Administratieve gegevens voor het uitvoeren van een 'trailblazer' CLI-opdracht voor Cisco Security Management-applicatie (SMA)

Inhoud

Inleiding

Om te beginnen met AsyncOS 11.4 en verder te gaan met AsyncOS 12.x voor security Management-applicatie (SMA) heeft de web user interface (UI) een nieuw ontwerp ondergaan evenals de interne verwerking van gegevens. De focus van dit artikel richt zich op veranderingen in het vermogen om door de nieuw opnieuw ontworpen web gebruikersinterface te bladeren. De implementatie van een meer technologisch geavanceerd ontwerp, heeft Cisco gewerkt om de gebruikerservaring te verbeteren.

Bijgedragen door Chris Arellano, Cisco TAC Engineer.

Voorwaarden

Opmerking: de "Management"-interface is de standaardinterface, gepresenteerd tijdens de eerste configuratie op het SMA. Van **Network > IP-interfaces** staat het wissen niet toe. Om deze reden zal het altijd de standaardinstelling zijn die de diensten zullen worden geverifieerd.

Zorg ervoor dat de volgende items zijn geverifieerd voordat u **trailblazerfig** toestaat:

1. SMA is bijgewerkt en wordt uitgevoerd met AsyncOS versie 12.x (of nieuwer)
2. Van **Network > IP-interfaces**, heeft de Management-interface **applicatiebeheer > HTTPS** ingeschakeld **Toepassingsbeheer > HTTPS-**poort moet worden geopend op firewall
3. Van **Network > IP Interfaces**, heeft de Management Interface **AsyncOS API > HTTP** en **AsyncOS > HTTPS** beide ingeschakeld. **AsyncOS API > HTTP** en **AsyncOS API > HTTPS** poorten moeten op firewall worden geopend
4. De poort "Trailblazer" moet via de firewall worden geopend Standaard is 4431
5. Zorg ervoor dat DNS de Management Interface "Hostname" kan oplossen d.w.z., **nslookup** ***sma.hostname*** geeft een IP-adres op
6. Zorg ervoor dat DNS de "*This is the default interface for the Spam Quarantine*" hostname/URL kan oplossen om toegang te krijgen tot de Spam Quarantine

Waarom

De 12.x Next generation SMA (NGSMA) GUI is opnieuw geïmplementeerd als een single-page toepassing (SPA) die gedownload wordt op de client (IE, Chrome, Firefox) om de gebruikerservaring te verbeteren. De SPA communiceert over de meerdere interne servers van de SMA, elk met een andere service.

De beperkingen van het CORS (Cross-Origin Resource Sharing) binnen de SPA-communicatie naar het SMA veroorzaken enkele belemmeringen voor de communicatie tussen de verschillende modules.

- CORS is een beveiligingsfunctie die bedoeld is om te voorkomen dat kwaadaardige opdrachten worden uitgevoerd binnen een vaste communicatielijn naar een andere interne dienst.

De interne servers zijn bereikbaar via verschillende genummerde TCP-poorten via de NGSMA. Elke TCP-poort vereist een afzonderlijke certificatie om te communiceren met de client. Onvoldoende communicatie met de interne servers van NGSMA vormt een probleem.

impact

De volgende generatie web interfaces, inclusief "/euq-login" en "ng-login".

Rapport voor AMP Cisco Threat Response (CTR) integratie.

Oplossing

Het eenvoudige voorbeeld van TCP-poorten die verschillende modules vertegenwoordigen vereist de certificaataanvaarding voor elke poort. Indien er geen betrouwbaar ondertekend certificaat op de SMA bestaat, zijn meerdere certificatenaccepten vereist aangezien de browser een transparante communicatie naar de modules initieert. Aan een gebruiker die misschien niet de behoefte aan TCP-poorten 6443, 443, 4431 begrijpt, kan de ervaring mogelijk verwarring veroorzaken.

Om verder te gaan dan deze uitdagingen, heeft Cisco NGinx geïmplementeerd om een proxy-functie uit te voeren tussen de client (browser client) en de servers (services bereikbaar via specifieke poorten). Nginx (gestileerd als NGINX of nginx) is een webserver die ook kan worden gebruikt als omgekeerde proxy, load balances, mail proxy en HTTP cache.

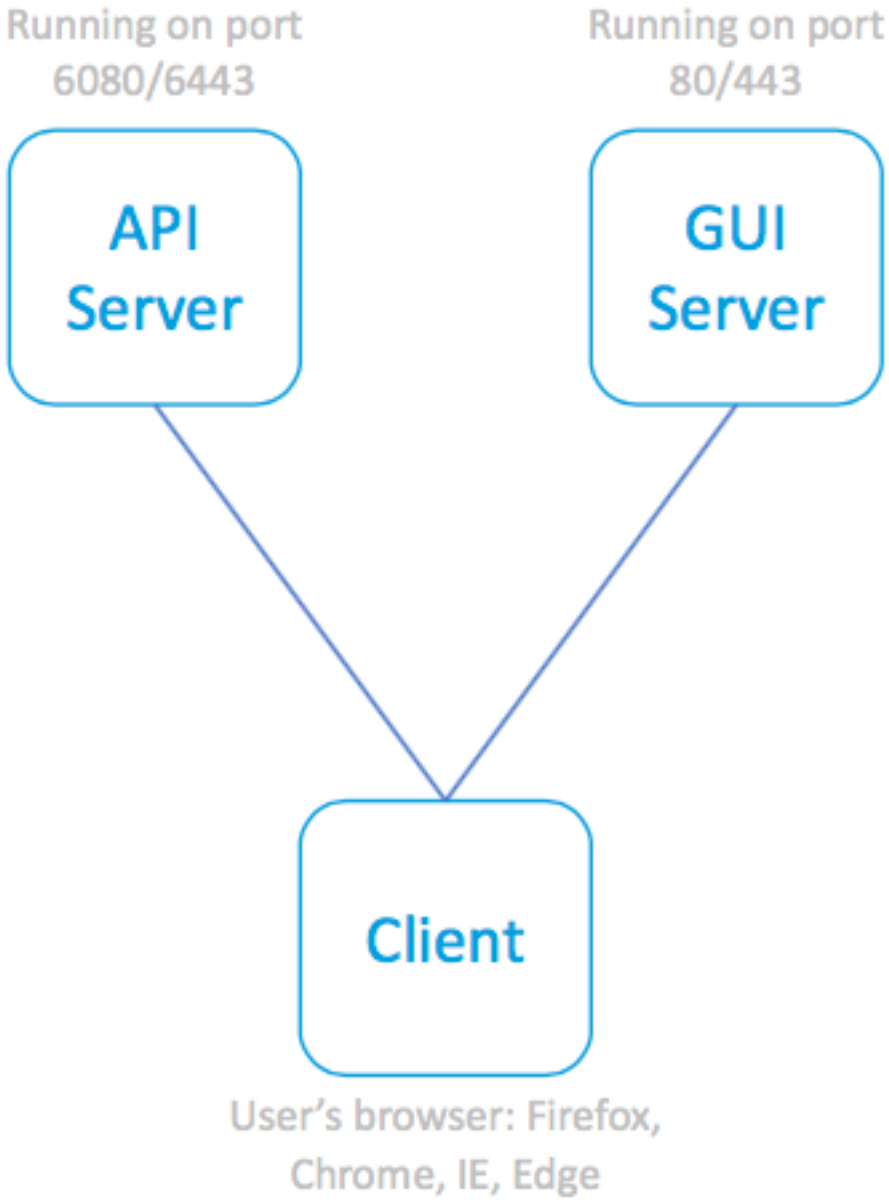
Dit betekent dat de communicatie naar één communicatiestream en één certificaat wordt goedgekeurd.

Cisco heeft de CLI opdracht gelabeld om deze functionaliteit als **trailblazerfig** mogelijk te maken.

In de eerste afbeelding worden twee huidige servers als voorbeeld gegeven:

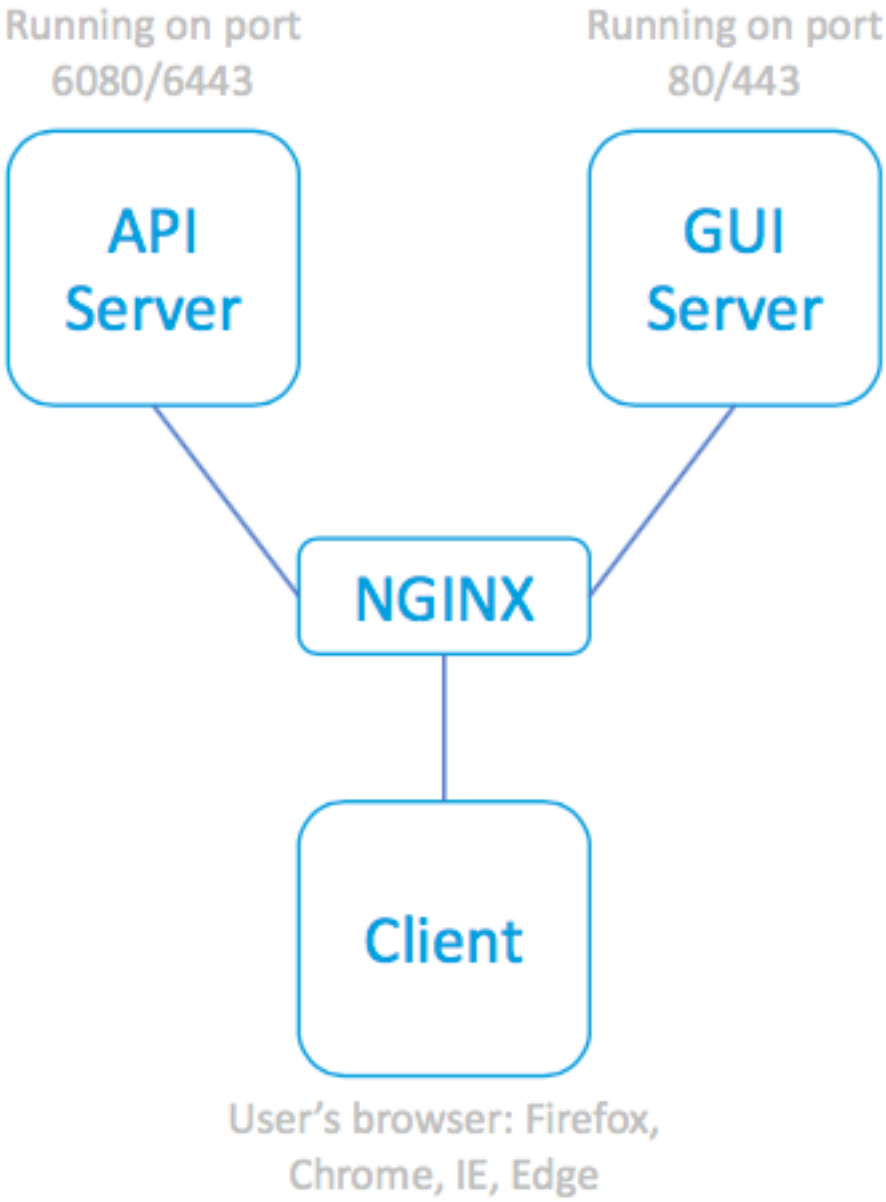
- API-server HTTP:6080 en HTTPS:6443
- GUI-server HTTP:80 en HTTPS:443

Voor het goedkeuren van communicatie van de GUI naar de API is goedkeuring en toegang tot de poort vereist.



SPA en bijbehorende servers

In de volgende illustratie is de NGINX-proxy voor de API- en GUI-processen verwerkt, waardoor de zorg voor beperkte communicatie wordt weggenomen.



SPA, met behulp van NGINX Proxy om de bijbehorende servers te bereiken

Opdrachtlijnvoorbeelden

Volle hulp:

```
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 controleren

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Inschakelen:

```
sma.local> trailblazerconfig enable

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

Controleer na het inschakelen de status:

```
sma.local> trailblazerconfig status

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

Samsung Syntax

De baanbreker enabled web access zou de trainer poort binnen het URL-adres omvatten:

- Het NGSMA-beheerportal verschijnt als volgt: https://hostname:4431/ng-login
- Het NGSMA-portaal met end-user quarantaine (of ISQ) wordt als volgt weergegeven: https://hostname:4431/euq-login

Probleemoplossing

Sommige implementaties zijn gericht op de secundaire interface voor spammeldingen. Als de Management Interface "hostname" niet kan worden opgelost in DNS (d.w.z., **nslookup *hostname***), dan formatteert trailblazer het programma niet.

Eén actie om de service direct te bevestigen en te herstellen is om een oplosbare hostname aan de beheerinterface toe te voegen. (Maak dan een A record om de toegewezen hostname correct op te lossen.)

Gebruikers-kant veiligheidsbeperkingen verhinderen toegang van de gebruikersomgeving tot de SMA 4431 TCP-poort:

1. Test om te waarborgen dat de poort beschikbaar is voor de browser
2. Voer de hostnaam en poort in als:
   https://hostname:4431

TCP-poort 443 niet geopend

- IE11: Deze pagina kan niet worden weergegeven
- Chroom: Deze site is niet bereikbaar. Geen verbinding
- Firefox: Kan geen verbinding maken

TCP-poort 4431 open en geautoriseerd certificaat

- IE: HTTP 406
- Chroom:<"error": {"bericht": "Niet toegestaan. "code": "401", "toelichting": "401 = Geen toestemming — zie vergunningstelsels."}
- Firefox: certificaataanvraag (ACCEPT). Firef aanvaarding van een postcertificaat > "Niet-geautoriseerd". 401

Correcte URL Syntax:

- Niet-trailblazer-enabled-systemen gebruiken poort 4431 niet in de naam: https://hostname/ng-login

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

- Met trailblazer-enabled-systemen zullen port nummer 4431 in de naam opnemen: https://hostname:4431/ng-login

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