Detalles administrativos del comando CLI "trailblazer" para Cisco Security Management Appliance (SMA)

Contenido

Introducción

Comenzando con AsyncOS 11.4 y continuando con AsyncOS 12.x para Security Management Appliance (SMA), la interfaz de usuario web (UI) ha experimentado un rediseño así como el procesamiento interno de datos. El enfoque de este artículo aborda los cambios en la capacidad de explorar la interfaz de usuario web recientemente rediseñada. Cisco ha trabajado para mejorar la experiencia del usuario con la implementación de un diseño más avanzado desde el punto de vista tecnológico.

Colaborado por Chris Arellano, ingeniero del TAC de Cisco.

Prerequisites

Nota: La interfaz de "administración" es la interfaz predeterminada, presentada durante la primera configuración en el SMA. Desde **Red > Interfaces IP**, no permite la eliminación. Por esta razón, siempre será la interfaz predeterminada la que se verificarán los servicios.

Asegúrese de que se hayan verificado los siguientes elementos antes de habilitar **trailblazerconfig**:

1. SMA se ha actualizado y está ejecutando AsyncOS versión 12.x (o posterior)
2. Desde **Red > Interfaces IP**, la interfaz de administración tiene **Administración de Dispositivos > HTTPS** habilitado **La administración del dispositivo > el** puerto **HTTPS** debe abrirse en el firewall
3. Desde **Network > IP Interfaces**, la Interfaz de Administración tiene **AsyncOS API > HTTP** y **AsyncOS > HTTPS** habilitados. **AsyncOS API > HTTP** y **AsyncOS API > HTTPS** los puertos deben abrirse en el firewall
4. El puerto "Trailblazer" debe abrirse a través del firewall El valor predeterminado es 4431
5. Asegúrese de que DNS pueda resolver el "nombre de host" de la interfaz de administración es decir, **nslookup** ***sma.hostname*** devuelve una dirección IP

6. Asegúrese de que DNS pueda resolver el "*Ésta es la interfaz predeterminada para Spam Quarantine*" hostname/URL configurado para acceder a Spam Quarantine

¿Por qué

La GUI de SMA de última generación (NGSMA) 12.x se ha reimplementado como una aplicación de página única (SPA) que se descarga en el cliente (IE, Chrome, Firefox) para mejorar la experiencia del usuario. El SPA se comunica con los varios servidores internos del SMA, cada uno de los cuales realiza un servicio diferente.

Las restricciones del CORS (Cross-Origin Resource Sharing) dentro de la comunicación del SPA al SMA causan algunos obstáculos a la comunicación entre los múltiples módulos.

- CORS es una función de seguridad diseñada para evitar que los comandos malintencionados se ejecuten dentro de una línea de comunicación establecida con otro servicio interno.

Los servidores internos son accesibles a través de diferentes puertos TCP numerados a través del NGSMA. Cada puerto TCP requiere una aprobación de certificado independiente para comunicarse con el cliente. La capacidad insuficiente para comunicarse con los servidores internos del NGSMA plantea un problema.

Impacto

Las interfaces web de última generación incluyen "/euq-login" y "ng-login".

Informe sobre la integración de AMP Cisco Threat Response (CTR).

Solución

El ejemplo simple de puertos TCP que representan diferentes módulos requiere la aceptación del certificado para cada puerto. Si no existe un certificado firmado de confianza en el SMA, se requieren varias aceptaciones de certificado cuando el navegador inicia una comunicación transparente con los módulos. Para un usuario que puede no entender la necesidad de los puertos TCP 6443, 443, 4431, la experiencia puede causar potencialmente confusión.

Para superar estos retos, Cisco ha implementado Nginx para realizar una función de proxy entre el cliente (cliente del navegador) y los servidores (servicios accesibles a través de puertos específicos). Nginx (estilizado como NGINX o nginx) es un servidor web que también se puede utilizar como proxy inverso, equilibrador de carga, proxy de correo y caché HTTP.

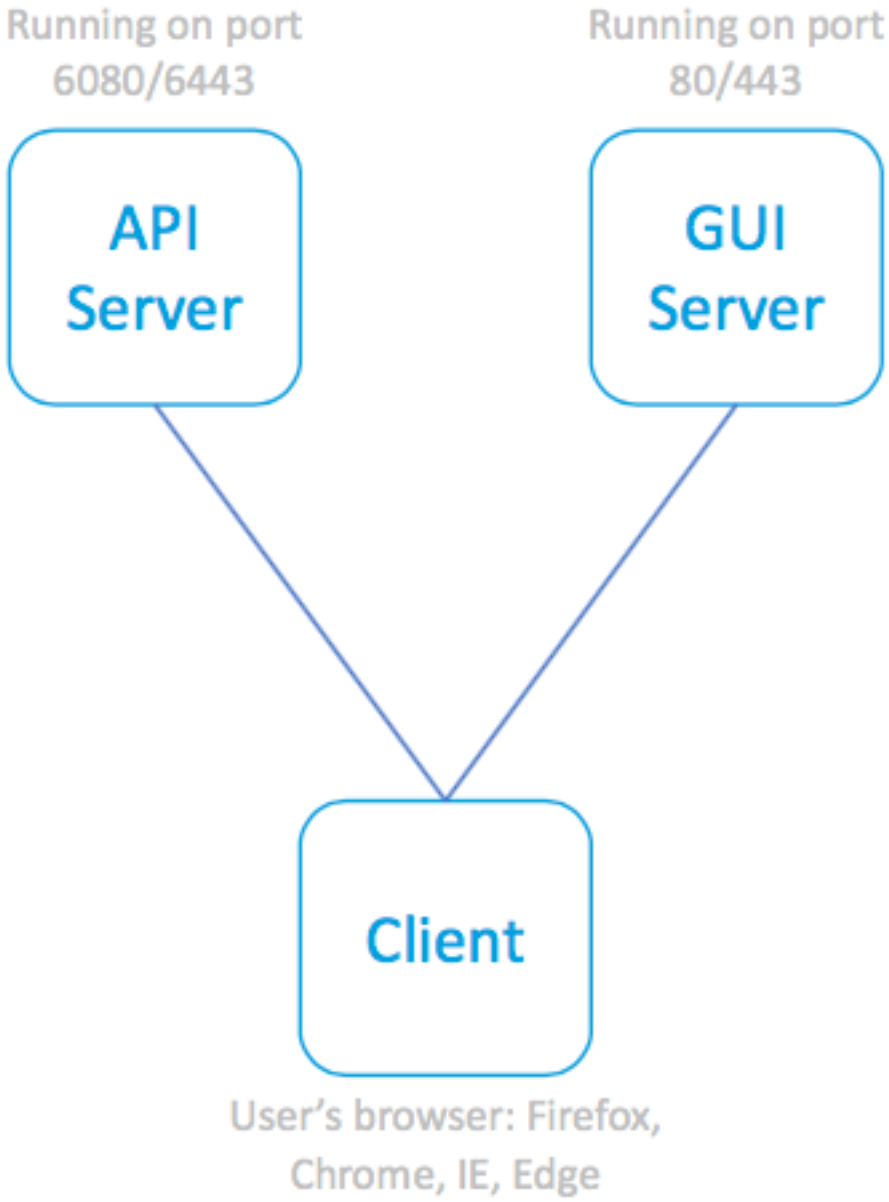
Esto condensa la comunicación a un único flujo de comunicación y aceptación del certificado.

Cisco ha etiquetado el comando CLI para habilitar esta funcionalidad como **trailblazerconfig**.

La primera ilustración muestra un ejemplo de dos servidores actuales:

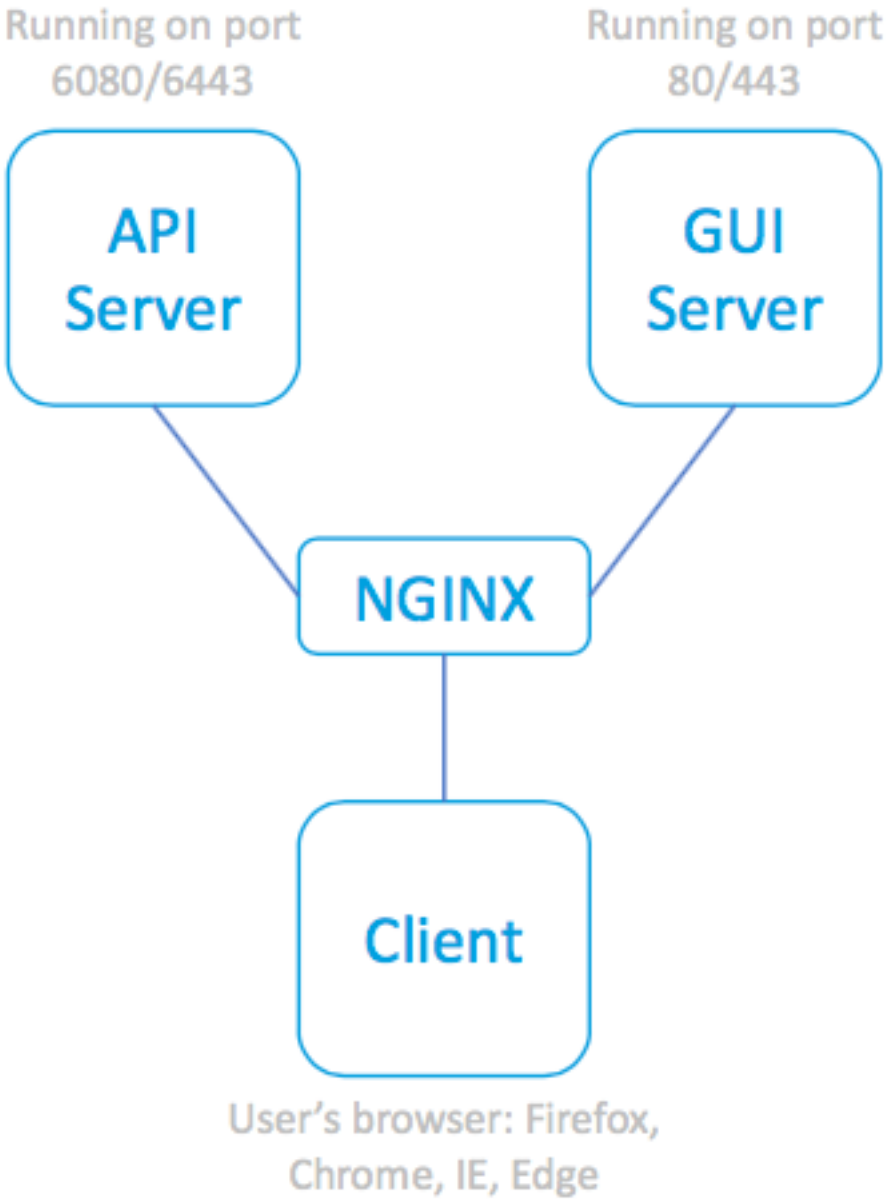
- Servidor API HTTP:6080 y HTTPS:6443
- Servidor GUI HTTP:80 y HTTPS:443

La aprobación de la comunicación de la GUI a la API requiere aprobación y acceso a los puertos.



SPA y servidores asociados

La siguiente ilustración incorpora el proxy Nginx delante de los procesos de la API y la GUI, lo que elimina el problema de las comunicaciones restringidas.



SPA, utilizando el proxy NGINX para alcanzar los servidores asociados

Ejemplos de la Línea de Comandos

Ayuda 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
```

Comprobar estado:

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Habilitar:

```
sma.local> trailblazerconfig enable

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

Post-enable, estado de verificación:

```
sma.local> trailblazerconfig status

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

Sintaxis de nombres de ejemplo

El acceso web habilitado para el pionero incluiría el puerto del pionero dentro de la dirección URL:

- El portal de gestión de NGSMA aparecería como: https://hostname:4431/ng-login
- El portal de cuarentena de usuario final (o ISQ) de NGSMA aparecería como: https://hostname:4431/euq-login

Resolución de problemas

Algunas implementaciones se centran en la interfaz secundaria para las notificaciones de spam. Si el "nombre de host" de la interfaz de administración no se puede resolver en DNS (es decir, **nslookup** ***hostname***), el pionero no se inicializará.

Una acción para confirmar y restaurar inmediatamente el servicio es agregar un nombre de host resoluble a la interfaz de administración. (A continuación, cree un registro A para resolver correctamente el nombre de host designado.)

Las restricciones de seguridad del lado del usuario impiden el acceso del entorno del usuario al puerto TCP SMA 4431:

1. Pruebe para asegurarse de que el puerto esté disponible para el explorador
2. Introduzca el nombre de host y el puerto como: https://hostname:4431

Puerto TCP 443 no abierto

- IE11: Esta página no se puede mostrar
- Cromado: No se puede acceder a este sitio. Rechazado para conectarse
- Firefox: No se puede conectar

Puerto TCP 4431 abierto y certificado aceptado

- IE: HTTP 406
- Cromado:{"error": {"mensaje": "No autorizado "código": "401", "explicación": "401 = Sin perr consulte esquemas de autorización."}}
- Firefox: Mensaje de certificado (ACCEPT). Firefox: postcertificate accept > "Unauthorize 401

Sintaxis de URL correcta:

- Los sistemas no habilitados para pionero no utilizarán el puerto 4431 con el nombre: https://hostname/ng-login

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

- Los sistemas habilitados para Trailblazer incluirán el número de puerto 4431 en el nombre: https://hostname:4431/ng-login

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