Detalles administrativos en el comando CLI del “pionero” para el dispositivo de la Administración del Cisco Security (SMA)

Contenido

Introducción

Comenzando con AsyncOS 11.4 y continuando con [AsyncOS 12.x para el dispositivo de la Administración de seguridad (SMA)](#), el interfaz del Web User (UI) ha experimentado un reajuste así como el procesamiento interno de los datos. El foco de este artículo dirige los cambios en la capacidad de hojear el interfaz nuevamente reajustado del Web User. La puesta en práctica de un diseño más tecnológico avanzado, Cisco ha trabajado para mejorar la experiencia del usuario.

Contribuido por Chris Arellano, ingeniero del TAC de Cisco.

Prerrequisitos

Nota: El interfaz de la “Administración” es el interfaz del valor por defecto, presentado durante la primera configuración en el SMA. **De la red > de los interfaces IP**, no permite la cancelacíon. Por este motivo, será siempre el interfaz del valor por defecto que mantiene será verificado.

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

1. SMA se ha actualizado y está funcionando con la versión 12.x de AsyncOS (o más nuevo)
2. **De la red > de los interfaces IP**, la interfaz de administración tiene la **Administración del dispositivo > HTTPS** activados **La Administración del dispositivo > el** puerto **HTTPS** se deben abrir en el Firewall
3. **De la red > de los interfaces IP**, la interfaz de administración tiene **AsyncOS API > HTTP** y **AsyncOS > HTTPS** ambos activados. **AsyncOS API > HTTP** y **AsyncOS los** puertos **API > HTTPS** se deben abrir en el Firewall
4. El puerto del “pionero” se debe abrir con el Firewall El valor por defecto es 4431
5. Asegúrese que el DNS pueda resolver la interfaz de administración “hostname” es decir, el nslookup **sma.hostname *vuelve una*** dirección IP
6. Asegúrese que el DNS pueda resolver “*esto sea el interfaz del valor por defecto para la*

cuarentena” hostname/URL del *Spam* configurada para tener acceso a la cuarentena del Spam

Porqué

12.x re-se ha ejecutado El GUI de la última generación SMA (NGSMA) como una sola aplicación de la página (BALNEARIO) que consigue descargó sobre el cliente (IE, Chrome, Firefox) para mejorar la experiencia del usuario. El BALNEARIO comunica a través a los servidores internos múltiples SMA, cada uno que lleva a cabo un diverso servicio.

Las restricciones de los CORAZONES (recursos compartidos del Cruz-origen) dentro de la comunicación del BALNEARIO al SMA causan algunos obstáculos a la comunicación entre los módulos múltiples.

- Los CORAZONES son una función de seguridad diseñada para evitar que los comandos malévolos ejecuten dentro de una línea de comunicación establecida a otro servicio interno.

Los servidores internos son accesibles a través de diversos puertos numerados TCP vía el NGSMA. Cada puerto TCP requiere una aprobación separada del certificado comunicar al cliente. La capacidad escasa de comunicar a los servidores internos NGSMA presenta un problema.

Impacto

Las interfaces Web de la última generación incluyendo “/euq-login” y la “ng-clave”.

Señale para la integración de la Respuesta de Cisco ante amenazas AMP (CTR).

Solución

El ejemplo simple de los puertos TCP que representan diversos módulos requiere la aceptación del certificado para cada puerto. Si un certificado firmado de confianza no existe en el SMA, después se requieren las aceptaciones del certificado múltiple mientras que el navegador inicia la comunicación clara a los módulos. A un usuario que pueda no entender la necesidad de los puertos 6443 TCP, 443, 4431, la experiencia pueden potencialmente causar la confusión.

Para moverse más allá de estos desafíos, Cisco ha ejecutado Nginx para realizar una función del proxy entre el cliente (cliente del buscador) y los servidores (servicios accesibles vía los puertos específicos). Nginx (estilizado como NGINX o nginx) es un servidor Web que puede también ser utilizado pues una representación inversa, un balanceador de la carga, un proxy del correo y un caché HTTP.

Esto condensa la comunicación a una solas secuencia de la comunicación y aceptación del certificado.

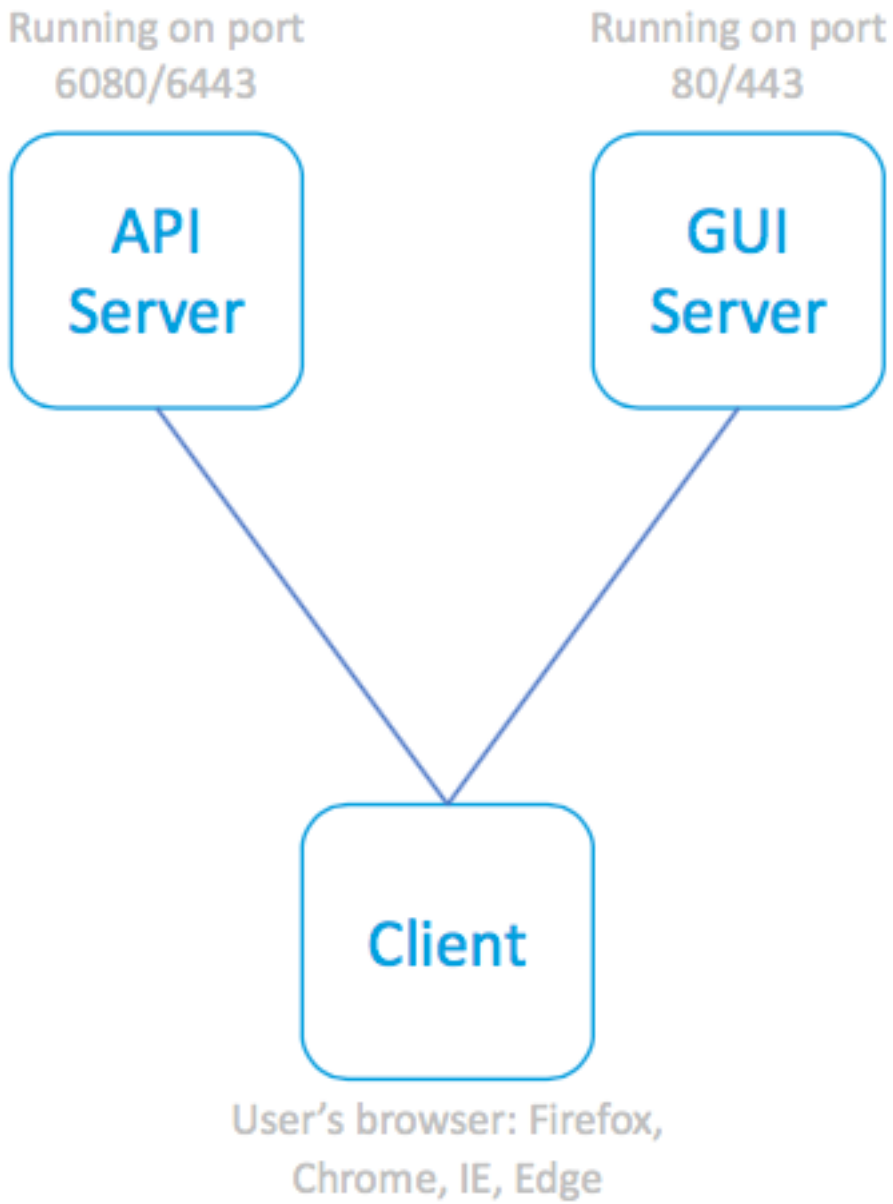
Cisco ha etiquetado el comando CLI de activar estas funciones como **trailblazerconfig**.

El primer ejemplo visualiza un ejemplo de dos servidores actuales:

- Servidor HTTP:6080 y HTTPS:6443 API

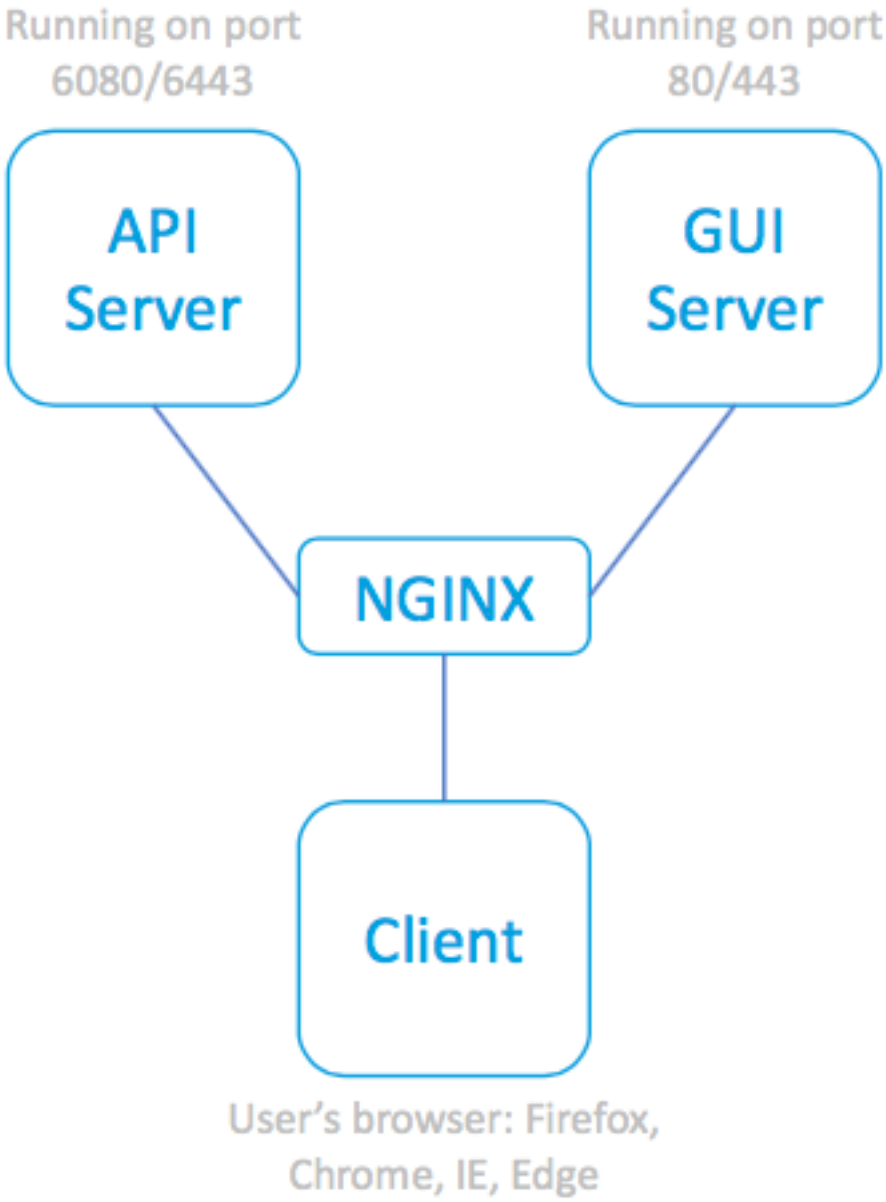
- Servidor HTTP:80 y HTTPS:443 GUI

La comunicación aprobada del GUI al API requiere la aprobación y el acceso del puerto.



BALNEARIO y servidores asociados

El ejemplo siguiente incorpora el proxy de Nginx delante de los procesos API y GUI - eliminación de la preocupación de las comunicaciones restrictas.



BALNEARIO, utilizando el proxy NGINX para alcanzar los servidores asociados

Ejemplos de la línea de comando

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
```

Estatus del control:

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Permiso:

```
sma.local> trailblazerconfig enable

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

Poste-permiso, estatus del control:

```
sma.local> trailblazerconfig status

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

Muestra que nombra el sintaxis

El Acceso Web activado pionero incluiría el puerto del pionero dentro de la dirección URL:

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

Resolución de problemas

Foco de algunas puestas en práctica en la interfaz secundaria para las notificaciones del Spam. SI la interfaz de administración “hostname” no es resoluble en DNS (es decir, **hostname del** nslookup***),*** después el pionero no podrá inicializarse.

Una acción a confirmar inmediatamente y el servicio del restore es agregar un hostname resoluble a la interfaz de administración. (Entonces cree un expediente A para resolver correctamente el hostname señalado.)

Las restricciones de seguridad del lado del usuario previenen el acceso del entorno del usuario hacia el puerto SMA 4431 TCP:

1. Pruebe para asegurarse que el puerto está disponible para el navegador
2. Ingrese el hostname y el puerto como:
   https:// *hostname:4431*

Puerto 443 TCP no abierto

- IE11: Esta página no puede ser visualizada
- Chrome: Este sitio no puede ser alcanzado. Rechazó conectar
- Firefox: Incapaz de conectar

Puerto 4431 TCP abierto y certificado validado

- IE: HTTP 406
- Chrome: {“error”: {“mensaje”: “Desautorizado “código”: el "401", “explicación”: "401 = ningú permiso -- vea los esquemas de la autorizaci
- Firefox: Mensaje del certificado (VALIDE). Fi aceptación del certificado del poste > “desautorizado.” 401

Sintaxis del URL correcta:

- los sistemas activados No-pionero no utilizarán el puerto 4431 en el nombre: https:// *hostname/ng-login*

  hostname - o de https:///euq-clave

- Los sistemas activados pionero incluirán el número del puerto 4431 en el nombre: https:// *hostname:4431/ng-login*

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