手動で構成されたユーザー構成のシグニチャを含めます。

② IPSシグネチャーに合致

その後、IPSエンジンはパケットを解凍、再アセンブル、および解析し、パケットをIPSシグニチャと照合します。一致するシグニチャが見つかった場合、IPSエンジンは一致した結果をIPSモジュールに発行します。一致するシグニチャが見つからない場合、IPSエンジンパケットの通過を直接許可します。



③ アクションを選択



シグニチャの一致結果に応じて、IPSモジュールは一致するシグニチャが属するIPSポリシーを識別します。次に、モジュールは、一致するIPSポリシーのシグニチャのアクションを選択します。IPSポリシーでは、シグニチャに対して降順で次のアクションを実行できます:

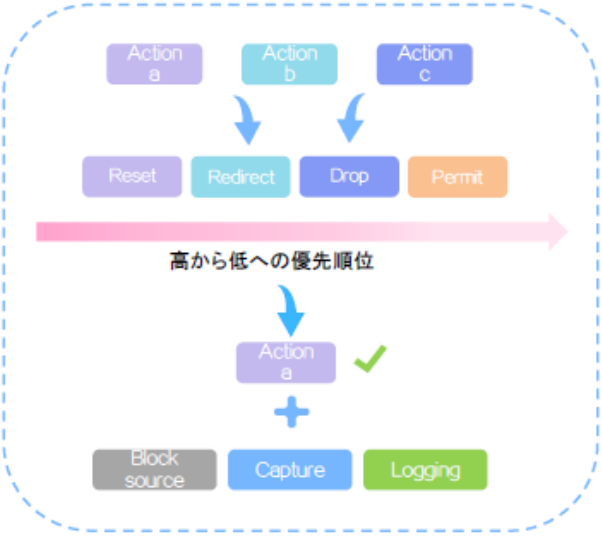
1. シグニチャに指定されたアクション。
2. すべての署名のグローバルアクション。
3. シグニチャの事前定義されたアクション。

④ 実行するアクションを決定します

IPSモジュールは、アクション選択の結果に従ってパケットに対してアクションを実行します。

- パケットが1つのIPSシグニチャのみに一致する場合、モジュールはそのシグニチャのアクションを実行します。
- パケットが複数のIPSシグニチャと一致する場合、モジュールは最も高い優先度のアクションを実行します。

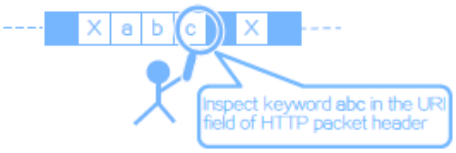
モジュールは、一致するIPSシグニチャにある場合、ブロックソース、キャプチャ、およびロギングアクションを実行します。



IPS利点

徹底的な保護

IPSは、パケット内のレイヤー2からレイヤー4の情報を検査できるだけでなく、アプリケーション層の情報（HTTPデータなど）を詳細に検査および分析して、潜在的な攻撃を発見することもできます。



豊富なリソースとタイムリーな更新を備えたIPSシグネチャーライブラリ

攻撃防御チームは、チームが最新の攻撃テクノロジーとトレンドをリアルタイムで取得した後、IPSシグニチャライブラリのシグニチャリソースを常に強化します。

チームは、公式Webサイトで最新のIPS署名ライブラリを定期的に公開しています。シグニチャライブラリには、主流のオペレーティングシステム、ネットワークデバイス、データベースシステム、アプリケーションシステムのすべての脆弱性シグニチャと、ワーム、ウイルス、トロイの木馬攻撃などの大規模なサイバー攻撃シグニチャが含まれています。

IPSシグネチャーライブラリ

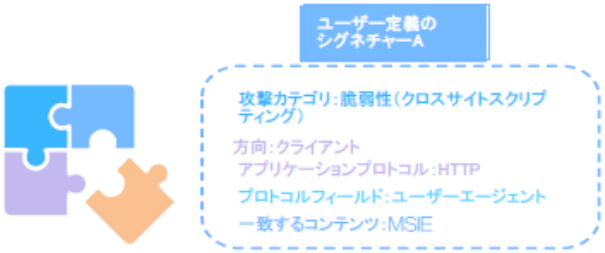
ライブラリを定期的に更新します（毎週）

24時間の緊急アップデート（重大なセキュリティの脆弱性が発見された場合）

IPSシグニチャを柔軟に定義する

さまざまな環境での多様な防御要件を満たすために、IPSはユーザー定義のIPSシグニチャをサポートしています。

ユーザーは、ネットワークの攻撃特性に応じてIPSシグニチャを定義できます。たとえば、ユーザーはIPSシグニチャを定義し、攻撃カテゴリ、攻撃アプリケーションプロトコル、およびIPSシグニチャのプロトコルフィールドを指定できます。

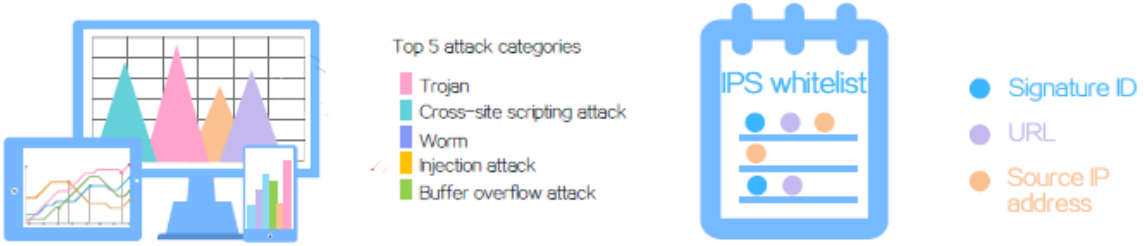


統計を視覚的に表示する

このデバイスは、IPSロギング、統計ランキング、攻撃傾向情報を視覚的に表示したり、表示された情報をレポートファイルにエクスポートしたりできます。これにより、ユーザーはネットワークセキュリティの状況を明確に把握し、防衛ポリシーを開発および調整するための強力なデータサポートを提供します。

誤警報を効果的に防止します

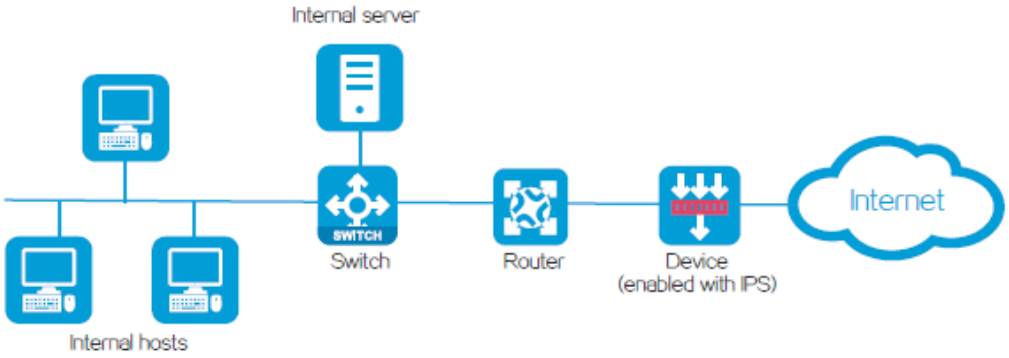
IPSログから誤ったアラームを見つけた場合は、ログ内の送信元IPアドレス、シグニチャID、およびURLをIPSホワイトリストに追加できます。デバイスは、IPSホワイトリストエントリに一致するすべてのパケットの通過を許可します。これにより、誤警報が減少します。



IPSアプリケーションシナリオ

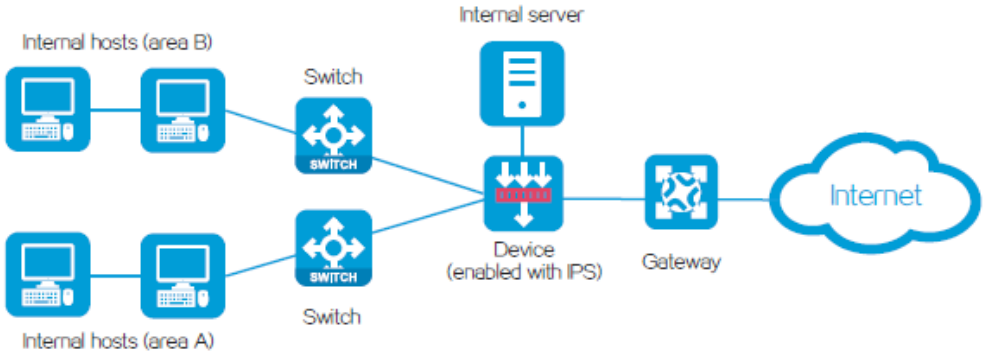
外部からの攻撃を防ぐために境界に配置します

内部サーバーとユーザーのセキュリティを保証するために、IPSが有効になっているデバイスを境界に配置して、トラフィックをリアルタイムで監視し、ハッキングトラフィックをブロックします。通常、IPSは、SQLインジェクション、クロスサイトスクリプティング攻撃、WebShellアップロード、WebLogic、Struts 2、Javaデシリアライズなどの攻撃を防ぐことができます。



イントラネットを保護するためにイントラネットに展開する

イントラネットでIPSが有効になっているデバイスを展開して、トラフィックをリアルタイムで監視し、異常なトラフィックをブロックします。このシナリオでは、IPSは内部サービスとホストのセキュリティを保証します。この機能は、内部サーバーの違法な外部接続をブロックし、内部の悪意のある攻撃からネットワークを防御し、侵入されたホストがイントラネット内で水平方向に広がるのを防ぐことができます。通常、IPSは、MS17-010、マイニングウイルス、イントラネットでの水平侵入攻撃などの攻撃を防ぐことができます。



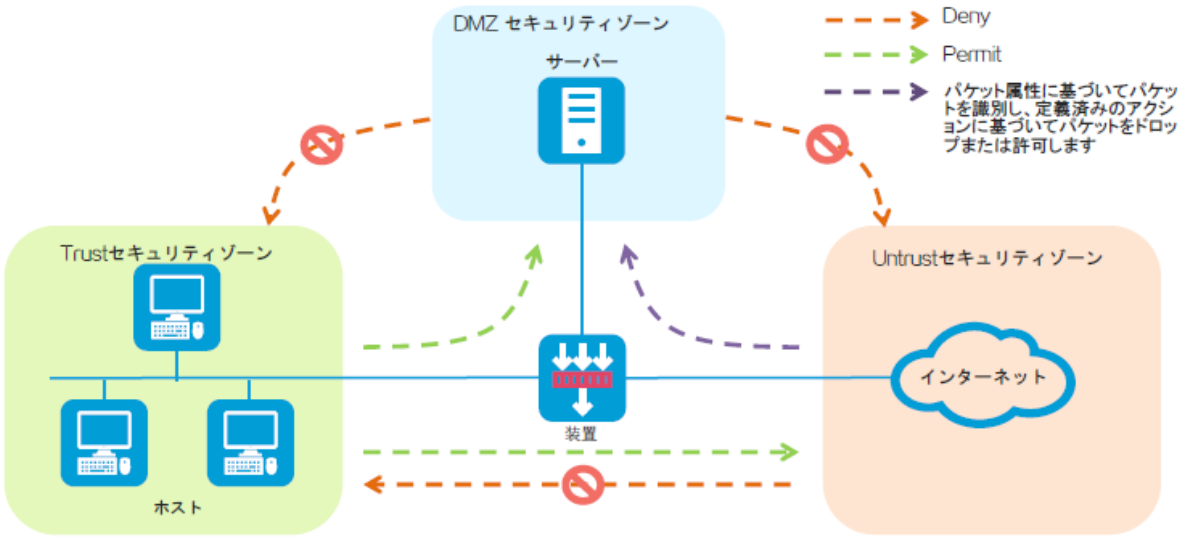
ライセンス要件

IPSモジュールをデバイスで実行するには、ライセンスが必要です。ライセンスの有効期限が切れても、IPS機能は引き続き使用できますが、デバイスのIPSシグニチャライブラリをアップグレードすることはできなくなります。

セキュリティポリシー

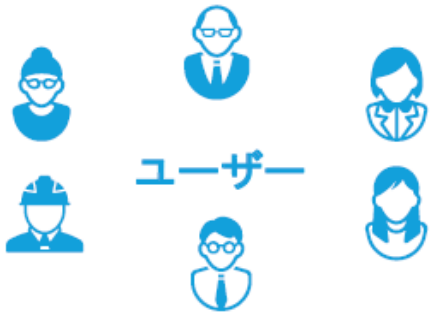
セキュリティポリシーについて

セキュリティ ポリシーは、属性ベースのパケット識別とフィルタリングを通じてパケット転送を制御できる、スマートなセキュリティ保護手段です。パケット識別、ディープ パケット インスペクション (DPI)、セキュリティ アクションの実行、スマート ポリシー分析、アプリケーション リスクベースの最適化など、複数のセキュリティ保護方法を組み合わせて、ネットワークに包括的な保護を提供します。



利点

セキュリティ ポリシーは、5 タプルだけでなく他のパケット属性にも基づいてパケットを識別し、正確なパケット制御を提供します。



ユーザー識別

セキュリティ ポリシーは、ユーザーの IP とアクセス場所が頻繁に変化する場合でも、アクセス ユーザーごとにパケットを正確に識別できます。

アプリケーション識別

セキュリティ ポリシーは、ビデオ、オーディオ、テキスト アプリケーションなど、何千ものアプリケーションのパケットを効果的に識別できます。

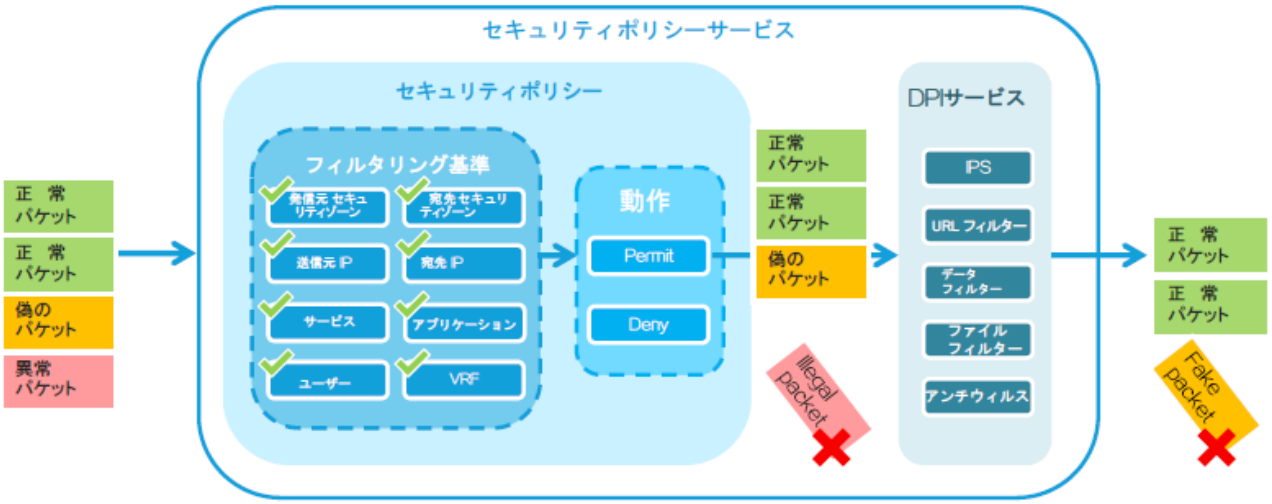
攻撃識別

DPI と連携することで、セキュリティ ポリシーはパケットの詳細な検査を実行して、ウイルスや侵入を防ぐことができます。

DNS によるホスト IP の自動取得

セキュリティ ポリシーは、DNS を通じてホストの IP アドレスを取得できます。これにより、ホストの IP アドレスが変更された場合でも、正しいホスト パケット識別が保証されます。

メカニズム



セキュリティ ポリシーは次のように動作します:

1. パケットを受信した後、デバイスはそのパケットを構成済みのセキュリティ ポリシーと照合します。
ポリシーのすべてのフィルタリング基準に一致する場合、パケットは一致したと見なされます。

- 一致するものが見つからない場合、デバイスはパケットを破棄します。
- 一致が見つかり、ポリシー アクションが**deny**の場合、デバイスはパケットを破棄します。
- 一致が見つかり、ポリシー アクションが**permit**の場合、デバイスは次のステップに進みます。

2. 一致したセキュリティ ポリシーに対して DPI サービスが構成されている場合、デバイスはパケットに対して詳細な検査を実行します。パケットに不正な特性が含まれている場合、デバイスはパケットをドロップします。不正な特性が見つからない場合、または DPI サービスが指定されていない場合、デバイスはパケットの通過を許可します。

スマートセキュリティポリシー

ポリシーの冗長性分析

この機能により、システムは既存のセキュリティ ポリシーのフィルタリング基準を比較し、ユーザーがそれらを削除するための冗長なポリシーを検出できます。

ポリシー名	フィルタリング基準	動作	冗長かどうか
Policy1	発信元 IP: 10.1.0.0/16	Permit	いいえ
Policy2	宛先 IP: 20.1.1.0/2	Deny	いいえ
Policy3	発信元 IP: 10.1.1.0/24	Permit	はい (最適化としてポリシーを削除する)
Policy4	宛先 IP: 30.1.1.0/24	Permit	いいえ

ポリシー一致分析

ポリシー 一致分析は、ユーザーがどのパケットとも一致しなかったセキュリティ ポリシーを見つけて分析し、セキュリティ ポリシー構成を最適化して、実際の状況により適切に対応するのに役立ちます。

ポリシーの最適化

- リスク分析

  この機能は、アプリケーション層検出エンジンを使用して、許可されたトラフィックのアプリケーション情報を分析します。 これにより、ユーザーは潜在的なリスクを発見し、防止策を講じることができます。

- ポリシーの最適化

  この機能は、リスク分析結果に基づいてポリシー最適化スキームを生成し、ユーザーがボタンをクリックしてリスクを削除できるようにします。

技術紹介

攻撃検知と防御

概要

重要なネットワーク セキュリティ機能として、攻撃の検出と防止により、デバイスは到着したパケットを検査することで攻撃を検出し、防止アクションを実行してプライベート ネットワークを保護できます。

攻撃の検出と防止により、シングル パケット攻撃、フラッド攻撃、およびスキャン攻撃を効果的に防御できます。

シングル パケット攻撃は、不正なパケット攻撃とも呼ばれます。攻撃者は通常、プロトコルに準拠していないパケットをデバイスに送信することにより、単一パケット攻撃を開始します。これにより、ターゲット システムが誤動作またはクラッシュします。

攻撃者は、短期間に大量の偽造リクエストを被害者に送信することにより、フラッド攻撃を開始します。
被害者は、正当なユーザーにサービスを提供するためにこれらの偽造された要求に対応するのに忙しく、DoS 攻撃が発生します。

攻撃者はスキャン ツールを使用して、ネットワークを調査し、脆弱なホストを見つけ、ホストで実行されているサービスを発見します。攻撃者はこの情報を使用して攻撃を仕掛けることができます。

利点

ユーザーの構成と管理を容易にするために、構成パラメーターが攻撃防止戦略に組み込まれています。

簡単な設定

インテリジェント閾値学習

リアルタイムのネットワーク トラフィックに応じて、攻撃防御のしきい値を適応的に調整して、攻撃検出の精度を向上させることができます。

さまざまな種類の攻撃防止データ統計を収集して、ユーザーがリアルタイムで攻撃防止状況を知ることができます。

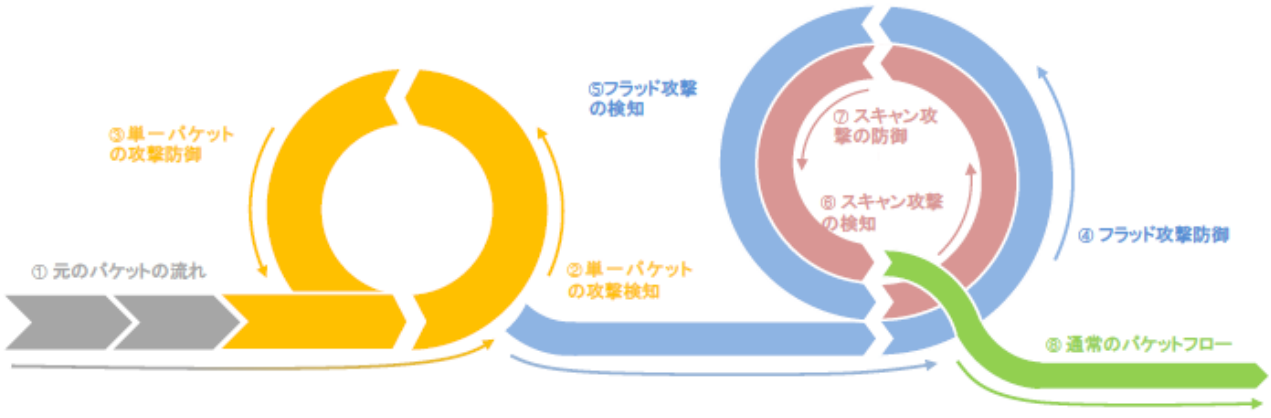
統計情報の表示

ウイルス攻撃防御

シングル パケット攻撃、フラッド攻撃、スキャン攻撃を効果的に防御できます。

処理手順

次の図に示すように、単一パケット攻撃の防御、フラッド攻撃の防御、およびスキャン攻撃の防御には、それぞれ独自の検出プロセスと防御プロセスがあります。



メカニズム

シングルパケット攻撃の検出

通常、単一パケットの攻撃者によって送信されたパケットには、署名が固定されています。パケットがシグニチャと一致する場合、デバイスは攻撃パケットを識別できます。

シングルパケット攻撃の防御

デバイスは、シングル パケット攻撃パケットをドロップし、シングル パケット攻撃ログを生成します。

- シングルパケット攻撃パケットをドロップします
- シングルパケット攻撃ログを生成します

デバイスは、次のタイプの単一パケット攻撃を検出して防止できます:

ICMPリダイレクト、ICMP到達不能、ICMPタイプ、ICMPv6タイプ、Land、Large ICMP、Large ICMPv6、IPオプション、IPオプション異常、フラグメント、インポッシブル、タイニーフラグメント、スマーフ、TCPフラグ、Traceroute、Winnuke、UDP Bomb、UDP Snork、UDP Fraggle、Teardrop、Ping of Death、および IPv6 ext-header。

フラッド攻撃の検出

デバイスは、IP アドレスから発信された、または IP アドレス宛てのパケットのレートがしきい値に達したときにフラッド攻撃が発生したと判断し、パケット レートがしきい値を下回ったときに攻撃が終了したと判断します。

フラッド攻撃防御

デバイスはパケットをドロップするかクライアント検証を実行し、フラッド攻撃ログを生成します。

クライアントの検証は、プロアクティブな防止機能です。Connect-Challenge-Respond メカニズムに基づいて、デバイスは主導的にパケット ソースの有効性を検証し、不正なクライアントからのパケットをドロップします。

- フラッド攻撃パケットを破棄する
- 攻撃元を検証する
- フラッド攻撃ログを生成する

デバイスは、次のタイプのフラッド攻撃を検出して防止できます。

SYN フラッド攻撃、ACK フラッド攻撃、SYN-ACK フラッド攻撃、FIN フラッド攻撃、RST フラッド攻撃、UDP フラッド攻撃、ICMP フラッド攻撃、ICMPv6 フラッド攻撃、DNS フラッド攻撃、DNS 応答フラッド攻撃、HTTP フラッド攻撃、SIP フラッド攻撃 .

スキャン攻撃の検出

このデバイスは、ネットワーク ユーザーによって開始されたターゲット システムへの接続速度を監視します。デバイスは、クライアントの宛先 IP または宛先ポートの変更頻度がしきい値を超えたことを検出すると、クライアントがスキャン攻撃を開始したと判断します。

スキャン攻撃防止

デバイスは、スキャン攻撃パケットをドロップするか、パケット ソースをブロックして、スキャン攻撃ログを生成します。

ヒント: デバイスがパケット ソースをブロックすると、そのソースからの後続のパケットがドロップされます。

- スキャン攻撃パケットを破棄する
- 攻撃パケット ソースをブロックします
- スキャン攻撃ログを生成します

このデバイスは、IP スイープ攻撃とポート スキャン攻撃を検出して防止できます

応用シナリオ

デバイスの自己保護

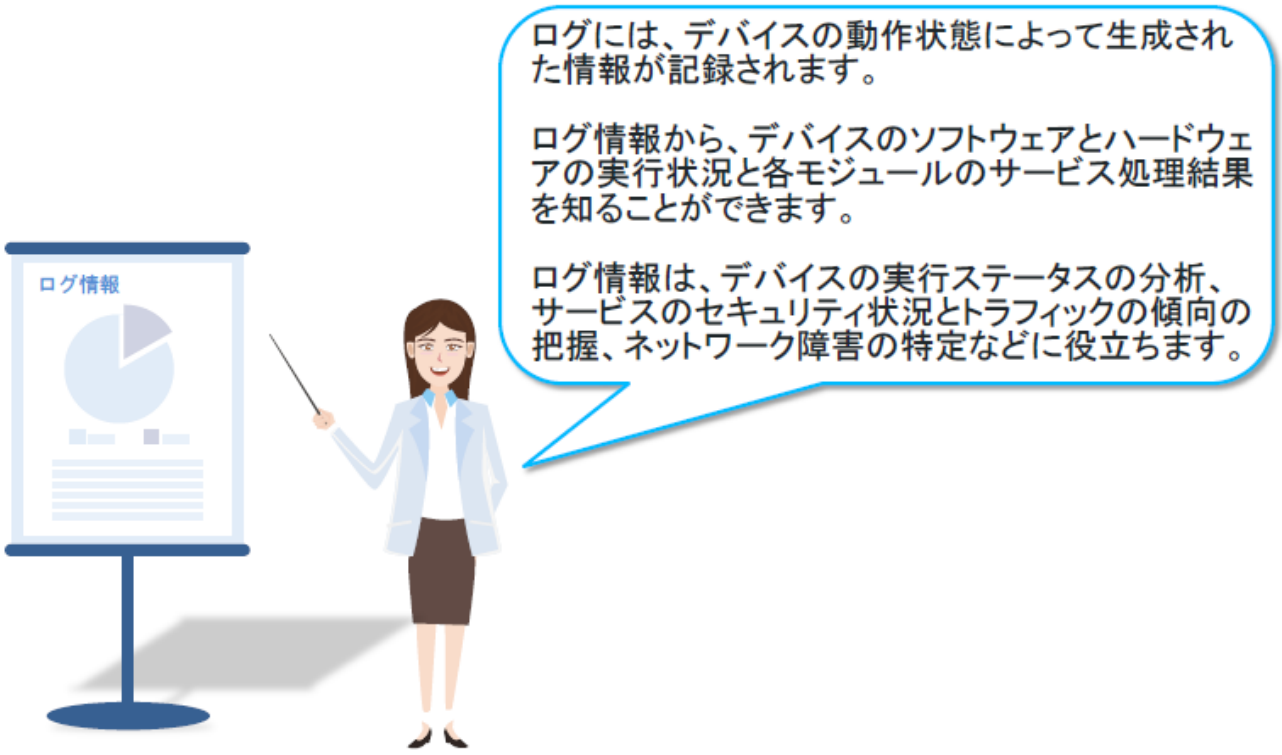
デバイスに攻撃と保護を適用して、デバイス自体を標的とするさまざまなサイバー攻撃からデバイスを保護します。

内部サーバー保護

デバイスのインターフェイスまたはセキュリティ ゾーンに攻撃と保護を適用して、内部サーバーとホストをさまざまなサイバー攻撃から保護します。

技術紹介　ログ情報

ログとは



ログの種類

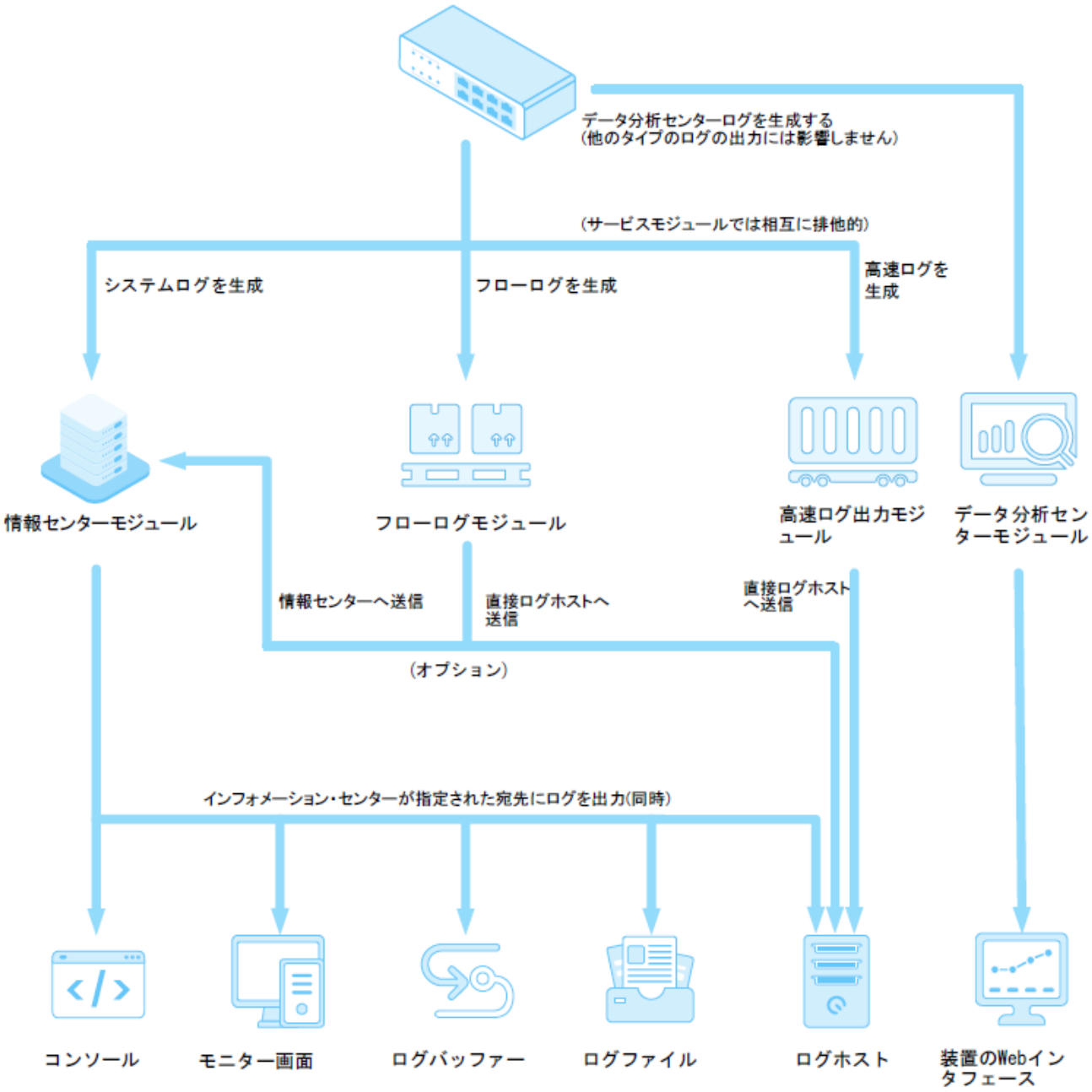
ログの種類	簡単な紹介	出力方法	適用のシナリオ
システムログ	システムログ（Syslog）は各サービスモジュールによって生成されたイベントまたは統計を記録します	システムログは、インフォメーションセンターモジュールを介してASCII形式で端末、コンソール、およびその他の宛先を監視するために出力されます。	デバイスの日常のメンテナンスと監視が必要なシナリオに適用できます。
フローログ	フローログ（User log）は、フローに基づいてセッション情報を記録します。フローログエントリには、セッションパケットの5つの情報とトラフィック統計が含まれます。	フローログはログホストに出力されるか、インフォメーションセンターに送信され、フローログモジュールを介してより効果的なバイナリ形式でさらに処理されます。	多数のセッションの統計分析とパケットトレーサビリティが必要なシナリオに適用できます。
高速ログ	高速ログ（FastlogまたはCustomlog）は、ほとんどのセキュリティサービスモジュールによって生成された統計またはイベントを記録します。	高速ログは、高速ログ出力モジュールを介して、ASCII 形式でインフォメーションセンターではなくログホストに出力されます。出力効率が高い。	セキュリティサービスモジュールの処理結果を監査、監視、および分析する必要があるシナリオに適用できます。
データ分析センターログ	データ分析センターのログは、デバイスによって生成されたイベントまたは統計をインテリジェントに分析し、分析結果を視覚的に表示します。	ログは、データ分析センターモジュールを介してさまざまなチャートや表でWebインターフェイスに表示されます。	ログ分析を視覚的に表示するシナリオに適用可能 デバイスのWebインターフェイスでの結果が必要です。

ログ出力処理

システムログ、フローログおよび高速出力ログは相互に排他的です。複数のログタイプをサポートするサービスモジュールでは、一度に出力できるログタイプは1つのみです。複数のログタイプの出力を同時に使用可能にした場合は、優先度の高いログタイプが出力されます。優先度の高い順に、高速ログ、フローログおよびシステムログが出力されます。ベストプラクティスとして、優先度の高いログタイプを使用してください。

データ分析センターのログと他の種類のログを、互いに影響を与えることなく同時に出力できます。

デバイスは、ログの種類によって異なる出力方法を使用します。次の図に出力プロセスを示します


データ分析センターログを生成する
(他のタイプのログの出力には影響しません)
(サービスモジュールでは相互に排他的)
システムログを生成
フローログを生成
高速ログを
生成
情報センターモジュール
フローログモジュール
高速ログ出力モジ
ュール
データ分析セン
ターモジュール
情報センターへ送信
直接ログホストへ
送信
直接ログホスト
へ送信
(オプション)
インフォメーション・センターが指定された宛先にログを出力(同時)
コンソール
モニター画面
ログバッファー
ログファイル
ログホスト
装置のWebイン
タフェース

アプリケーション・シナリオに応じて適切な出力先を使用できます。次の表に、各出力先の詳細な概要を示します。

出力先	応用シナリオ	
コンソール	コンソールからデバイスにローカルでログインし、次の操作を実行する必要がある場合に適用できます。 ログをリアルタイムで表示します 。	・ リアルタイムのログ表示をサポートします ・ ログを保存せず、履歴ログの表示もサポートしていません。
モニター画面	TelnetおよびSSHを介してリモートでデバイスにログインしてリアルタイムにログを表示する必要がある場合に適用されます	・ リアルタイムのログ表示をサポートします ・ ログを保存せず、履歴ログの表示もサポートしていません。
ログバッファー	ログレベルまたはモジュールに従って、デバイスによって生成された最新のログをフィルタリングおよび表示する必要があるシナリオに適用できます。	・ 最近生成された少数のログのみを保存します ・ デバイスのリブート後にログの損失防止は行われません ・ display logbufferのコマンドの使用をサポートし、ログレベルまたはモジュールに従って最新のログをフィルタリングおよび表示します。
ログファイル	特定の履歴期間に生成されたログを表示またはエクスポートする必要があるシナリオに適用できます。	・ 長時間生成されたログの保存をサポートします ・ デバイスのリブート後のログファイルの損失防止をサポートします ・ moreコマンドを使用したログファイルの内容の表示、またはログをPCのファイルに保存するエクスポートをサポート
ログホスト	複数のデバイスで生成されたログをログホストで一元管理し、大量のログを長期間保存する必要がある場合に適用	・ 装置のストレージスペースを使用しない ・ 複数のデバイスで生成されたログの一元管理と大量のログの保存をサポートします。 ・ ログの分析と視覚的表示をサポートします。
装置Webインタフェース	デバイスのWebインターフェイスにログ分析結果を視覚的に表示する場合に適用できます。	・ インテリジェント解析結果の視覚的表示をサポートし、理解を容易にします ・ ログの記憶容量は、記憶媒体のサイズによって異なります。

サービスモジュールによるログタイプのサポート

ログタイプのサポートは、サービスモジュールによって異なります。次の表に、サービスモジュールのサポートを示します。

ログの種類	サービスモジュールのサポート
システムログ	ほとんどのサービスモジュールは、システムログの生成をサポートしています。サービスを表示するにはシステムログをサポートするモジュールでは、display info-center source moduleコマンドの後に疑問符(?)を入力します。
フローログ	フローログの生成をサポートしているのは、セッション管理モジュール、NATモジュール、AFTモジュール、およびロードバランシングモジュールだけです。
高速ログ	ほとんどのセキュリティサービスモジュール(セキュリティポリシー、IPS、アンチウイルスなど)では、高速ログの生成がサポートされています。高速ログをサポートするセキュリティサービスモジュールを表示するには、customlog形式の後に疑問符(?)を入力します。
データ分析センターログ	ほとんどのサービスモジュールは、Data Analysis Centerログの生成をサポートしています。表示するにはData Analysis Centerログをサポートするサービスモジュールの場合は、dac log-collect serviceコマンドの後に疑問符(?)を入力します。

ログの設定

システムログの設定

Step 1: サービスモジュールのロギングをイネーブルにします(一部のサービスモジュールでロギングがイネーブルになっています)

Step 2: インフォメーションセンターを有効にします(デフォルトで有効)。

Step 3: インフォメーションセンターモジュールで出力先を指定します(デフォルトの出力先はログファイルとログバッファーです)

フローログの設定

Step 1: サービスモジュールのロギングをイネーブルにします(一部のサービスモジュールでロギングがイネーブルになっています)。

Step 2: フローログモジュールで出力先を指定します。(デフォルトの出力先はログホストです。ベストプラクティスとして、フローログ出力先としてログホストを指定します。

Step 3: 出力先に従って、対応する設定を完了します

- Output flow logs to the log hosts:フローログモジュールでログホストのIPアドレスとポートを指定します
- 情報センターへのフローログの出力:情報センターモジュールで出力先を指定します。(デフォルトの出力先はログファイルとログバッファです。)

高速ログ設定

Step 1: サービスモジュールのロギングをイネーブルにします(一部のサービスモジュールでロギングがイネーブルになっています)

Step 2: サービスモジュールの高速ログ出力をイネーブルにします

Step 3: 高速ログ出力モジュールでログホストのIPアドレスとポートを指定します。

データ分析センターのログ設定

Step 1: サービスモジュールのロギングをイネーブルにします(一部のサービスモジュールでロギングがイネーブルになっています)。

Step 2: データ分析センターモジュールでログ収集を有効にします

技術紹介

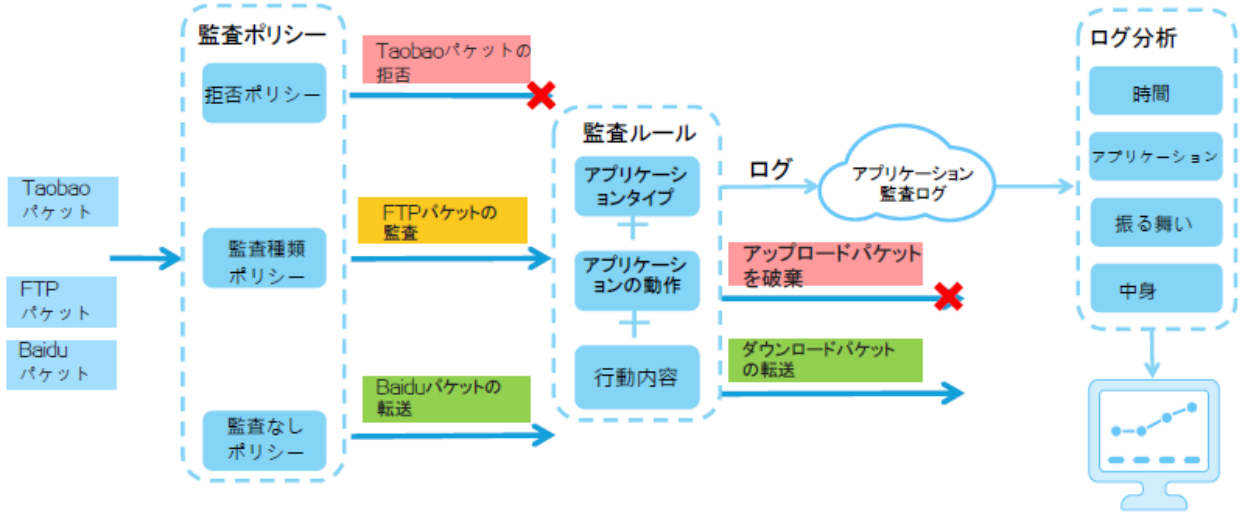
DPI アプリケーション監査と管理

アプリケーション監査と管理について

DPI サービスとして、アプリケーションの監査と管理により、インターネットで使用されている主流のアプリケーション（QQ、163 メール、Baidu など）を正確に識別できます。この機能は、ユーザーのインターネット アクセス行動と行動内容を監査および記録することができます。

動作概要

アプリケーション監査と管理のワークフローは以下の通り:



1. 監査ポリシー: ポリシー タイプごとに異なるパケット一致基準を定義できます。監査ポリシーには次のタイプがあります:

   - 拒否ポリシー—ポリシーの一致基準を満たすパケットをドロップします。
   - 監査種類ポリシー—ポリシーの一致基準を満たすパケットを監査します。
   - 監査なしポリシー—ポリシーの一致基準を満たすパケットを監査しません。

2. 監査規則: 監査タイプのポリシーに一致するパケットは、監査規則のアプリケーション カテゴリ、アプリケーションの動作、および動作の内容と照合されます。一致が見つかったパケットに対して、監査ルールの対応するアクションが実行されます。さらに、デバイスは監査プロセスと結果をログに記録し、ログをログ ライブラリに送信します。

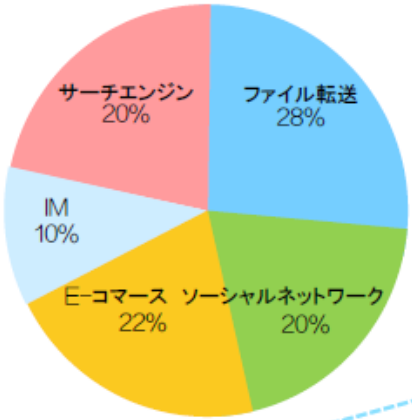
3. ログの分析と提示: デバイスは、ログ ライブラリからログ (たとえば、IM ログ) を抽出し、統計分析を実行し、分析結果を提示します。

ビジュアルなプレゼンテーション

アプリケーションの監査と管理は、従業員のネットワーク行動をさまざまな次元から提示し、企業の管理者が営業時間中の従業員の活動やネットワークトレース、および潜在的なリスクについて学習できるようにします。

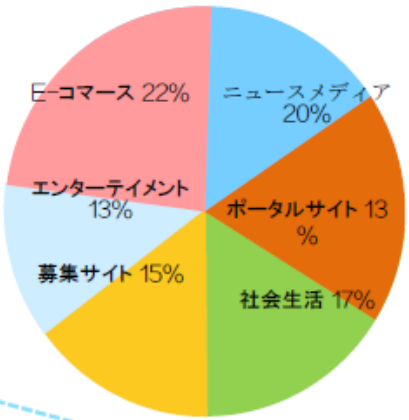
アプリケーショントラフィック分析

企業の管理者が営業時間中の活動について学習できるように、アプリケーショントラフィックの帯域幅に基づいてネットワークの動作を示します。



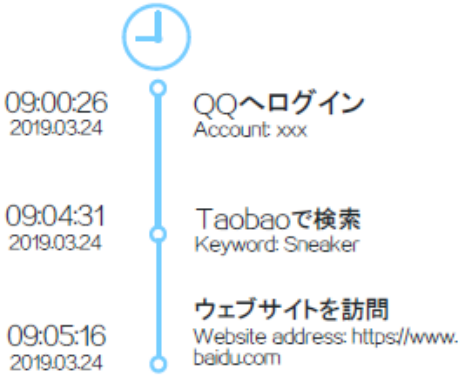
ウェブサイト分析

企業の管理者が辞任のリスクや世論のリスクなどの潜在的なリスクについて学ぶために、Web サイトの種類に基づいてネットワークの動作を提示します。



ユーザー追跡

時間軸の形式でネットワークの動作トレースを記録して表示します。



典型的な応用


情報セキュリティを保護
従業員の電子メールの送受信とファイル転送を監視および制御して、エンタープライズを防止します。
従業員の生産性を向上
IM chat やオンライン ショッピングなどのネットワーク動作を識別して制御します。
機密情報が漏洩するのを防ぎます。
従業員のオンライン発言を監視します
Web サイトやフォーラムでの従業員の意見を監視および管理し、従業員の不適切な発言が企業のイメージを損なうことを防ぎます。