目次

概要

この資料に Cisco Web セキュリティ アプライアンス (WSA) および最適化されたパフォーマンスのための関連付けられているコンポーネントを設計する方法を記述されています。

背景説明

WSA のためのソリューションを設計するとき、アプライアンスの設定自体に関して注意深い考察、だけでなく、また関連するネットワークデバイスおよび機能を必要とします。 各ネットワークは多数のデバイスおよびそれらの 1 つがネットワークに正しく加わらなければ、ユーザー エクスペリエンスのコラボレーション低下するかもしれませんです。

WSA を設定するとき考慮する必要がある 2 つの主要なコンポーネントがあります: ハードウェアおよびソフトウェア。 ハードウェアは 2 つの異なる型入って来ます。 第 1 は物理的 なタイプの S160、S360、S660、S370 および S670 シリーズ モデルのような生命 (EoL) モデルの S170、S380 および S680 シリーズ モデル、またもう一方の端のようなハードウェア、です。 他のハードウェア タイプは S000v、S100v および S300v シリーズモデルのような仮想、です。 Operating System （ OS ）はこのハードウェアで動作するコアの FreeBSD に基づいている *Web のための AsyncOS* と呼ばれます。

WSA はプロキシサービスを提供し、またすべてのトラフィック (HTTP、HTTPS および File Transfer Protocol （ FTP ）) をスキャンし、検査し、分類します。 TCP の上をこれらのプロトコル実行すべては正しい動作のための Domain Name System （ DNS ）にとても依存し。 これらの理由により、ネットワーク稼働状況はアプライアンスの正しい動作および企業制御のの内側と外側の両方にネットワークのさまざまな一部が付いている通信のために重要、です。

設計

情報を使用して下さい最適化されたパフォーマンスのための WSA および関連コンポーネントを

設計するためにこのセクションに説明がある。

ネットワーク

誤りが無い、ファースト ネットワークは WSA の正しい動作のために重要です。 ネットワークが不安定である場合、ユーザ エクスペリエンスは低下するかもしれません。 ネットワーク上の問題は通常 Webページが達するために時間がかかる検出するまたは到達不能ときです。 最初の傾斜は責任アプライアンスですが、のは通常不品行な振舞いをうネットワークです。 従ってネットワークが HTTP、HTTPS、FTP および DNS のような高レベル アプリケ– ションプロトコルのための最もよいサービスを提供するようにするために、注意深い考察および監査は作る必要があります。

一般的な考慮事項

最もよいネットワーク 動作を確認するために設定できるいくつかの一般的な考慮事項はここにあります:

- スパニングツリーオペレーションが正しいこと、そして頻繁ではないスパニングツリー計算およびトポロジーの変更がないことことレイヤ2（L2）ネットワークが安定 して いる確認して下さい。

- 使用するルーティング プロトコルはまた速やかな収束および安定性を提供する必要があります。 Open Shortest Path First（OSPF）ファースト タイマーか Enhanced Interior Gateway Routing Protocol（EIGRP）はそのようなネットワークのためのよい選択です。

- WSA の少なくとも 2 つのデータインターフェイスを常に使用して下さい: エンドユーザ コンピュータに直面する 1 つ、および送信 オペレーションのためのもう 1 つ（アップストリーム プロキシかインターネットに接続される）。 これは TCP ポートの数が排出されるか、またはネットワーク バッファーが一杯になるとき可能性のある リソースを除去するために抑制します、のようなされます（の使用と特にの内側と外側の両方にのための単一 のインターフェイス）。

- セキュリティを強化するために管理だけトラフィックのためのマネージメントインターフェイスを捧げて下さい。 これを GUI によって実現させるために、**ネットワーク > インターフェイス**にナビゲート し、**別途のルーティング（アプライアンス マネジメント サービスだけに制限 される M1 ポート）**チェックボックスをチェックして下さい。

- ファースト DNSサーバを使用して下さい。 WSA によるどのトランザクションでも少なくとも 1 DNS lookup を必要とします（そうでなかったらキャッシュで）。 遅く、または影響あらゆるトランザクション不品行な振舞いをい、遅らせられるか、または遅いインターネット接続として観察される DNSサーバ。

- 別々のルーティング テーブルが使用されるとき、これらのルールは適用されます:

  すべてのインターフェイスはデフォルト *管理* ルーティング テーブル（M1、P1、P2）に含まれています。

データインターフェイスだけデータ ルーティング テーブルに含まれています。

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に、しかしむしろサービスごとにないあります。 たとえば、WSA と Microsoft Active Directory （AD）ドメインコントローラ間のトラフィックは管理 ルーティング テーブルで規定 される、この表の P1/P2 インターフェイスの指摘するルーティングを設定することは可能性のあるですルーティングに常に従い。 マネージメントインターフェイスを使用するデータ ルーティング テーブルにルーティングを含めることはできません。

ロード バランシング

最もよいネットワーク 動作を確認するために設定できるいくつかのロードバランシング考慮事項はここにあります:

- DNS ローテーションか。 これは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。 各クライアントは別の IP アドレスにこれを解決し、異なるプロキシを使用します。 制限は変更を行う必要がある場合、そうそれ提供しますロバストネスの低いレベルを DNS レコードの変更が再度ブートする（キャッシュするローカル DNS）にクライアントで示されることです。 ただし、これはエンドユーザに対して透過的です。

- プロキシアドレス コントロール（PAC）ファイルか。 これらは各 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。 それに直接または同じプロキシに同じ URL を常に転送する機能があります。

- オートディスカバリか。 これは 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 メソッドの使用を。 通常、これらの最初 3 つの考慮事項は 1 ソリューションに結合されます。 ただし、これは複雑であり、多くのユーザ エージェントは、Microsoft Office のような、Adobe Downloader、JavaScript およびフラッシュする、PAC ファイルを全然読み込むことができません。

- Web Cache Control Protocol （WCCP）か。 このプロトコル（特に WCCP バージョンは 2）複数間のロードバランシングを 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。

- 別々のロードバランシング アプライアンスか。 Cisco は専用マシンとしてロードバランサを使用することを推奨します。

ファイアウォール

最もよいネットワーク 動作を確認するために設定できるいくつかのファイアウォール考慮事項はここにあります:

- インターネット制御メッセージ プロトコル （ICMP）が各ソースからのネットワーク全体許可されるようにして下さい。 これは WSA が ICMPエコー要求（タイプ 8）およびによってエコーリプライ（0）タイプ決まる、および ICMP 到達不能フラグメンテーションが必要となりますパス最大移行ユニット（MTU）ディスカバリ メカニズムによって RFC 1191 に記述さ

れているように、決まるので、重要です、（タイプ 3、4）コード。 **pathmtudiscovery** CLI コマンドで WSA のパスMTU ディスカバリをディセーブルにする場合、WSA は RFC 879 によって 576 バイトのデフォルトMTU を、使用します。 これは増加されたオーバーヘッドによるパフォーマンスおよびパケットの再組立てに影響を与えます。

- ネットワークのの中の非対称的なルーティングがないことを確認して下さい。 これが WSA の問題の間、通信の両側を受け取らなかったのでパスに沿って見つけられるどのファイアウォールでもパケットを廃棄します。

- ファイアウォールによって、規則的なエンド ユーザー コンピューター ステーションとして脅威から WSA IP アドレスを除外することは非常に重要です。 ファイアウォールは余りにも多くの接続による WSA IP アドレスをブラックリストに載せるかもしれません（概要ファイアウォール ナレッジによって）。

- ネットワーク アドレス変換（NAT）がカスタマー プレマイズ デバイスのあらゆる WSA IP アドレスのために用いられる場合、各 WSA が NAT で別途の外部グローバルアドレスを使用するようにして下さい。 多重 WSAs のために NAT を使用すれば単一 外部グローバルアドレスがある、これらの問題に出会うかもしれません:

  WSAs すべてからの外界 使用への接続すべて単一 外部グローバルアドレス、およびファイアウォールはすぐにリソースを使い果たします。

  その単一 の 宛先の方のトラフィックのスパイクがある場合、宛先 サーバはそれをブラックリストに載せ、アクセスからこのリソースに全体の企業を断ち切るかもしれません。 これは会社 Cloud ストレージ、オフィス Cloud 接続、または毎コンピュータ アンチウィルスソフトウェア更新として貴重なリソースであるかもしれません。

識別

*論理的のおよび*プリンシパルが識別のすべてのコンポーネントで適用することを覚えていて下さい。 たとえば、ユーザーエージェントおよび IP アドレスを両方設定すれば、それはこの IP アドレスからのユーザーエージェントを意味します。 それはユーザーエージェントかこの IP アドレスを意味しません。

同じ代用型（またはサロゲート無し）および/またはユーザーエージェントの認証のために 1 つの識別を使用して下さい。

認証を含まれているプロキシ認証を、Internet Explorer のような、Mozilla Firefox サポートする、および Google クロム必要とする既知 ブラウザ/ユーザーエージェントのためのユーザーエージェント ストリングが各識別を確認することは重要です。 インターネットアクセスを必要とするが、ありましたり proxy/WWW 認証をサポートしませんいくつかのアプリケーションが。

識別は最初の一致されたエントリで終了する一致のための検索との一致された上下です。 従って *識別 1* および *識別 2* を設定してもらえばおよびトランザクション一致識別 1、それは識別 2.に対してチェックされません。

アクセス/復号化/ルーティング/Malware 送信ポリシー

これらのポリシーはトラフィックの異なる型に対して適用します:

- アクセスポリシーは明白な HTTP または FTP 接続に対して適用します。 彼らはトランザクションが受け入れられるか、または廃棄する必要があるかどうか判別します。

- 復号化ポリシーは HTTPS トランザクションが復号化されるか、廃棄されるか、または渡す必要があるかどうか判別します。 トランザクションが復号化される場合、それの連続した部分は明白な HTTP 要求として見られる場合があり、アクセスポリシーと一致します。 HTTPS 要求を廃棄する必要がある場合復号化ポリシーで、ないアクセスポリシーでそれを廃棄して下さい。 さもなければ、それは復号化され、次に廃棄されるべき廃棄されたトランザクションのためのより多くの CPU およびメモリを最初に消費します。

- ルーティングポリシーは彼の WSA によって可能にしたそれトランザクションのアップストリーム 方向を判別します。 これはまたは WSA が*コネクタ* モードにあるか、適用し、Cloud Web セキュリティ タワーにトラフィックをあればアップストリーム プロキシが送信 します。

- 送信 malware ポリシーは Webサーバの方のエンドユーザからの HTTP または FTP アップロードに対して適用します。 これは通常です HTTP ポスト要求見られます。

ポリシーの各型に関しては、*論理的のか*プリンシパルが適用することを覚えておくことは重要です。 複数の識別を参照してもらう場合トランザクションは設定されるの識別一致する必要があります。

粒状制御に関しては、これらのポリシーを使用して下さい。 ポリシーごとの不正確に設定された識別はポリシーで参照される複数の識別を使用することは有利である問題を作成できます。 それらがちょうどポリシーのより遅い一致に対するトラフィック の 種類を識別することをことを識別影響を与えないトラフィックに覚えていて下さい。

多くの場合時、復号化ポリシーは認証と識別を使用します。 これが間違っていないし、時々必要である間、復号化 ポリシーで参照される認証を用いる識別の使用は認証が起こることができるように復号化 ポリシーを一致するすべてのトランザクションが復号化されることを意味します。 復号化操作は廃棄されるか、または渡されるかもしれませんが認証を用いる識別があるので、復号化はより遅いドロップするかパススルー トラフィック起こります。 これは高く、避ける必要があります。

コンフィギュレーションはアクセスポリシーすべては識別すべてが含まれているところで、観察されましたまたはより多くの識別がおよび 30 含まれているまたはより多くのアクセスポリシー 30。 この場合アクセスポリシーすべてで一致する場合、この多くの識別を使用する必要がありません。 これはアプライアンス オペレーションに害を与えない間、解決する試みで混合を作成し、パフォーマンスに関して高いです。

カスタム URL カテゴリー

カスタム URL カテゴリーの使用は通常誤解され、誤用される WSA の強力なツールです。 たとえば、コンフィギュレーションがあります識別で一致のためのすべてのビデオ サイトが含まれている。 WSA にビデオ サイトが URL を変更するとき自動的に更新組み込みツールがあります、頻繁に発生する。 従って、それは WSA が URL カテゴリーを自動的に管理するようにする理にかない特別な、まだ分類されたサイトのためにカスタム URL カテゴリーを使用します。

正規表現と非常に注意して下さい。 ドット（。）およびスターのような特殊文字一致が（*）使

用される場合、広範な CPU および非常にメモリであると証明するかもしれません。 WSA は各トランザクションに対してそれを一致するために正規表現を拡張します。 たとえば、正規表現はここにあります:

この式はワード*例*を紹介している URL を、だけでなく、*example.com* ドメイン 一致する。 *ドット*の使用を避け、正規表現で*主演*し、最終的な解決策としてだけそれらを使用して下さい。

問題を作成するかもしれない正規表現のもう一つの例はここにあります:

ファイルされるこの例を正規表現で使用する場合だけでなく、*www.example.com* を一致するが、ここではドットとしてまた *www.www3example2com.com は*、*文字*を意味します。 *www.example.com だけ*一致する望む場合ドットをエスケープして下さい:

この場合この形式のカスタム URL カテゴリ ドメインの中でこれを含むことができるとき、正規表現 機能を使用する原因がありません:

反Malware および評判

複数のスキャン エンジンが有効に なる場合、また適応性があるスキャンを有効に する オプションを検討して下さい。 適応性があるスキャンは事前スキャンが各要求および使用されたスキャン要求のはずである広範囲のエンジンを判別する WSA の強力で小さいエンジンですが。 これはわずかに WSA のパフォーマンスを向上します。