Administrative Details zum CLI-Befehl "trailblazer" für die Cisco Security Management Appliance (SMA)

Inhalt

Einführung

Beginnend mit AsyncOS 11.4 und der Fortsetzung von AsyncOS 12.x für Security Management Appliance (SMA) wurde die Webbenutzeroberfläche (UI) neu konzipiert und die interne Verarbeitung der Daten durchgeführt. Der Schwerpunkt dieses Artikels liegt auf Änderungen bei der Möglichkeit, die neu überarbeitete Web-Benutzeroberfläche zu durchsuchen. Durch die Implementierung eines technologisch fortschrittlicheren Designs hat Cisco das Anwendererlebnis verbessert.

Mitarbeiter: Chris Arellano, Cisco TAC Engineer.

Voraussetzungen

Hinweis: Die "Management"-Schnittstelle ist die Standardschnittstelle, die bei der ersten Konfiguration auf dem SMA angezeigt wird. Von **Netzwerk > IP-Schnittstellen** aus ist das Löschen nicht zulässig. Aus diesem Grund ist es immer die Standardschnittstelle, die Dienste überprüft werden.

Stellen Sie sicher, dass die folgenden Elemente überprüft wurden, bevor Sie **trailblazerconfig** aktivieren:

1. SMA wurde aktualisiert und führt AsyncOS-Version 12.x (oder höher) aus.
2. Über **Netzwerk > IP-Schnittstellen** ist **Appliance Management > HTTPS** aktiviert. **Appliance-Management > HTTPS**-Port muss in der Firewall geöffnet werden
3. Von **Netzwerk > IP-Schnittstellen** ist **AsyncOS API > HTTP** und **AsyncOS > HTTPS** beide aktiviert. **AsyncOS-API > HTTP** und **AsyncOS-API > HTTPS**-Ports müssen in der Firewall geöffnet werden
4. Der "Trailblazer"-Port muss über die Firewall geöffnet werden. Der Standardwert ist 4431.
5. Stellen Sie sicher, dass DNS die Management-Schnittstelle "Hostname" auflösen kann. d. h., **nslookup** ***sma.hostname*** gibt eine IP-Adresse zurück

6. Stellen Sie sicher, dass DNS den für den Zugriff auf die Spam-Quarantäne konfigurierten Hostnamen/URL "*This is the default interface for the Spam Quarantine*" auflösen kann.

Warum

Die 12.x Next Generation SMA (NGSMA)-GUI wurde als Single Page Application (SPA) neu implementiert, die auf den Client (IE, Chrome, Firefox) heruntergeladen wird, um die Benutzerfreundlichkeit zu verbessern. Der SPA kommuniziert mit den verschiedenen internen Servern der SMA, die jeweils einen anderen Service ausführen.

CORS (Cross-Origin Resource Sharing)-Beschränkungen innerhalb der SPA-Kommunikation mit der SMA verursachen einige Hindernisse für die Kommunikation zwischen den verschiedenen Modulen.

- CORS ist eine Sicherheitsfunktion, die verhindert, dass bösartige Befehle innerhalb einer etablierten Kommunikationsleitung zu einem anderen internen Dienst ausgeführt werden.

Die internen Server sind über verschiedene nummerierte TCP-Ports über die NGSMA erreichbar. Jeder TCP-Port benötigt eine separate Zertifikatsgenehmigung, um mit dem Client zu kommunizieren. Eine unzureichende Kommunikation mit den internen Servern der NGSMA ist problematisch.

Auswirkungen

Die Webschnittstellen der nächsten Generation umfassen "/euq-login" und "ng-login".

Bericht zur Integration von AMP Cisco Threat Response (CTR).

Lösung

Das einfache Beispiel für TCP-Ports, die verschiedene Module darstellen, erfordert die Zertifikatsakzeptanz für jeden Port. Wenn für die SMA kein vertrauenswürdiges signiertes Zertifikat vorhanden ist, sind mehrere Zertifikatsakzepte erforderlich, wenn der Browser eine transparente Kommunikation mit den Modulen initiiert. Für Benutzer, die die Notwendigkeit der TCP-Ports 6443, 443, 4431 möglicherweise nicht verstehen, kann diese Erfahrung zu Verwirrung führen.

Um diese Herausforderungen zu überwinden, hat Cisco Nginx implementiert, um eine Proxyfunktion zwischen dem Client (Browser-Client) und den Servern (Services, die über bestimmte Ports erreichbar sind) auszuführen. Nginx (stylisiert als NGINX oder Nginx) ist ein Webserver, der auch als Reverse Proxy, Load Balancer, Mail-Proxy und HTTP-Cache verwendet werden kann.

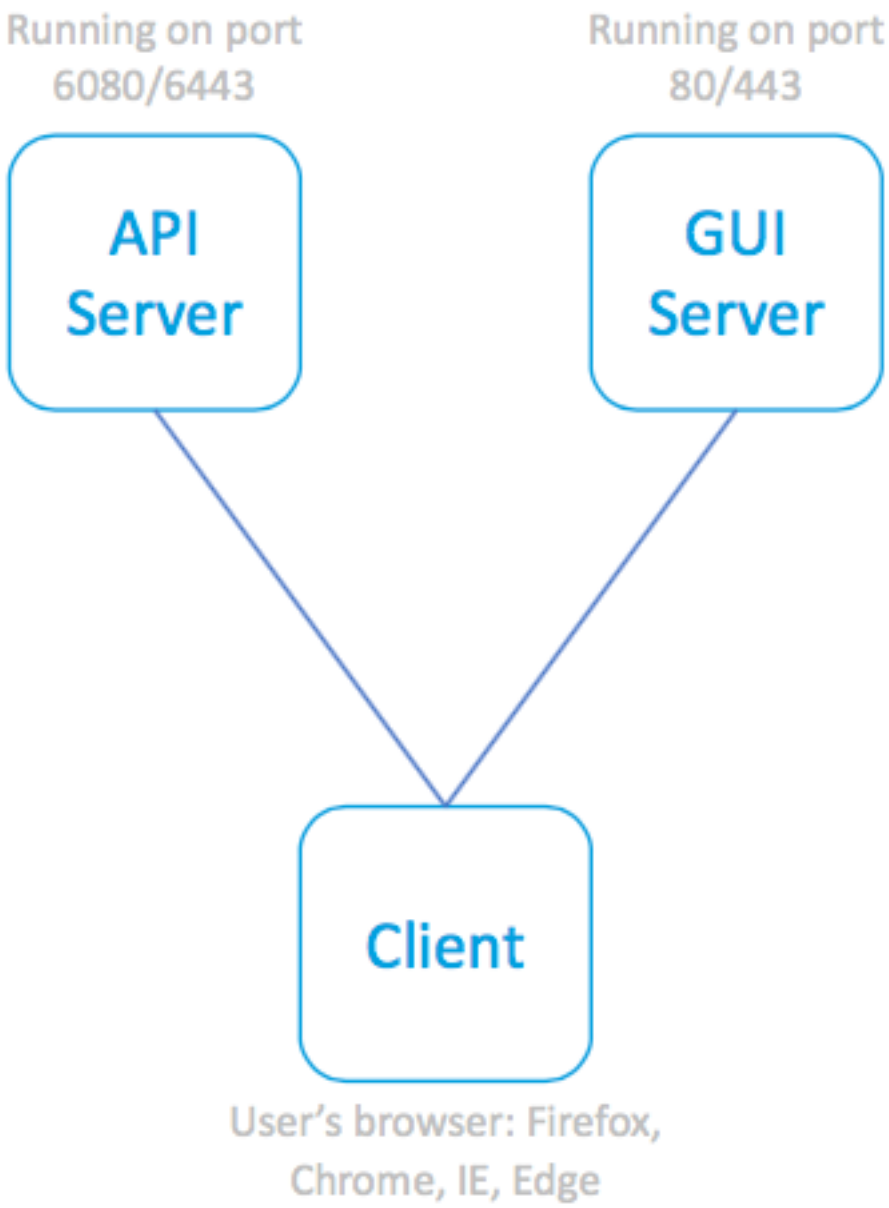
Dadurch wird die Kommunikation zu einem einzigen Kommunikationsstream und einer Zertifikatsakzeptanz zusammengefasst.

Cisco hat den CLI-Befehl als **trailblazerconfig** bezeichnet.

In der ersten Abbildung wird ein Beispiel für zwei aktuelle Server angezeigt:

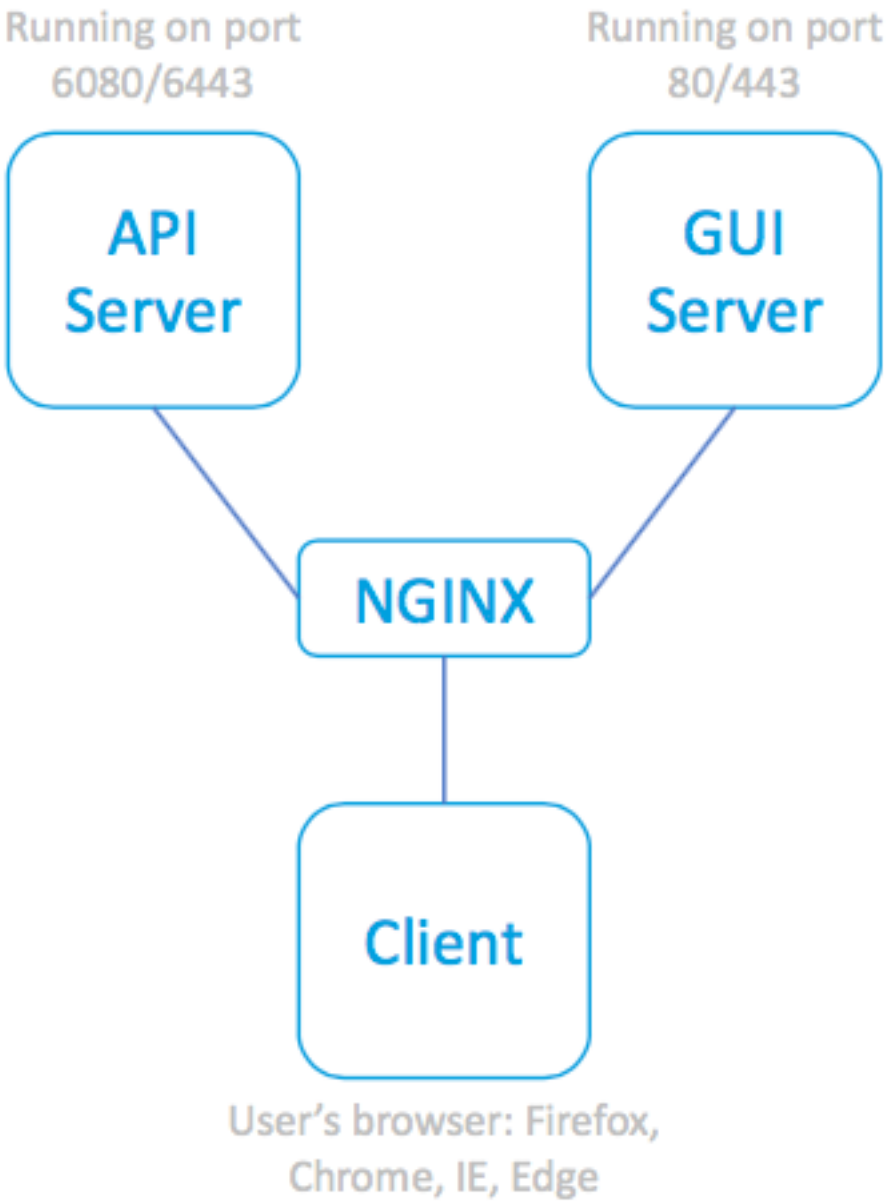
- API-Server HTTP:6080 und HTTPS:6443
- GUI-Server HTTP:80 und HTTPS:443

Für die Genehmigung der Kommunikation von der GUI zur API sind Genehmigungen und Port-Zugriff erforderlich.



SPA und zugehörige Server

Die nächste Abbildung enthält den Nginx-Proxy vor API- und GUI-Prozessen, wodurch die Bedenken bei eingeschränkter Kommunikation wegfallen.



SPA, wobei der NGINX-Proxy zum Erreichen der verknüpften Server verwendet wird

Befehlszeilenbeispiele

Vollständige Hilfe:

```
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
```

Status überprüfen:

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Aktivieren:

```
sma.local> trailblazerconfig enable

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

Status nach der Aktivierung überprüfen:

```
sma.local> trailblazerconfig status

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

Beispielbenennungssyntax

Der Webzugriff mit aktiviertem Trailblazer umfasst den trailblazer-Port in der URL-Adresse:

- Das NGSMA-Managementportal erscheint wie folgt: https://*Hostname*:4431/ng-login
- Das NGSMA-Endbenutzer-Quarantäneportal (ISQ) wird angezeigt als: https://*Hostname*:4431/euq-login

Fehlerbehebung

Einige Implementierungen konzentrieren sich auf die sekundäre Schnittstelle für Spam-Benachrichtigungen. Wenn die Management-Schnittstelle "hostname" im DNS nicht auflösbar ist (z. B. **nslookup *hostname***), kann trailblazer nicht initialisiert werden.

Eine Aktion zur sofortigen Bestätigung und Wiederherstellung des Diensts besteht darin, der Verwaltungsschnittstelle einen auflösbaren Hostnamen hinzuzufügen. (Erstellen Sie dann einen A-Datensatz, um den angegebenen Hostnamen korrekt aufzulösen.)

Sicherheitsbeschränkungen auf Benutzerseite verhindern den Zugriff von der Benutzerumgebung auf den SMA 4431 TCP-Port:

1. Stellen Sie sicher, dass der Port für den Browser verfügbar ist.
2. Geben Sie den Hostnamen und den Port wie folgt ein: https://*Hostname*:4431

TCP-Port 443 nicht geöffnet

- IE11: Diese Seite kann nicht angezeigt werden.
- Chrome: Diese Seite kann nicht erreicht werden. Verbindung verweigert
- Firefox: Verbindung kann nicht hergestellt werden

TCP-Port 4431 offen und Zertifikat akzeptiert

- IE: HTTP 406
- Chrome:{"Fehler": {"Message": "Unauthorized "Code": "401", "Erklärung": "401 = Keine Genehmigung — siehe Autorisierungsschem
- Firefox: Eingabeaufforderung (AKZEPTIERE Firefox: die Annahme des Zertifikats bestätig "Unauthorized". 401

Korrekte URL-Syntax:

- Nicht-Trailblazer-fähige Systeme verwenden im Namen nicht Port 4431: https://*Hostname*/ng-login

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

- Trailblazer-fähige Systeme tragen die Portnummer 4431 im Namen: https://*Hostname*:4431/ng-login

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