Dettagli amministrativi sul comando CLI "trailer" per Cisco Security Management Appliance (SMA)

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Perché](#)
[Conseguenze](#)
[Soluzione](#)
[Esempi di riga di comando](#)
[Sintassi di denominazione di esempio](#)
[Risoluzione dei problemi](#)

Introduzione

A partire dalla versione AsyncOS 11.4 e continuando con AsyncOS 12.x for Security Management Appliance (SMA), l'interfaccia utente Web (UI) è stata riprogettata e sottoposta a un'elaborazione interna dei dati. In questo articolo vengono descritte le modifiche apportate alla possibilità di esplorare l'interfaccia utente Web appena riprogettata. Cisco ha lavorato per migliorare l'esperienza dell'utente nell'implementazione di un design più tecnologicamente avanzato.

Contributo di Chris Arellano, Cisco TAC Engineer.

Prerequisiti

Nota: l'interfaccia di "gestione" è l'interfaccia predefinita, visualizzata durante la prima configurazione sullo SMA. Da **Rete > Interfacce IP**, non consente l'eliminazione. Per questo motivo, sarà sempre l'interfaccia predefinita a verificare i servizi.

Prima di abilitare **Trablazerconfig**, verificare che siano stati verificati i seguenti elementi:

1. SMA è stato aggiornato ed è in esecuzione AsyncOS versione 12.x (o successiva)
2. Da **Rete > Interfacce IP**, l'interfaccia di gestione ha **Gestione accessorio > HTTPS** abilitato **Gestione accessorio >** La porta **HTTPS** deve essere aperta sul firewall
3. Da **Rete > Interfacce IP**, l'interfaccia di gestione ha **AsyncOS API > HTTP** e **AsyncOS > HTTPS** entrambi abilitati. **AsyncOS API > HTTP** e **AsyncOS API >** Le porte **HTTPS** devono essere aperte sul firewall
4. La porta "Trailblazer" deve essere aperta attraverso il firewall Il valore predefinito è 4431
5. Assicurarsi che DNS sia in grado di risolvere l'interfaccia di gestione "Hostname" ad esempio, **nslookup** ***sma.hostname*** restituisce un indirizzo IP
6. Verificare che il DNS sia in grado di risolvere l'URL/nome host "*Questa è l'interfaccia predefinita per la quarantena della posta indesiderata*" configurato per accedere alla

quarantena della posta indesiderata

Perché

La GUI NGSMA (Next Generation SMA) 12.x è stata reimplementata come un'applicazione a pagina singola (SPA) che viene scaricata sul client (IE, Chrome, Firefox) per migliorare l'esperienza utente. L'SP A comunica attraverso i più server interni dell'SMA, ciascuno dei quali esegue un servizio diverso.

Le restrizioni CORS (Cross-Origin Resource Sharing) all'interno della comunicazione SPA allo SMA causano alcuni ostacoli alla comunicazione tra i moduli multipli.

- CORS è una funzionalità di protezione progettata per impedire l'esecuzione di comandi dannosi all'interno di una linea di comunicazione stabilita con un altro servizio interno.

I server interni sono raggiungibili tramite diverse porte TCP numerate tramite NGSMA. Ogni porta TCP richiede un'approvazione separata del certificato per comunicare con il client. L'insufficiente capacità di comunicare con i server interni di NGSMA rappresenta un problema.

Conseguenze

Interfacce Web di nuova generazione, tra cui "/euq-login" e "ng-login".

Report per l'integrazione di AMP Cisco Threat Response (CTR).

Soluzione

Il semplice esempio di porte TCP che rappresentano moduli diversi richiede l'accettazione del certificato per ciascuna porta. Se nell'SMA non esiste un certificato firmato attendibile, sono necessarie più accettazioni di certificati poiché il browser avvia una comunicazione trasparente con i moduli. Per gli utenti che potrebbero non comprendere la necessità delle porte TCP 6443, 443, 4431, l'esperienza potrebbe causare confusione.

Per superare queste sfide, Cisco ha implementato Nginx per eseguire una funzione proxy tra il client (client browser) e i server (servizi raggiungibili tramite porte specifiche). Nginx (stilizzato come NGINX o Nginx) è un server Web che può essere utilizzato anche come proxy inverso, bilanciamento del carico, proxy di posta e cache HTTP.

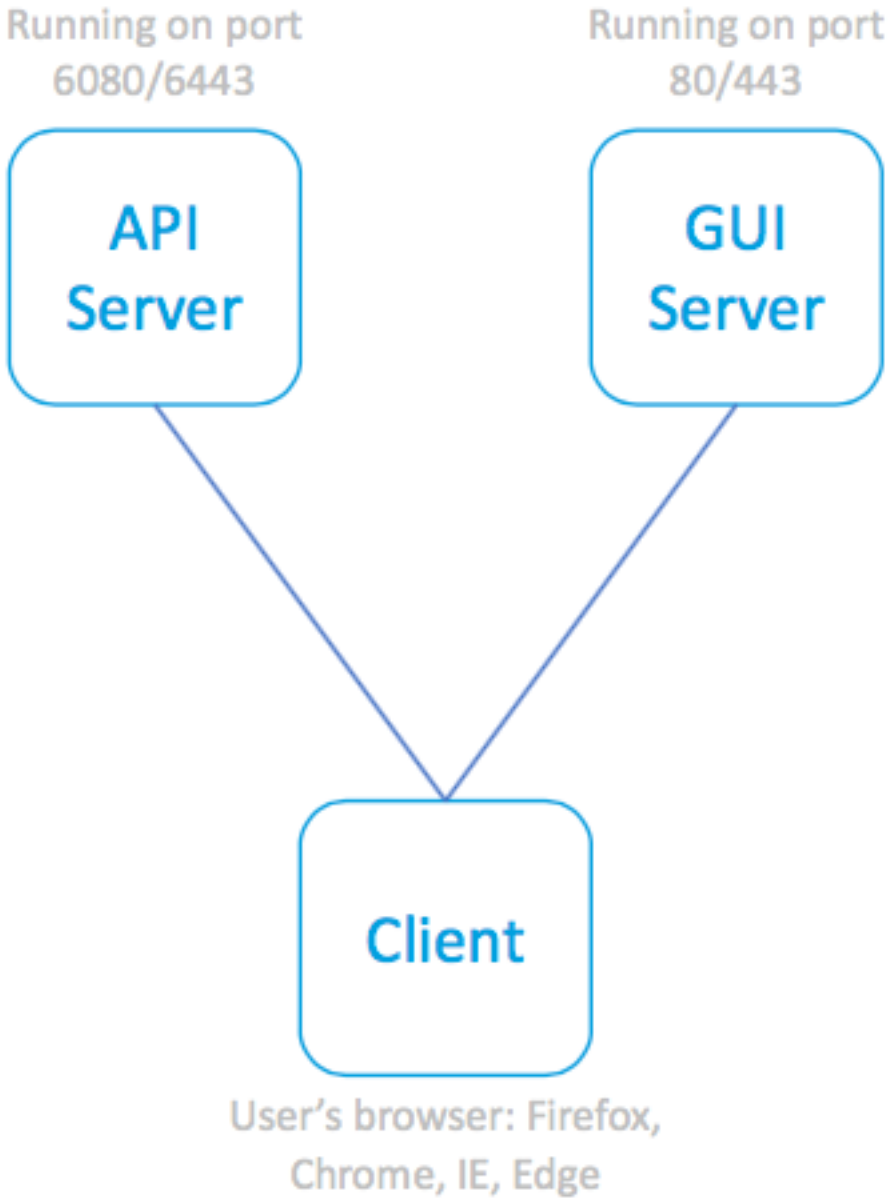
In questo modo la comunicazione viene condensata in un unico flusso di comunicazione e l'accettazione del certificato.

Cisco ha etichettato il comando CLI per abilitare questa funzionalità come **trailer**azerconfig.

La prima illustrazione mostra un esempio di due server correnti:

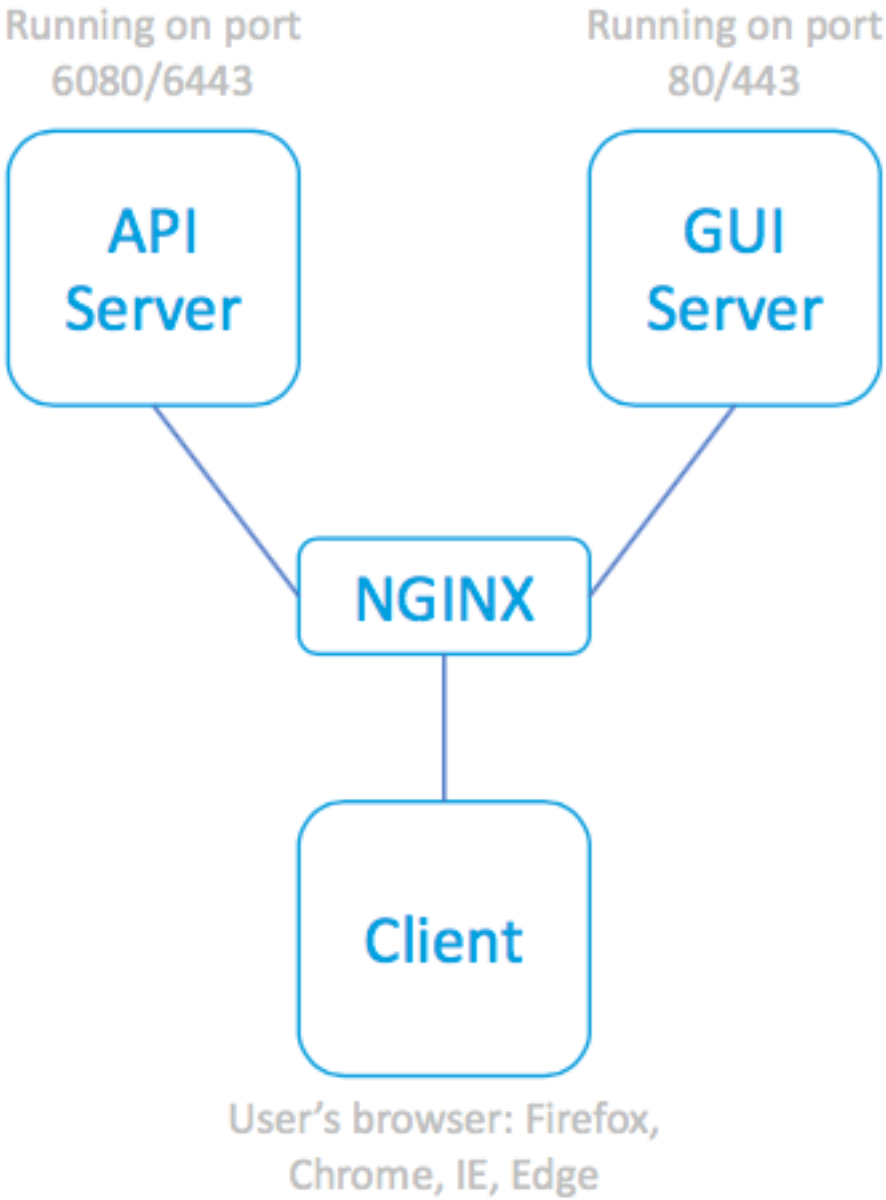
- API Server HTTP:6080 e HTTPS:6443
- GUI Server HTTP:80 e HTTPS:443

L'approvazione della comunicazione dalla GUI all'API richiede l'approvazione e l'accesso alla porta.



SPA e server associati

La figura seguente incorpora il proxy Nginx davanti ai processi API e GUI, eliminando il problema delle comunicazioni limitate.



SPA, utilizzando il proxy NGINX per raggiungere i server associati

Esempi di riga di comando

Guida completa:

```
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
```

Controlla stato:

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Abilita:

```
sma.local> trailblazerconfig enable

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

Post-abilitazione, verifica stato:

```
sma.local> trailblazerconfig status

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

Sintassi di denominazione di esempio

L'accesso Web abilitato per trailer includerà la porta trailer all'interno dell'indirizzo URL:

- Il portale di gestione di NGSMA è il seguente: https://hostname:4431/ng-login
- Il portale NGSMA per la quarantena degli utenti finali (o ISQ) viene visualizzato come segue: https://hostname:4431/euq-login

Risoluzione dei problemi

Alcune implementazioni si concentrano sull'interfaccia secondaria per le notifiche di posta indesiderata. SE l'interfaccia di gestione "hostname" non è risolvibile in DNS (ad esempio, **nslookup *hostname***), l'inizializzazione di trailer non riuscirà.

Per confermare e ripristinare immediatamente il servizio, è possibile aggiungere un nome host risolvibile all'interfaccia di gestione. Quindi, creare un record A per risolvere correttamente il nome host designato.

Le restrizioni di sicurezza lato utente impediscono l'accesso dall'ambiente utente alla porta TCP SMA 4431:

1. Verificare che la porta sia disponibile per il browser
2. Immettere il nome dell'host e la porta come:
   https://hostname:4431

Porta TCP 443 non aperta

- IE11 Impossibile visualizzare la pagina
- Cromatura: Impossibile raggiungere il sito. Rifiutato connessione
- Firefox Impossibile connettersi

Porta TCP 4431 aperta e certificato accettato

- IE: HTTP 406
- Cromo:{"errore": {"messaggio": "Non autorizz "codice": "401", "spiegazione": "401 = Nessu autorizzazione — vedere gli schemi di autorizzazione."}
- Firefox Richiesta certificato (ACCEPT). Firef pubblicare l'accettazione del certificato > "No autorizzato". 401

Sintassi corretta dell'URL:

- I sistemi che non supportano la funzione di rimorchio non utilizzeranno la porta 4431 nel nome:
  https://hostname/ng-login

  -oppure- https://*nomehost*/euq-login

- I sistemi abilitati Trailblazer includeranno il numero di porta 4431 nel nome:
  https://hostname:4431/ng-login

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