Administrative details on 'trailblazer' CLI command for Cisco Security Management Appliance (SMA)

Contents

[Introduction](#)
[Prerequisites](#)
[Why](#)
[Impact](#)
[Solution](#)
[Command Line Examples](#)
[Sample Naming Syntax](#)
[Troubleshooting](#)

Introduction

Starting with AsyncOS 11.4 and continuing with [AsyncOS 12.x for Security Management Appliance (SMA)](#), the web user interface (UI) has undergone a redesign as well as the internal processing of data. The focus of this article addresses changes in the ability to browse the newly redesigned web user interface. The implementation of a more technologically advanced design, Cisco has worked to improve the user experience.

Contributed by Chris Arellano, Cisco TAC Engineer.

Prerequisites

Note: The "Management" Interface is the default interface, presented during the first configuration on the SMA. From **Network > IP Interfaces**, It does not allow deletion. For this reason, it will always be the default interface which services will be verified.

Ensure the following items have been verified prior to enabling **trailblazerconfig**:

1. SMA has been upgraded and is running AsyncOS version 12.x (or newer)
2. From **Network > IP Interfaces**, the Management interface has **Appliance Management > HTTPS** enabled **Appliance Management > HTTPS** port must be opened on firewall
3. From **Network > IP Interfaces**, the Management Interface has **AsyncOS API > HTTP** and **AsyncOS > HTTPS** both enabled. **AsyncOS API > HTTP** and **AsyncOS API > HTTPS** ports must be opened on firewall
4. The "Trailblazer" port must be opened through the firewall Default is 4431
5. Ensure DNS can resolve the Management Interface "Hostname"
   i.e., **nslookup *sma.hostname*** returns an IP address
6. Ensure DNS can resolve the "*This is the default interface for the Spam Quarantine*" hostname/URL configured to access the Spam Quarantine

Why

The 12.x Next Generation SMA (NGSMA) GUI has been re-implemented as a Single Page Application (SPA) which gets downloaded onto the Client (IE, Chrome, Firefox) to improve user experience. The SPA communicates across to the SMA's multiple internal servers, each performing a different service.

CORS (Cross-Origin Resource Sharing) restrictions within the SPA communication to the SMA cause some obstacles to communication between the multiple modules.

- CORS is a security feature designed to prevent malicious commands from executing within an established line of communication to another internal service.

The internal servers are reachable through different numbered TCP ports via the NGSMA. Each TCP port requires a separate certificate approval to communicate to the Client. Insufficient ability to communicate to the NGSMA's internal servers presents a problem.

Impact

The Next Generation Web Interfaces including "/euq-login" and "ng-login".

Report for AMP Cisco Threat Response (CTR) integration.

Solution

The simple example of TCP ports representing different modules requires the certificate acceptance for each port. If a trusted signed certificate does not exist on the SMA, then multiple certificate acceptances are required as the browser initiates transparent communication to the modules. To a user who may not understand the need for TCP Ports 6443, 443, 4431, the experience may potentially cause confusion.

To move beyond these challenges, Cisco has implemented Nginx to perform a proxy function between the client (browser client) and the servers (services reachable via specific ports). Nginx (stylized as NGINX or nginx) is a web server which can also be used as a reverse proxy, load balancer, mail proxy and HTTP cache.

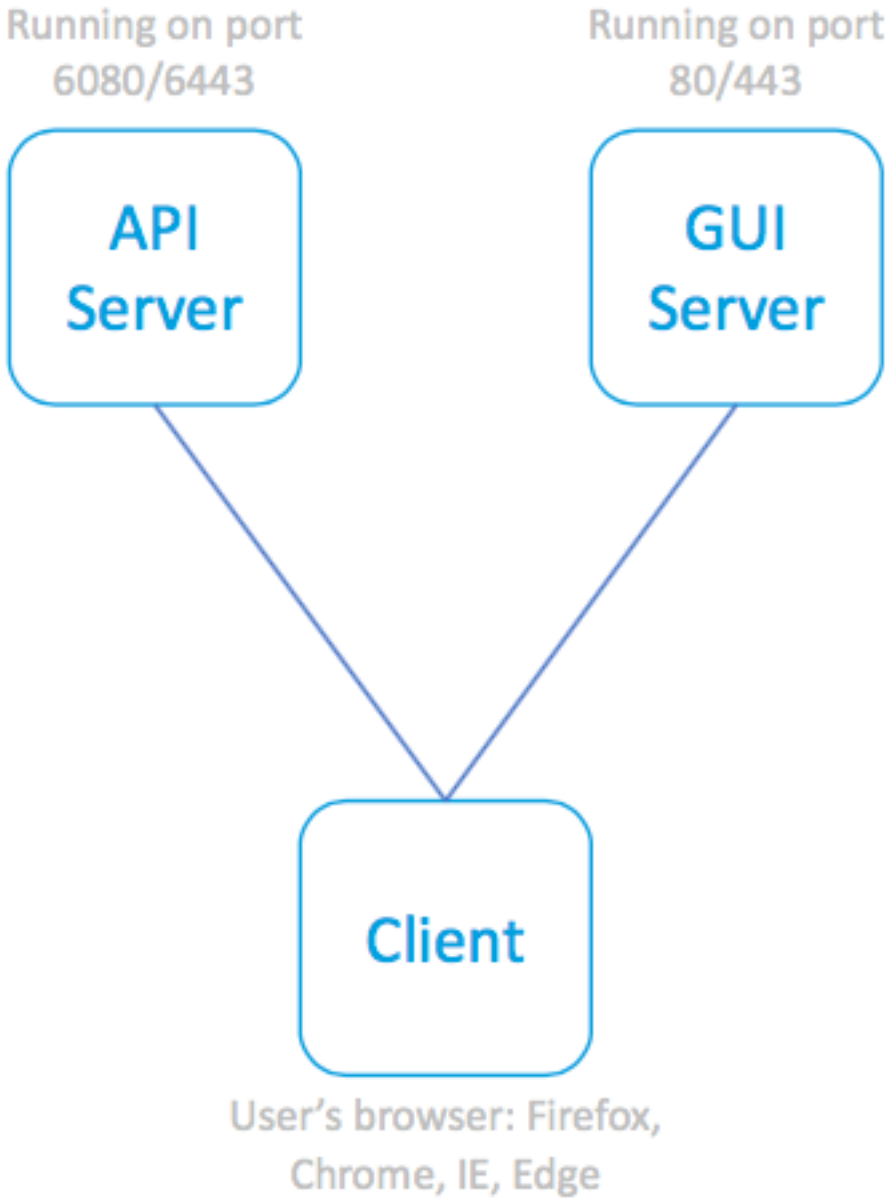
This condenses the communication to a single communication stream and certificate acceptance.

Cisco has labeled the CLI command to enable this functionality as **trailblazerconfig**.

The first illustration displays an example of two current servers:

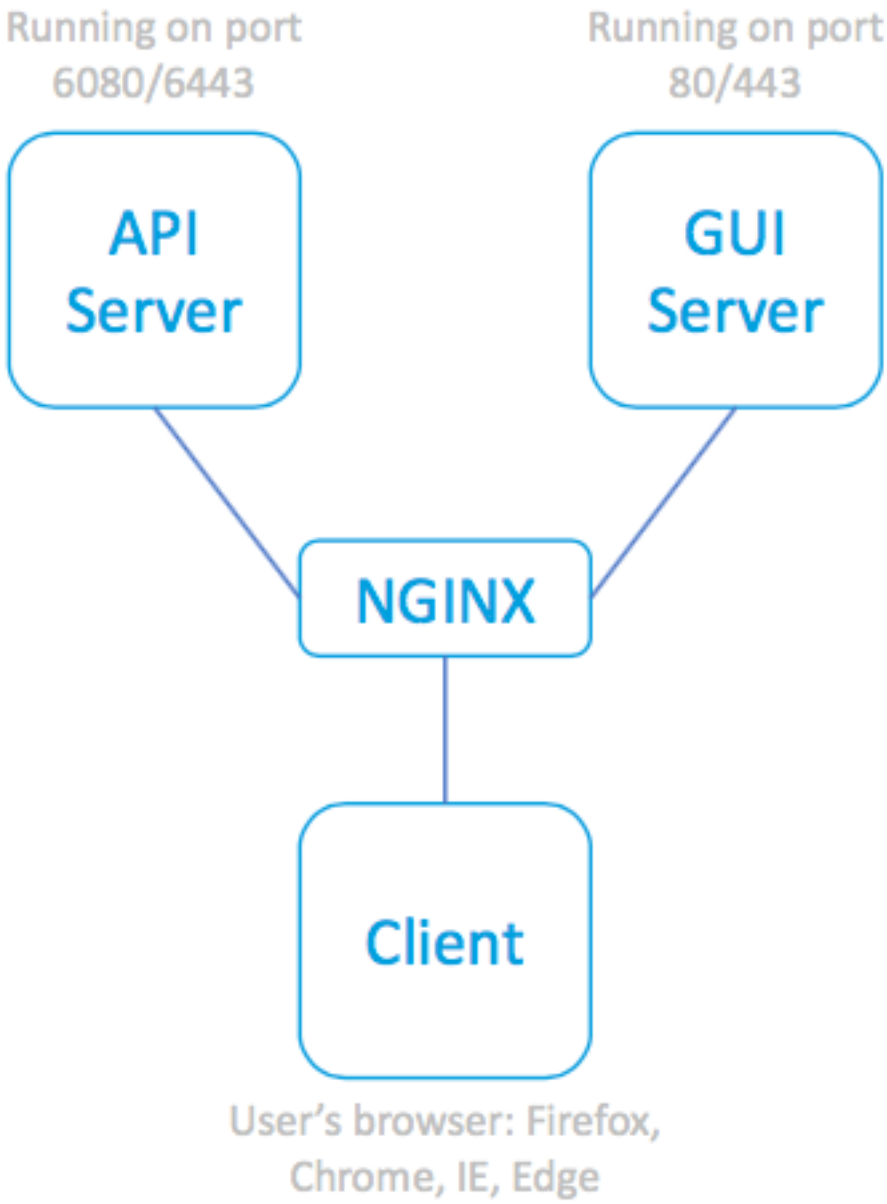
- API Server HTTP:6080 and HTTPS:6443
- GUI Server HTTP:80 and HTTPS:443

Approving communication from the GUI to the API requires approval and port access.



SPA and associated servers

The next illustration incorporates the Nginx proxy in front of the API and GUI Processes - eliminating the concern of restricted communications.



SPA, utilizing NGINX Proxy to reach the associated servers

Command Line Examples

Full help:

```
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
```

Check status:

```
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.
```

Post-enable, check status:

```
sma.local> trailblazerconfig status

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

Sample Naming Syntax

The trailblazer enabled web access would include the trailblazer port within the URL Address:

- The NGSMA Management portal would appear as: https://*hostname*:4431/ng-login
- The NGSMA End User Quarantine (or ISQ) portal would appear as: https://*hostname*:4431/euq-login

Troubleshooting

Some implementations focus on the secondary interface for spam notifications. IF the Management Interface "hostname" is not resolvable in DNS (i.e., **nslookup *hostname***), then trailblazer will fail to initialize.

One action to immediately confirm and restore service is to add a resolvable hostname to the management interface. (Then create an A record to correctly resolve the designated hostname.)

User-side security restrictions prevent access from the user environment towards the SMA 4431 TCP Port:

1. Test to ensure the port is available to the browser
2. Enter the hostname and port as: https://*hostname*:4431

TCP Port 443 not open

TCP Port 4431 open and certificate accepted

- **IE11: This Page can't be displayed**
- **Chrome: This site can't be reached. Refused to connect**
- **Firefox: Unable to Connect**

- **IE: HTTP 406**
- **Chrome:{"error": {"message": "Unauthori "code": "401", "explanation": "401 = No permission -- see authorization schemes."**
- **Firefox: Certificate Prompt (ACCEPT). Fir post certificate acceptance > "Unauthoriz 401**

Correct URL Syntax:

- Non-trailblazer enabled systems will not use port 4431 in the name: https://*hostname*/ng-login

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

- Trailblazer enabled systems will include port number 4431 in the name: https://*hostname*:4431/ng-login

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