Web セキュリティ アプライアンス設計ガイド

目次

概要

このドキュメントでは、最適なパフォーマンスを得るために Cisco Web セキュリティ アプライアンス（WSA）および関連コンポーネントを設計する方法について説明します。

背景説明

WSA 用のソリューションを設計するときには、アプライアンス自体の設定だけでなく、関連するネットワーク デバイスとそれらの機能についても注意深く考慮する必要があります。 それぞれのネットワークは多数のデバイスからなるコラボレーションであり、ネットワーク内のいずれか 1 つが正しい方法で参加しない場合、ユーザ エクスペリエンスが低下する可能性があります。

WSA を設定するときには、主に 2 つのコンポーネントを考慮する必要があります。 つまりハードウェアとソフトウェアです。 ハードウェアには 2 つの種類があります。 1 つは物理ハードウェア タイプで、S170、S380、S680 シリーズ モデルや、その他のサポート終了（EoL）モデル（S160、S360、S660、S370、S670 シリーズ モデル）があります。 もう 1 つは仮想ハードウェア タイプで、S000v、S100v、S300v シリーズ モデルなどがあります。 このハードウェアで実行されるオペレーティング システム（OS）は *AsyncOS for Web* と呼ばれ、これはコアとして FreeBSD に基づいています。

WSA はプロキシ サービスを提供し、さらにすべてのトラフィック（HTTP、HTTPS、ファイル転送プロトコルつまり FTP）をスキャン、検査、分類します。 これらすべてのプロトコルは TCP 上で実行され、これらが正常に動作するにはドメイン ネーム システム（DNS）に大きく依存します。 こうした理由で、アプライアンスが正しく動作し、（企業の制御範囲内外を問わず）ネットワークのさまざまな部分と通信するためには、ネットワークの健全性が重要です。

設計

最適なパフォーマンスを得るために WSA および関連コンポーネントを設計するには、このセクションで説明する情報を使用します。

ネットワーク

WSA が正しく動作するには、エラーのない高速なネットワークが不可欠です。 ネットワークが不安定になると、ユーザ エクスペリエンスが低下する可能性があります。 ネットワークの問題が検出されるのは、通常、Web ページに到達するのに時間がかかったり、到達できないときです。このような場合、まずアプライアンスの問題だと思いがちですが、通常はネットワークの動作の問題です。 したがって HTTP、HTTPS、FTP、DNS などの高度なアプリケーション プロトコル向けにネットワークが最適なサービスを提供できるよう、注意深く考慮して監査する必要があります。

一般的な考慮事項

最適なネットワーク動作を実現するための一般的な考慮事項を次に示します。

- レイヤ 2（L2）ネットワークが安定していること、スパニング ツリーが正しく動作していること、スパニング ツリーの計算とトポロジの変更が頻繁に発生しないことを確認します。

- 使用されるルーティング プロトコルもまた、高速コンバージェンスと安定性を備えている必要があります。 Open Shortest Path First（OSPF）高速タイマーまたは Enhanced Interior Gateway Routing Protocol（EIGRP）がこのようなネットワークに適しています。

- WSA で少なくとも次の 2 つのデータ インターフェイスを常に使用してください。 1 つはエンドユーザ コンピュータに面し、もう 1 つはアウトバウンド操作用です（アップストリーム プロキシやインターネットに接続されます）。 このようにする目的は、リソース制約の可能性（たとえば TCP ポート数がすべて使用されたり、ネットワーク バッファが満杯になったりすること）を防ぐためです。内外の両方で単一のインターフェイスを使用すると、これが発生しやすくなります。

- セキュリティを強化するために、管理トラフィック専用の管理インターフェイスを使用してください。 GUI を介してこれを設定するには、[Network] > [Interfaces] までナビゲートして [Separate routing (M1 port restricted to appliance management services only)] チェックボックスをオンにします。

- 高速な DNS サーバを使用します。 WSA を介したトランザクションでは、少なくとも 1 つの DNS ルックアップが必要です（キャッシュに存在しない場合）。 DNS サーバが低速（または動作が不適切）である場合、すべてのトランザクションが影響を受けて、インターネット接続が遅延している、または低速であると見なされます。

- 別個のルーティング テーブルが使用される場合は、次の規則が適用されます。

  すべてのインターフェイスがデフォルト *Management* ルーティング テーブルに含まれます

（M1、P1、P2）。

データ インターフェイスのみが *Data* ルーティング テーブルに含まれます。

注: ルーティング テーブルの分離はインターフェイスごとではなく、サービスごとに行われます。 たとえば WSA と Microsoft Active Directory（AD）ドメイン コントローラの間のトラフィックは、Management ルーティング テーブルで指定された経路に常に従います。このテーブルで P1/P2 インターフェイスから出る経路を編集することができます。 管理インターフェイスを使用する経路を Data ルーティング テーブルに含めることはできません。

ロード バランシング

ネットワークの動作を最適化するために、次のようなロード バランシングを実装することを考慮できます。

- DNS ローテーション â はこれ単一ホスト名がプロキシとして使用されるが、DNSサーバの倍数 A レコードがありますとき使用される用語です。 各クライアントはこれを別個の IP アドレスに解決し、異なるプロキシを使用します。 制約事項として、DNS レコードの変更が再起動後にクライアントに反映されるため（ローカル DNS キャッシュ）、変更が必要になった場合の堅牢性が低くなります。 しかし、これはエンドユーザに意識されずに行われます。

- プロキシアドレス制御（PAC）ファイル â はこれら各 URL がその中の文書による機能に基づいてブラウザでどのように処理する必要があるか判別するプロキシ自動スクリプトを書くファイルです。 同じ URL を常に直接転送したり、同じプロキシに転送したりする機能があります。

- オートディスカバリ â はこれ PAC ファイルを記述します（前の考慮事項に説明がある）得るために DNS/DHCP 方式の使用を。 通常、この最初の 3 つの考慮事項が 1 つのソリューションに統合されます。 ただし、これは複雑になる場合があり、多くのユーザ エージェント（Microsoft Office、Adobe ダウンローダ、JavaScript、Flash など）では PAC ファイルをまったく読み取ることができません。

- Web Cache Control Protocol（WCCP） â このプロトコル（特に WCCP バージョンは 2）複数間の負荷バランシングを WSAs 作成し、ハイ アベイラビリティを組み込む強く、また非常に強力な方法を提供します。

- 専用マシンとしてロードバランサを使用することを別途の負荷バランシング アプライアンス â Cisco は推奨します。

ファイアウォール

最適なネットワーク動作を実現するための、ファイアウォールに関する考慮事項を次に示します。

- 各ソースからネットワーク全体でのインターネット制御メッセージ プロトコル（ICMP）が許可されることを確認します。 これが重要である理由は、WSA がパス Maximum Transition Unit（MTU）検出機能に依存するためです（RFC 1191 の説明を参照）。この機能は ICMP

エコー要求（タイプ 8）およびエコー応答（タイプ 0）に依存し、ICMP 到達不能フラグメンテーションを必要とします（タイプ 3、コード 4）。 CLI コマンド **pathmtudiscovery** を使って WSA でパス MTU 検出を無効にした場合、WSA は RFC 879 に従ってデフォルト MTU 576 バイトを使用します。 これによりオーバーヘッドが増加し、パケットが再構築されてパフォーマンスが影響を受けます。

- ネットワーク内に非対称ルーティングが存在しないことを確認してください。 これは WSA の問題ではありませんが、パスでファイアウォールが検出されると、通信の両側をまだ受信していないため、パケットがドロップされます。

- ファイアウォールでは、通常のエンドユーザ コンピュータ ステーションとして WSA IP アドレスを脅威から除外することが非常に重要です。 ファイアウォールは、（一般的なファイアウォールの知識に従って）接続が多すぎるために WSA IP アドレスをブラックリストに含める可能性があります。

- 顧客宅内デバイスで WSA IP アドレス用にネットワーク アドレス変換（NAT）が採用されている場合、各 WSA が NAT で個別の外部グローバル アドレスを使用するようにしてください。 1 つの外部グローバル アドレスを持つ複数の WSA 用に NAT を使用すると、次のような問題が発生する可能性があります。

  すべての WSA からのすべての外部接続で単一の外部グローバル アドレスが使用され、ファイアウォールのリソースが急速に不足します。

  その 1 つの宛先へのトラフィックでスパイクが発生すると、宛先サーバがそれをブラックリストに含める可能性があり、企業全体が遮断されてこのリソースにアクセスできなくなる恐れがあります。 これは重要なリソースかもしれません。企業のクラウド ストレージ、オフィスのクラウド接続、または各コンピュータのウイルス対策ソフトウェアが更新を行うためです。

ID

ID のすべての構成要素に*論理積*の原則が当てはまることに注意してください。 たとえばユーザ エージェントと IP アドレスの両方を設定する場合、この IP アドレス*から*のユーザ エージェントを意味します。 ユーザ エージェント*または*この IP アドレスという意味ではありません。

同じサロゲート タイプ（またはサロゲートなし）および/またはユーザ エージェントの認証用に 1 つの ID を使用します。

Internet Explorer、Mozilla Firefox、Google Chrome など、プロキシ認証をサポートする既知のブラウザ/ユーザ エージェント用のユーザ エージェント文字列を、認証を必要とするそれぞれの ID に必ず含めることが重要です。 アプリケーションの中には、インターネット アクセスを必要としてもプロキシ/WWW 認証をサポートしないものがあります。

ID は上位から下位に照合され、いずれかのエントリで最初に一致すると、一致の検索が終了します。 このため、*ID 1* と *ID 2* が設定されている場合にあるトランザクションが ID 1 に一致すると、ID 2 との照合検査は行われません。

アクセス/復号化/ルーティング/発信マルウェア ポリシー

これらのポリシーは、次のようにさまざまなトラフィック タイプに対して適用されます。

- アクセス ポリシーはプレーン HTTP 接続または FTP 接続に対して適用されます。 トランザクションを受け入れるか、それとも廃棄（ドロップ）すべきかを決定します。

- 復号化ポリシーは、HTTPS トランザクションを復号化するか、廃棄するか、それともパススルー（通過）させるかを決定します。 トランザクションが復号化された場合、その結果の一部はプレーン HTTP 要求として認識可能になり、アクセス ポリシーに対して照合されます。 ある HTTPS 要求を廃棄する必要がある場合、アクセス ポリシーではなく復号化ポリシーでそれを廃棄してください。 こうしないと、破棄対象のトランザクションがまず復号化されてから破棄されるため、CPU とメモリが余分に消費されます。

- ルーティング ポリシーは、WSA によって許可されたトランザクションのアップストリーム方向を決定します。 アップストリーム プロキシが存在する場合、または WSA が*コネクタ* モードでクラウド Web セキュリティ タワーにトラフィックを送る場合に、これが該当します。

- 発信（アウトバウンド）マルウェア ポリシーは、エンドユーザから Web サーバに向かう HTTP または FTP アップロードに対して適用されます。 これは通常、HTTP ポスト要求で見られます。

各ポリシー タイプで*論理和*の原則が当てはまることに注意してください。 複数の ID が参照される場合、設定された任意の ID にトランザクションが照合されます。

より細かく制御するには、これらのポリシーを使用します。 各ポリシーで ID が誤って設定されると問題が発生する可能性があります。1 つのポリシーで参照される複数の ID を使用した方が適切です。 ID がトラフィックに影響を与えないことに注意してください。ID は単に、あとでポリシーで照合できるようにトラフィック タイプを識別するだけです。

多くの場合、復号化ポリシーでは認証で ID を使用します。 これは決して問題ではなく、これが必要な場合もありますが、復号化ポリシーで参照される認証とともに ID を使用すると、復号化ポリシーに一致するすべてのトランザクションが認証用に復号化されることになります。 復号化操作が廃棄またはパススルーされることもありますが、認証用の ID が存在するため、あとでトラフィックを廃棄またはパススルーするために復号化が発生します。 これは高コストであり、避けるべきです。

設定によっては 30 個以上の ID と 30 個以上のアクセス ポリシーを含み、すべてのアクセス ポリシーにすべての ID が含まれる場合もあることがわかっています。 この場合、すべてのアクセス ポリシーで ID が照合されるならば、これほど多くの ID を使用する必要はありません。 これによってアプライアンスの動作に悪影響が及ぶわけではありませんが、トラブルシューティングを試みたときに混乱を招き、パフォーマンスの観点から見て高コストです。

カスタム URL カテゴリ

よく誤解/誤用されているとはいえ、カスタム URL カテゴリを強力なツールとして使用できます。 たとえば、ID での照合用にすべてのビデオ サイトを含む構成が存在します。 WSA には、ビデオ サイトの URL が（頻繁に）変更されたときに自動更新を行う組み込みツールが備わっています。 したがって、WSA で URL カテゴリを自動的に管理し、特殊な未分類サイト用にカスタム URL カテゴリを使用するのが適切です。

正規表現を使用する際には細心の注意が必要です。 たとえばドット (.) やアスタリスク (*) などの特殊文字の照合を使用すると、結果的に CPU やメモリを非常に消費することがあります。 WSA はすべての正規表現を展開して各トランザクションと照合します。 たとえば、次の正規表現について考えてください。

```
example.*
```

この表現は、*example.com* ドメインだけでなく、*example* という語を含むすべての URL に一致します。 正規表現では *ドット*や*アスタリスク*の使用をできるだけ避け、最後の手段としてのみ使用してください。

問題を発生させる可能性のある正規表現の例をもう 1 つ示します。

```
www.example.com
```

このドットは任意の文字を意味するため、この例を [Regular Expressions] フィールドで使用すると、*www.example.com* だけでなく *www.www3example2com.com* にも一致します。 *www.example.com* のみを一致させるには、次のようにドットをエスケープします

```
www\.example\.com
```

このケースでは、正規表現を使用する理由がありません。次の形式を使ってこれをカスタム URL カテゴリ ドメイン内部に含めることができるためです。

```
www.example.com
```

マルウェア対策とレピュテーション

複数のスキャン エンジンが有効になっている場合は、適応型スキャンも有効にするという選択肢を考慮してください。 WSA 上の適応型スキャンは、それぞれの要求を事前スキャンし、どの包括的エンジンを使って要求をスキャンすべきかを決定する、小規模ながら強力なエンジンです。 これにより WSA のパフォーマンスが若干向上します。