Detalhes administrativos sobre o comando CLI do 'pionblazer' para o Cisco Security Management Appliance (SMA)

Contents

Introduction

Começando com o AsyncOS 11.4 e continuando com o AsyncOS 12.x para o Security Management Appliance (SMA), a interface de usuário da Web (UI) passou por um novo design e também pelo processamento interno de dados. O foco deste artigo trata das alterações na capacidade de navegar na interface de usuário da Web reprojetada recentemente. Com a implementação de um projeto mais avançado tecnologicamente, a Cisco trabalhou para melhorar a experiência do usuário.

Contribuído por Chris Arellano, engenheiro do TAC da Cisco.

Prerequisites

Observação: a interface de "gerenciamento" é a interface padrão, apresentada durante a primeira configuração no SMA. Em **Rede > Interfaces IP**, não permite a exclusão. Por esse motivo, será sempre a interface padrão que os serviços serão verificados.

Certifique-se de que os seguintes itens foram verificados antes de habilitar o **pionazerconfig**:

1. O SMA foi atualizado e está executando o AsyncOS versão 12.x (ou mais recente)
2. Em **Rede > Interfaces IP**, a interface de gerenciamento tem **Gerenciamento de dispositivos > HTTPS** habilitado **Gerenciamento de dispositivos > A** porta **HTTPS** deve ser aberta no firewall
3. Em **Rede > Interfaces IP**, a Interface de Gerenciamento tem **API AsyncOS > HTTP** e **AsyncOS > HTTPS** ativados. **API AsyncOS > HTTP** e **API AsyncOS >** portas **HTTPS** devem ser abertas no firewall
4. A porta "Trailblazer" deve ser aberta pelo firewall O padrão é 4431
5. Certifique-se de que o DNS possa resolver o "hostname" da interface de gerenciamento por exemplo, **nslookup** ***sma.hostname*** retorna um endereço IP
6. Certifique-se de que o DNS possa resolver o nome de host/URL "*Esta é a interface padrão*

para a Quarentena de spam" configurado para acessar a Quarentena de spam

Por quê

A GUI 12.x Next Generation SMA (NGSMA) foi reimplementada como SPA (Single Page Application, aplicativo de página única) que é baixada para o cliente (IE, Chrome, Firefox) para melhorar a experiência do usuário. O SPA comunica-se através dos vários servidores internos do SMA, cada um executando um serviço diferente.

As restrições CORS (Cross-Source Resource Sharing) dentro da comunicação SPA ao SMA causam alguns obstáculos à comunicação entre os vários módulos.

- O CORS é um recurso de segurança projetado para impedir que comandos mal-intencionados sejam executados em uma linha estabelecida de comunicação para outro serviço interno.

Os servidores internos podem ser acessados através de diferentes portas TCP numeradas através do NGSMA. Cada porta TCP requer uma aprovação de certificado separada para se comunicar com o Cliente. A capacidade insuficiente de se comunicar com os servidores internos do NGSMA apresenta um problema.

Impacto

As interfaces da Web de próxima geração, incluindo "/euq-login" e "ng-login".

Relatório da integração do AMP Cisco Threat Response (CTR).

Solução

O exemplo simples de portas TCP que representam diferentes módulos exige a aceitação do certificado para cada porta. Se não existir um certificado assinado confiável no SMA, então são necessárias várias aceitações de certificado à medida que o navegador inicia uma comunicação transparente com os módulos. Para um usuário que pode não entender a necessidade das Portas TCP 6443, 443, 4431, a experiência pode causar confusão.

Para superar esses desafios, a Cisco implementou o Nginx para executar uma função de proxy entre o cliente (cliente de navegador) e os servidores (serviços acessíveis através de portas específicas). O Nginx (estilizado como NGINX ou nginx) é um servidor Web que também pode ser usado como proxy reverso, balanceador de carga, proxy de correio e cache HTTP.

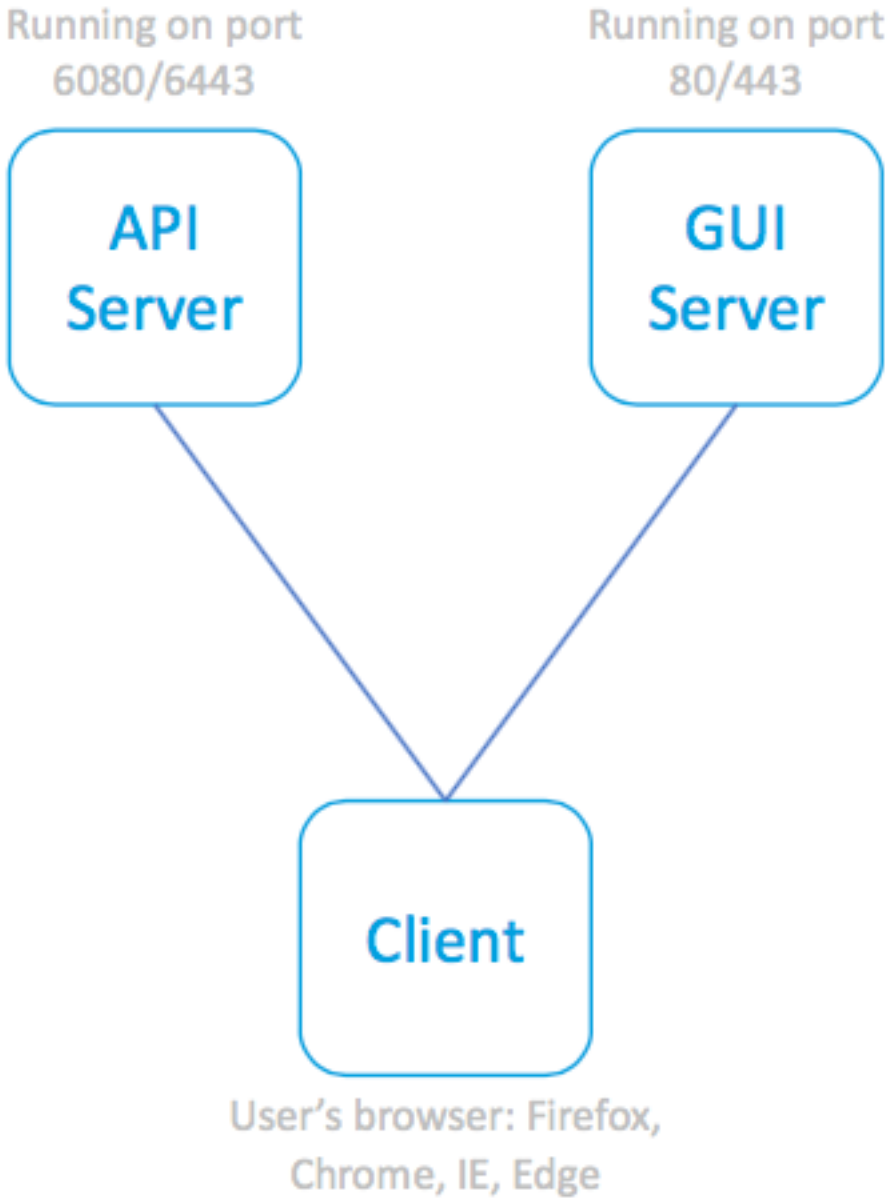
Isso condensa a comunicação para um único fluxo de comunicação e aceitação de certificado.

A Cisco rotulou o comando CLI para habilitar essa funcionalidade como **pionazerconfig**.

A primeira ilustração exibe um exemplo de dois servidores atuais:

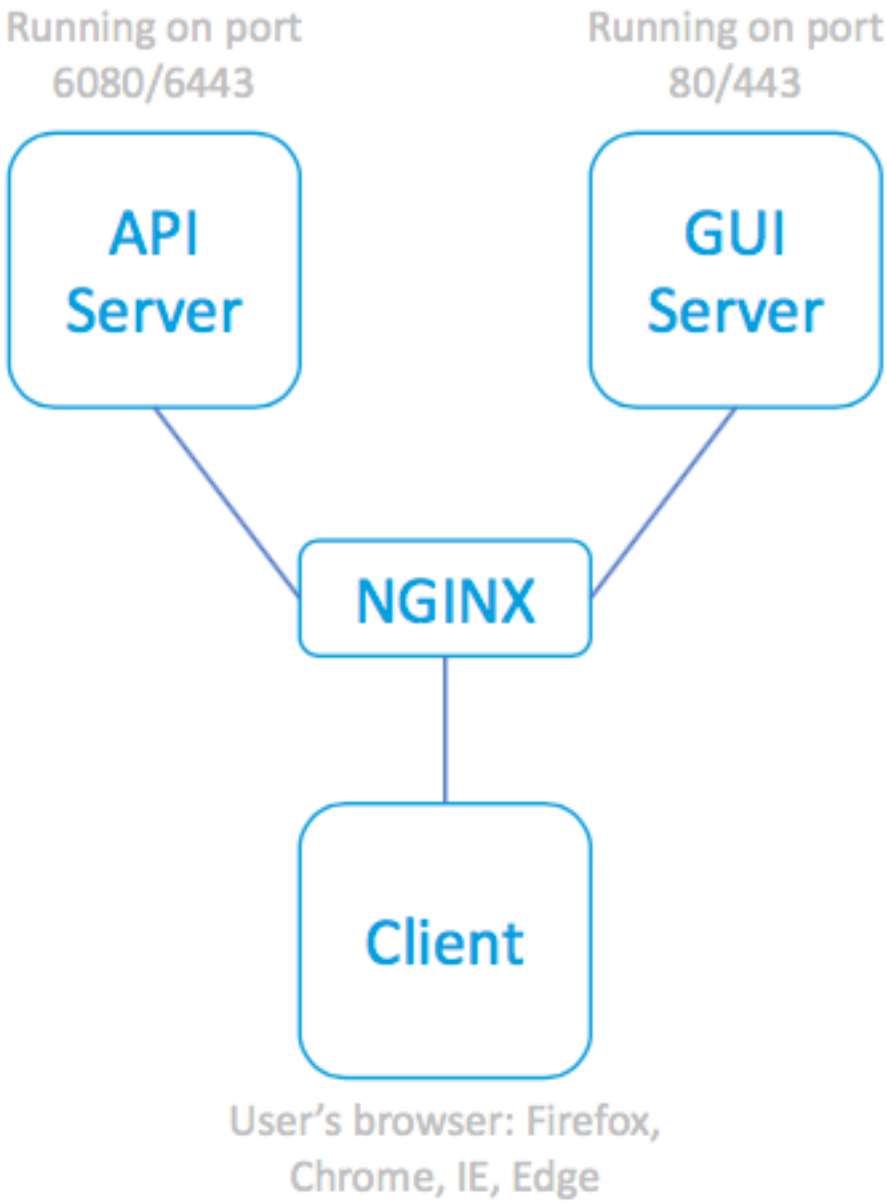
- Servidor API HTTP:6080 e HTTPS:6443
- Servidor GUI HTTP:80 e HTTPS:443

A aprovação da comunicação da GUI para a API requer aprovação e acesso à porta.



SPA e servidores associados

A próxima ilustração incorpora o proxy Nginx em frente aos processos de API e GUI - eliminando a preocupação de comunicações restritas.



SPA, utilizando o proxy NGINX para acessar os servidores associados

Exemplos de linha de comando

Ajuda 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
```

Verificar status:

```
sma.local> trailblazerconfig status

trailblazer is not running
```

Enable:

```
sma.local> trailblazerconfig enable

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

Pós-ativação, status da verificação:

```
sma.local> trailblazerconfig status

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

Exemplo de sintaxe de nome

O acesso à Web habilitado para o iniciador incluiria a porta do iniciador no endereço URL:

- O NGSMA Management Portal apareceria como: https://hostname:4431/ng-login
- O portal NGSMA End User Quarantine (ou EUQ) apareceria como: https://hostname:4431/euq-login

Troubleshooting

Algumas implementações se concentram na interface secundária para notificações de spam. Se o "hostname" da interface de gerenciamento não for resolvível no DNS (ou seja, **nslookup *hostname***), o pionblazer não inicializará.

Uma ação para confirmar e restaurar imediatamente o serviço é adicionar um nome de host resolvível à interface de gerenciamento. (Em seguida, crie um registro A para resolver corretamente o nome de host designado.)

As restrições de segurança do lado do usuário impedem o acesso do ambiente do usuário em direção à porta TCP SMA 4431:

1. Teste para garantir que a porta esteja disponível para o navegador
2. Insira o nome do host e a porta como: https://hostname:4431

Porta TCP 443 não aberta

- IE11: Esta página não pode ser exibida
- Cromo: Este site não pode ser acessado. Recusado de conectar
- Firefox: Não é possível conectar

Porta TCP 4431 aberta e certificado aceito

- IE: HTTP 406
- Cromo:{"erro": {"mensagem": "Não autorizad "código": "401", "explicação": "401 = Sem permissão — consulte esquemas de autorização."}}
- Firefox: Prompt de certificado (ACCEPT). Fi pós-aceitação do certificado > "Não autoriza 401

Sintaxe de URL correta:

- Os sistemas não habilitados para pioneiros não usarão a porta 4431 no nome: https://hostname/ng-login

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

- Os sistemas habilitados para Trailblazer incluirão o número de porta 4431 no nome: https://hostname:4431/ng-login

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