Détails administratifs sur la commande CLI « trailblazer » pour Cisco Security Management Appliance (SMA)

Contenu

Introduction

Àpartir de AsyncOS 11.4 et en continuant avec AsyncOS 12.x pour l'appliance de gestion de la sécurité (SMA), l'interface utilisateur Web (UI) a subi une reconception ainsi que le traitement interne des données. L'objet de cet article porte sur les modifications apportées à la capacité de naviguer dans l'interface utilisateur Web récemment reconçue. La mise en oeuvre d'une conception plus avancée sur le plan technologique a permis à Cisco d'améliorer l'expérience utilisateur.

Contribué par Chris Arellano, ingénieur TAC Cisco.

Conditions préalables

Remarque : l'interface de gestion est l'interface par défaut, présentée lors de la première configuration sur le SMA. Dans **Network > IP Interfaces**, il n'autorise pas la suppression. Pour cette raison, ce sera toujours l'interface par défaut qui vérifiera les services.

Assurez-vous que les éléments suivants ont été vérifiés avant d'activer la **configuration de semi-blazerconfig** :

1. SMA a été mis à niveau et exécute AsyncOS version 12.x (ou ultérieure)
2. Àpartir de **Network > IP Interfaces**, l'interface de gestion a **Appliance Management > HTTPS** activé **Gestion de l'appareil > Le** port **HTTPS** doit être ouvert sur le pare-feu
3. Àpartir de **Network > IP Interfaces**, l'interface de gestion a **AsyncOS API > HTTP** et **AsyncOS > HTTPS** toutes deux activées. **API AsyncOS > API HTTP** et **AsyncOS > Les** ports **HTTPS** doivent être ouverts sur le pare-feu
4. Le port Trailblazer doit être ouvert via le pare-feu Le défaut est 4431
5. Assurez-vous que DNS peut résoudre l'interface de gestion « Nom d'hôte » par exemple, **nslookup** ***sma.hostname*** retourne une adresse IP
6. Assurez-vous que DNS peut résoudre l'*interface par défaut de la quarantaine du spam*, nom

d'hôte/URL configuré pour accéder à la quarantaine du spam

Pourquoi ?

L'interface utilisateur graphique SMA nouvelle génération 12.x (NGSMA) a été réimplémentée en tant qu'application sur une seule page (SPA) qui est téléchargée sur le client (IE, Chrome, Firefox) pour améliorer l'expérience utilisateur. Le SPA communique entre les différents serveurs internes du SMA, chacun exécutant un service différent.

Les restrictions CORS (Cross-Origin Resource Sharing) au sein de la communication SPA vers SMA empêchent la communication entre les différents modules.

- CORS est une fonctionnalité de sécurité conçue pour empêcher l'exécution de commandes malveillantes dans une ligne de communication établie vers un autre service interne.

Les serveurs internes sont accessibles via différents ports TCP numérotés via le NGSMA. Chaque port TCP nécessite une approbation de certificat distincte pour communiquer au client. L'incapacité à communiquer avec les serveurs internes du NGSMA pose un problème.

Incidence

Les interfaces Web de nouvelle génération incluant "/euq-login » et « ng-login ».

Rapport sur l'intégration d'AMP Cisco Threat Response (CTR).

Solution

L'exemple simple de ports TCP représentant différents modules nécessite l'acceptation du certificat pour chaque port. Si un certificat signé approuvé n'existe pas sur le SMA, plusieurs acceptations de certificat sont requises lorsque le navigateur initie une communication transparente avec les modules. Pour un utilisateur qui ne comprend peut-être pas la nécessité des ports TCP 6443, 443, 4431, cette expérience peut être source de confusion.

Pour aller au-delà de ces défis, Cisco a mis en oeuvre Nginx pour exécuter une fonction de proxy entre le client (client de navigateur) et les serveurs (services accessibles via des ports spécifiques). Nginx (stylisé NGINX ou nginx) est un serveur web qui peut également être utilisé comme proxy inverse, équilibreur de charge, proxy de messagerie et cache HTTP.

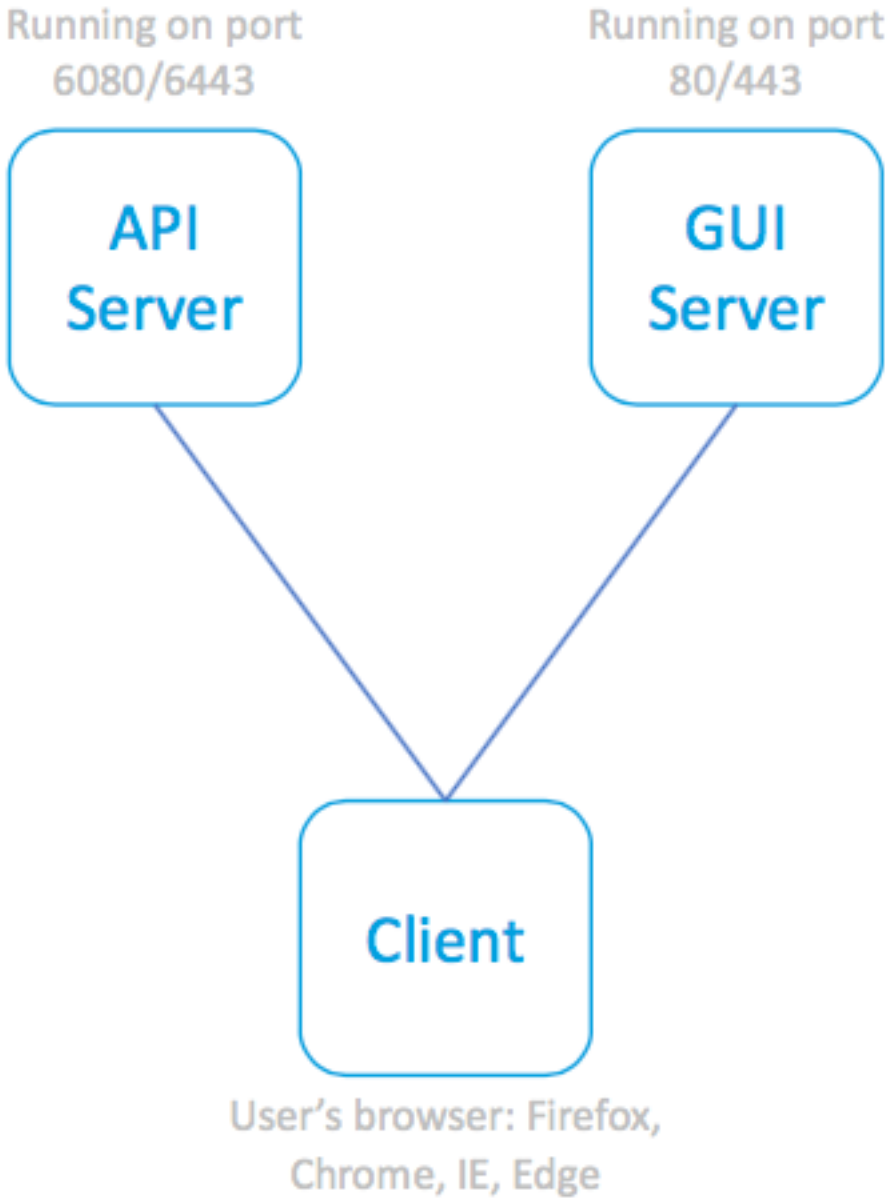
Ceci confirme la communication à un seul flux de communication et l'acceptation du certificat.

Cisco a défini la commande CLI pour activer cette fonctionnalité comme **semi-blazerconfig**.

La première illustration présente un exemple de deux serveurs actuels :

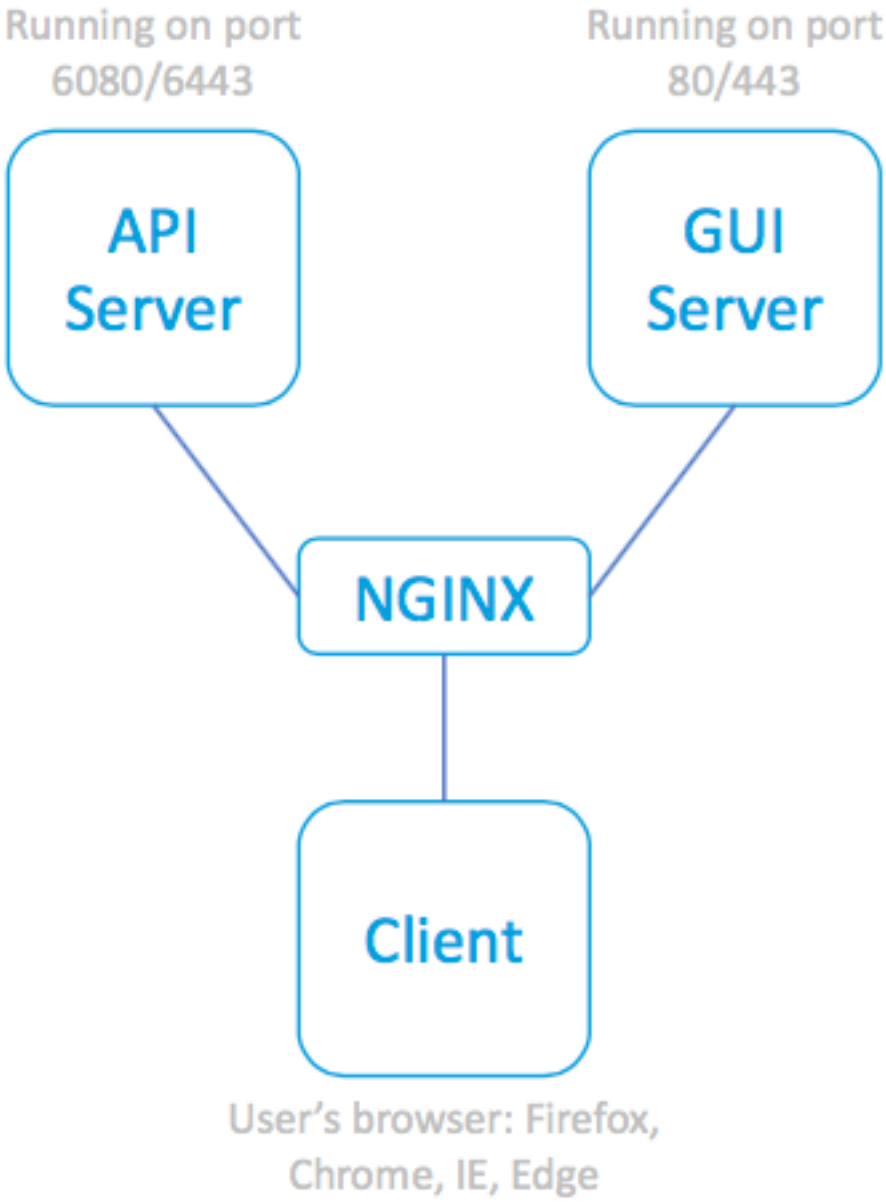
- Serveur API HTTP:6080 et HTTPS:6443
- Serveur GUI HTTP:80 et HTTPS:443

L'approbation de la communication de l'interface utilisateur graphique à l'API nécessite l'approbation et l'accès aux ports.



SPA et serveurs associés

L'illustration suivante incorpore le proxy Nginx devant les processus API et GUI, éliminant ainsi les problèmes de communication restreinte.



SPA, utilisation du proxy NGINX pour atteindre les serveurs associés

Exemples de ligne de commande

Aide complète :

```
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
```

État de la vérification :

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Activer :

```
sma.local> trailblazerconfig enable

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

Post-activation, état de la vérification :

```
sma.local> trailblazerconfig status

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

Exemple de syntaxe de nom

L'accès Web activé pour le semi-conducteur inclurait le port du semi-conducteur dans l'adresse URL :

- Le portail de gestion NGSMA apparaît comme suit : https://hostname:4431/ng-login
- Le portail de quarantaine de l'utilisateur final (ou ISQ) NGSMA apparaît comme suit : https://hostname:4431/euq-login

Dépannage

Certaines mises en oeuvre se concentrent sur l'interface secondaire pour les notifications de spam. Si le nom d'hôte de l'interface de gestion n'est pas résolvable dans le DNS (c'est-à-dire **nslookup** ***hostname***), le semi-azer ne pourra pas s'initialiser.

Une action pour confirmer et restaurer immédiatement le service consiste à ajouter un nom d'hôte résolvable à l'interface de gestion. (Créez ensuite un enregistrement A pour résoudre correctement le nom d'hôte désigné.)

Les restrictions de sécurité côté utilisateur empêchent l'accès de l'environnement utilisateur vers le port TCP SMA 4431 :

1. Tester pour vérifier que le port est disponible pour le navigateur
2. Entrez le nom d’hôte et le port comme suit :
   https://hostname:4431

Port TCP 443 non ouvert

- IE11 : Impossible d'afficher cette page
- Chrome : Impossible d'accéder à ce site. Refusé de connexion
- Firefox : Impossible de se connecter

Port TCP 4431 ouvert et certificat accepté

- IE : HTTP 406
- Chrome :{« erreur » : {« message » : « Non autorisé. », « code » : « 401 », « explication » 401 = Aucune autorisation — voir les schéma d'autorisation. »}}
- Firefox : Invite de certificats (ACCEPT). Firef validation de l'acceptation du certificat > « No autorisé. » 401

Syntaxe correcte de l'URL :

- Les systèmes qui ne sont pas compatibles avec les semi-conducteurs n'utilisent pas le port 4431 du nom :
  https://hostname/ng-login

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

- Les systèmes compatibles Trailblazer incluent le numéro de port 4431 dans le nom :
  https://hostname:4431/ng-login

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