

次世代ファイアウォールを支える App-ID 技術

アプリケーション識別技術における従来型ファイアウォール/UTM 製品との決定的な違い

従来型ファイアウォール製品におけるアプリケーション識別/制御機能の実態

最近、ファイアウォールにおけるアプリケーションベースの可視化と制御に関する話題を多く耳にする様になりました。現在、ステートフル・インスペクションベースのファイアウォールベンダーの多くは、自社のファイアウォール製品をアプリケーション識別と制御が可能な次世代ファイアウォールと呼んでいます。しかし、これらの製品はアプリケーションベースの可視化と制御を行うために、いまだに初期段階のトラフィック分類にポート番号やネットワークプロトコルによる識別を行っています。そして、従来の IPS エンジンを組み合わせることで、アプリケーション識別と制御を実行しています。

近年のネットワークベースで動作するアプリケーションの進化と脅威の巧妙化により、ポートベースでトラフィックの分類や制御を行う従来型のファイアウォール製品が意味をなさなくなっている中、ファイアウォールにおけるアプリケーションベースでの識別と制御について議論が行われることはとても意味があると言えます。

しかし、多くのベンダーが従来型のファイアウォール機能をベースにした製品を次世代ファイアウォールと表現している中、Palo Alto Networks の App-ID 技術によるアプリケーション識別機能が他の従来型の製品と根本的に異なることを明確にしておくことは、とても重要なことであると言えます。

App-ID 技術は Palo Alto Networks 社の次世代ファイアウォール製品で使用しているトラフィック分類技術で、他のベンダーの技術とは根本的に異なります。そして、この App-ID 技術はスタンドアロン型 IPS 製品など、従来のセキュリティソリューションを統合することを可能にします。

App-ID 技術の特徴と実装

・ App-ID 機能は常に動作 :

App-ID によるトラフィック分類はオプション機能でもなく、設定の有効化が必要でもなく常に動作しています。又、アプリケーション識別の為に何らかのシグネチャを有効化する必要もありません。

・ 常に最初に分類処理を実行 :

App-ID のトラフィック分類処理は、Palo Alto Networks 次世代ファイアウォール装置にトラフィックが到達した際、常に最初に分類処理が行われます。全てのファイアウォール装置と同様、

Palo Alto Networks 次世代ファイアウォールも、デフォルトでは全てのトラフィックを拒否しますが、ポリシーで許可されたトラフィックについては全ての App-ID が特別な設定なしにトラフィックの分類を実行します。

・ 全てのトラフィックが対象 :

App-ID は常にすべてのトラフィックを分類します。他の多くのベンダー製品と異なり、特定のネットワークプロトコルのみが対象というわけではありません。全ての App-ID はデバイスを通るビジネスアプリケーション、一般消費者向けアプリケーション、ネットワークプロトコルなど全てを分類します。特定のネットワークプロトコルのみの通信を分類するために何らかの設定が必要になることはありません。なぜなら App-ID は自動的に常に全てのトラフィックをチェックしているためです。

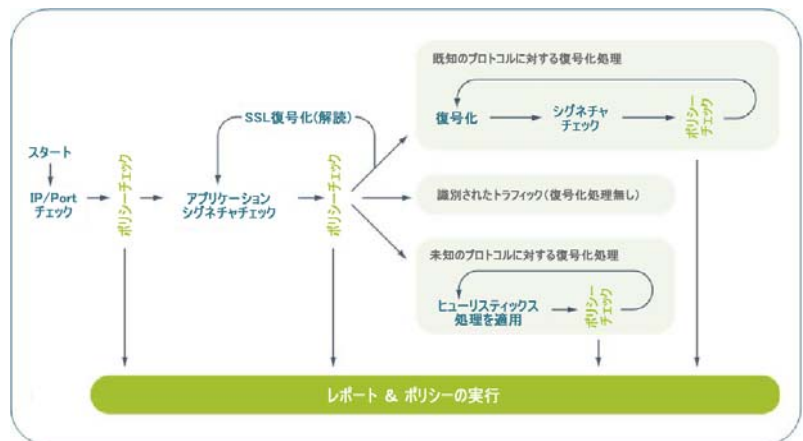


図 1 : App-ID によるアプリケーション識別処理の流れ

次世代ファイアウォールを支える App-ID 技術



アプリケーション識別技術における従来型ファイアウォール/UTM 製品との決定的な違い

・全てのポートが対象：

App-ID は常に全てのポートをチェックしています。アプリケーションが標準ポートを使用して通信した場合はもちろん、アプリケーションが標準以外のポートを使用して通信した場合でも自動的にトラフィックを分類することができます。

・アプリケーションのバージョンや OS に依存しない：

App-ID はサービスレイヤーで動作し、アプリケーションがクライアントとサーバ間でどのような通信が行われたのかをモニタリングします。これは、バージョンの違いやクライアントやサーバの OS 種別を意識しないことを意味します。例えば、BitTorrent は複数のバージョンがあり、複数の OS 間でファイルのやり取りが行われますが、バージョンや OS 毎に複数のシグネチャを用いてトラフィックの分類や制御を行う他の製品と異なり、Palo Alto Networks は単一の App-ID による処理を実現しています。

・全トラフィック分類技術：

各 App-ID は、他の多くの IPS 製品の様にシグネチャのみで構成されている訳ではありません。あらゆる App-ID はアプリケーションを正確に識別するために、最大 4 つのトラフィック分類メカニズムを使用します。しかし、アプリケーションを特定するために何らかの特別な設定を行う必要は全く必要ありません。App-ID は自動的に系統的で適切な識別手段を適用し、正確なアプリケーション識別処理を実現しています。

Palo Alto Networks 製品を利用するお客様は、Web 管理画面の ACC(アプリケーション・コマンド・センター)ページを通して App-ID によって識別された結果や関係するルールを見ることが出来ます。そして、数クリックのマウス操作で、アプリケーションの詳細やユーザ毎の通信内容、脅威(攻撃)等の情報を容易に確認することが出来ます。

App-ID 機能により、アプリケーションベースでトラフィックの可視化や制御が容易に可能になるため、システム管理者は積極的なセキュリティ管理を行うことが可能になります。

通信内容の記録やレポート、脅威の解析機能なども App-ID 機能による優位性を最大限に活かしたものとなり、システム管理者は、正確に識別されたアプリケーションベースの情報を元に迅速なセキュリティインシデントの調査を行うことが可能になります。

最後に、アプリケーションベースの識別処理についての違いが明確であることを確認するために、他のファイアウォールベンダーに対して以下の質問を投げかけてみて下さい。

質問 1. 全てのアプリケーション識別機能はデフォルトで有効になっていますか？

質問 2. アプリケーション識別機能は、全てのトラフィックを対象にしたものですか？それとも特定のトラフィックやポートを指定して行うタイプですか？

質問 3. アプリケーション識別機能は自動的に全てのポートを対象として動作しますか？それとも何らかの設定を必要としますか？

質問 4. 全てのトラフィックや全てのポートを対象としたアプリケーション識別機能を利用する場合、何ステップの設定作業が必要ですか？

質問 5. アプリケーション別の通信量やユーザ毎、又は脅威毎の通信を可視化するツールは製品本体価格の中に含まれていますか？

質問 6. アプリケーションベースのトラフィック制御とファイアウォールポリシー管理画面は統合されていますか？それとも個別に管理するタイプですか？

質問 7. カタログ/データシートに記載のスループットデータは、アプリケーションベースの識別機能を有効にした時のものですか？それとも、従来のポートベースの分類を行った時のものですか？