Ciscoセキュリティ管理アプライアンス(SMA)の「trailblazer」CLIコマンドの管理の詳細

内容

概要

AsyncOS 11.4以降で[AsyncOS 12.x for Security Management Appliance(SMA)を引き続き使用する](#)と、Webユーザインターフェイス(UI)が再設計され、データの内部処理が行われました。この記事では、新しく再設計されたWebユーザインターフェイスを参照する機能の変更について説明します。 より高度な技術設計の実装により、シスコはユーザエクスペリエンスの向上に努めてきました。

著者：Cisco TACエンジニア、Chris Arellano

前提条件

注意： 「管理」インタフェースは、SMAの最初の構成時に表示されるデフォルトのインタフェースです。**「ネットワーク」>「IPインタフェース」から**は、削除はできません。 このため、サービスが検証されるデフォルトインターフェイスは常に使用されます。

trailblazerconfigを有効にする前に、次の項目が確認されていることを**確認します**。

1. SMAがアップグレードされ、AsyncOSバージョン12.x（またはそれ以降）が実行されている
2. [Network] > [IP Interfaces]で、管理インターフェイスの[Appliance Management] > [HTTPS]**が有効になって**います **アプライアンスの管理> HTTPSポート**をファイアウォールで開く必要があります
3. [Network] > [IP Interfaces]の順に選択すると、管理インターフェイスで**AsyncOS API > HTTPとAsyncOS > HTTPSの両方が有効**になります。 **[AsyncOS API] > [HTTP and AsyncOS API] > [HTTPS ports must be opened on** firewall]
4. 「Trailblazer」ポートは、ファイアウォールを介して開く必要があります デフォルトは4431
5. DNSが管理インターフェイス「ホスト名」を解決できることを確認します。つまり、nslookup ***sma***.hostname**は*IPアドレス***を返します
6. DNSが、スパム検疫にアクセスするように設定された「*This is the default interface for the Spam Quarantine*」ホスト名/URLを解決できることを確認します

理由

12.x次世代SMA(NGSMA)GUIは、クライアント(IE、Chrome、Firefox)にダウンロードされるシングルページアプリケーション(SPA)として再実装され、ユーザエクスペリエンスを向上させます。 SPAはSMAの複数の内部サーバと通信し、それぞれが異なるサービスを実行します。

SMAへのSPA通信におけるCORS(Cross-Origin Resource Sharing)制限により、複数のモジュール間の通信に障害が発生します。

- CORSは、悪意のあるコマンドが確立された通信回線内で別の内部サービスに実行されるのを防ぐために設計されたセキュリティ機能です。

内部サーバは、NGSMAを介して異なる番号付きTCPポートを介して到達可能です。各TCPポートは、クライアントと通信するために個別の証明書承認を必要とします。 NGSMAの内部サーバと通信する機能が不十分なため、問題が発生します。

影響

「/euq-login」および「ng-login」を含む次世代Webインターフェイス

AMP Cisco Threat Response(CTR)統合のレポート。

解決方法

異なるモジュールを表すTCPポートの簡単な例では、各ポートの証明書受け入れが必要です。 信頼できる署名付き証明書がSMAに存在しない場合、ブラウザがモジュールへの透過的な通信を開始するため、複数の証明書受け入れが必要です。 TCPポート6443、443、および4431の必要性を理解していないユーザに対しては、この経験が混乱を引き起こす可能性があります。

これらの課題を克服するため、シスコはNginxを実装して、クライアント（ブラウザクライアント）とサーバ（特定のポートを介して到達可能なサービス）間でプロキシ機能を実行しています。 Nginx（NGINXまたはnginxとしてスタイル化）は、リバースプロキシ、ロードバランサ、メールプロキシ、HTTPキャッシュとしても使用できるWebサーバです。

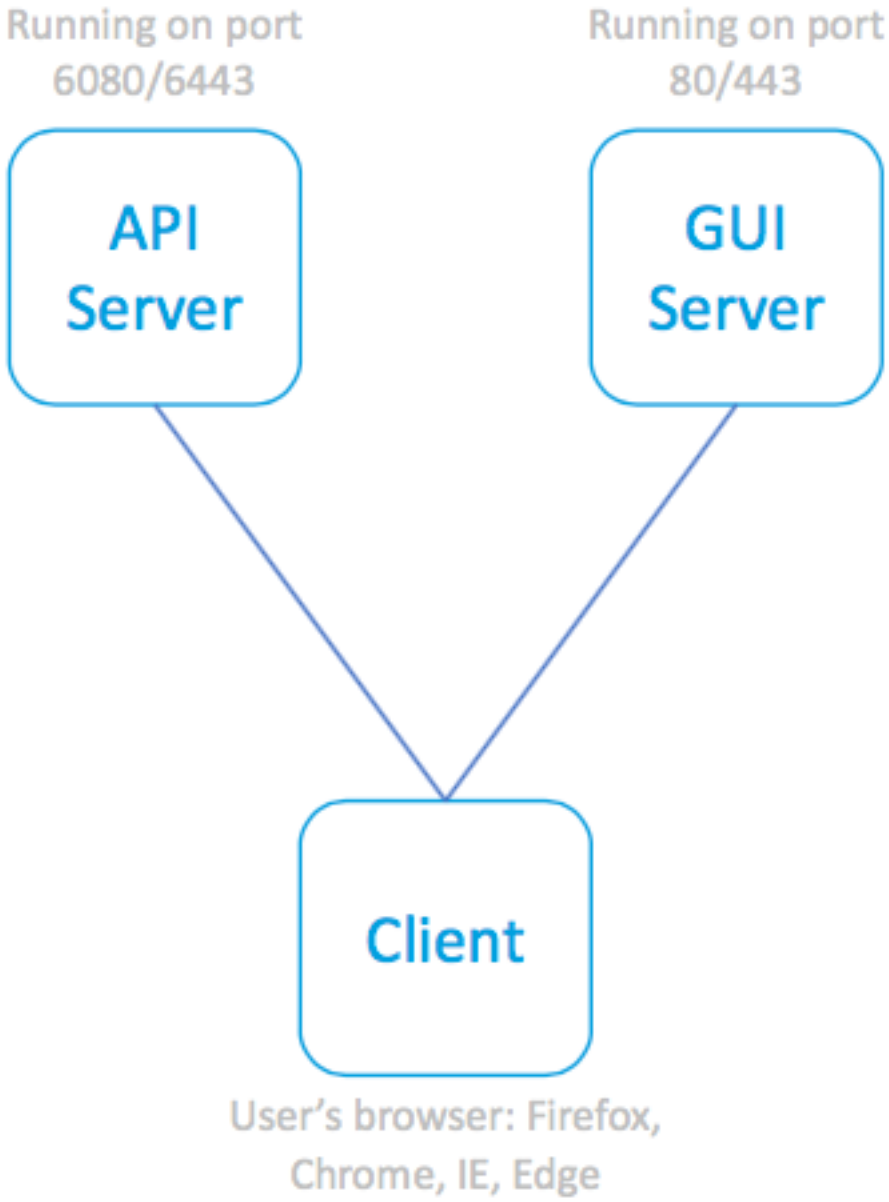
これにより、通信が1つの通信ストリームと証明書受け入れに集約されます。

シスコでは、この機能をtrailblazerconfigとして有効にするCLIコマンドにラベルを付**けています**。

最初の図は、2つの現在のサーバの例を示しています。

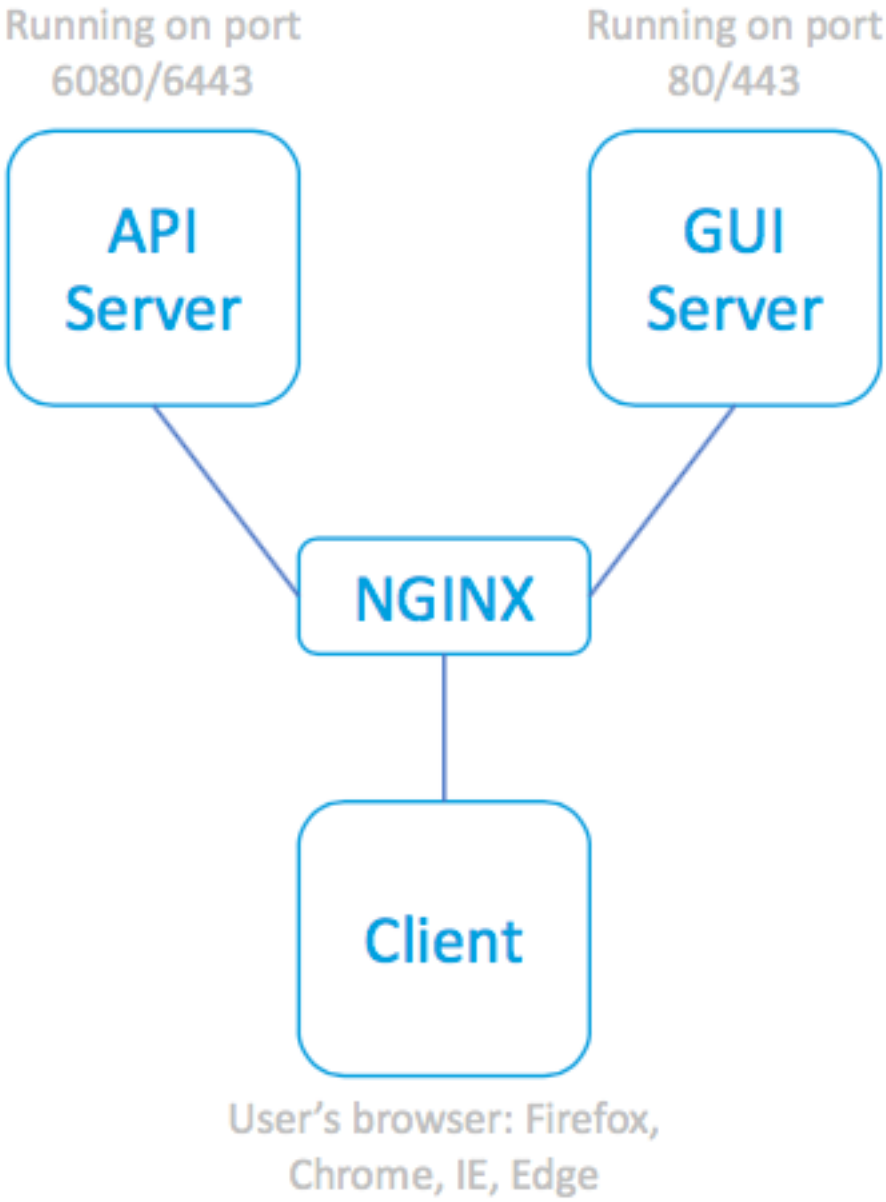
- API Server HTTP:6080およびHTTPS:6443
- GUIサーバHTTP:80およびHTTPS:443

GUIからAPIへの通信を承認するには、承認とポートアクセスが必要です。



SPAおよび関連サーバ

次の図では、APIおよびGUIプロセスの前にNginxプロキシが組み込まれており、通信の制限の心配がなくなります。



SPA（NGINXプロキシを使用して関連サーバに到達）

コマンドラインの例

フルヘルプ：

```
sma.local> help trailblazerconfig

trailblazerconfig

   Configure and check the trailblazer.
(Please make sure existing UI is functioning on https)
   trailblazerconfig enable <https_port> <http_port>
   trailblazerconfig disable
   trailblazerconfig status

   Sub-commands:
       enable          - Runs the trailblazer either on
                         default ports (https_port: 4431 and http_port: 801)
```

```
                    or optionally specified https_port and http_port
      disable       - Disable the trailblazer
      status        - Check the status of trailblazer

   Options:
      https_port    - HTTPS port number, Optional
      http_port     - HTTP port number, Optional
```

ステータスの確認：

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Enable:

```
sma.local> trailblazerconfig enable

trailblazer is enabled.
To access the Next Generation web interface, use the port 4431 for HTTPS.
```

イネーブルステータスを確認します。

```
sma.local> trailblazerconfig status

trailblazer is running with https on port 4431.
```

ネーミング構文の例

trailblazerが有効なWebアクセスには、URLアドレス内のtrailblazerポートが含まれます。

- NGSMA管理ポータルは次のように表示されます。https://hostname:4431/ng-login
- NGSMAエンドユーザ隔離(ISQ)ポータルは次のように表示されます。
  https://hostname:4431/euq-login

トラブルシューティング

一部の実装では、スパム通知のセカンダリインターフェイスに焦点を当てています。管理インターフェイス「ホスト名」がDNSで解決できない場合(**nslookupホスト名など**)、trailblazerは初期化に失敗します。

サービスを即時に確認して復元する1つのアクションは、解決できるホスト名を管理インターフェイスに追加することです。（次に、指定されたホスト名を正しく解決するためのAレコードを作成します）。

ユーザ側のセキュリティ制限により、ユーザ環境からSMA 4431 TCPポートへのアクセスが防止されます。

1. ポートがブラウザで使用可能であることを確認するためのテスト
2. ホスト名とポートを次のように入力します。
   https://hostname:4431

TCPポート443が開いていません

- **IE11:このページは表示できません**
- **Chrome:このサイトにはアクセスできません。接続が拒否されました**
- **Firefox：接続できない**

TCPポート4431が開き、証明書が受け入れられま

- **IE:HTTP 406**
- **Chrome:{"error":{「メッセージ」:「Unauthorized.」、「code」:「401」、「説明:"401 =アクセス許可がありません。許可スキを参照してください。"}}**
- **Firefox：証明書プロンプト(ACCEPT)。Firefox：post certificate acceptance > [Unauthorized]を選択します。 401**

正しいURL構文：

- 非trailblazer対応システムでは、名前にポート4431は使用されません。
  https://hostname/ng-login

  -or- https:// *hostname*/euq-login

- Trailblazer対応システムの名前には、ポート番号4431が含まれます。
  https://hostname:4431/ng-login

  -or- https:// *hostname*:4431/euq-login