Cisco SMA(Security Management Appliance)용 '트레일블레이저' CLI 명령에 대한 관리 세부사항

목차

소개

AsyncOS 11.4부터 시작하여 AsyncOS 12.x for Security Management Appliance(SMA)를 계속 진행하면서 웹 사용자 인터페이스(UI)는 재설계와 내부 데이터 처리를 거쳤습니다.이 문서에서는 새로 디자인된 웹 사용자 인터페이스를 검색하는 기능의 변화를 다룹니다. Cisco는 더 기술적으로 진보된 설계를 구현하여 사용자 환경을 개선했습니다.

기고자: Cisco TAC 엔지니어 Chris Arellano

사전 요구 사항

참고: "Management" 인터페이스는 SMA의 첫 번째 컨피그레이션 중에 표시되는 기본 인터페이스입니다. **Network(네트워크) > IP Interfaces(IP 인터페이스)**에서 삭제를 허용하지 않습니다. 따라서 서비스는 항상 기본 인터페이스이므로 확인됩니다.

trailablzerconfig를 활성화하기 전에 다음 항목이 **확인되었는지 확인합니다**.

1. SMA가 업그레이드되었으며 AsyncOS 버전 12.x 이상을 실행 중입니다.
2. Network(**네트워크) > IP Interfaces(IP 인터페이스)**에서 관리 인터페이스에는 Appliance **Management(어플라이언스 관리) > HTTPS**가 활성화됨 **Appliance Management(어플라이언스 관리) > HTTPS** 포트는 방화벽에서 열어야 합니다.
3. Network(**네트워크) > IP Interfaces(IP 인터페이스)**에서 관리 인터페이스에는 AsyncOS **API > HTTP** 및 **AsyncOS > HTTPS**가 모두 활성화되어 있습니다. **AsyncOS API > HTTP** and **AsyncOS API > HTTPS** 포트는 방화벽에서 열어야 합니다.
4. "Trailazer" 포트는 방화벽을 통해 열어야 합니다. 기본값은 4431입니다.
5. DNS가 관리 인터페이스 "호스트 이름"을 확인할 수 있는지 확인
   예: nslookup **sma *.hostname은*** IP 주소를 반환합니다.
6. DNS가 스팸 쿼런틴에 액세스하도록 구성된 "*This is the default interface for the Spam Quarantine*" hostname/URL을 확인할 수 있는지 확인합니다.

왜

12.x NGSMA(Next Generation SMA) GUI는 사용자 경험을 개선하기 위해 클라이언트(IE, Chrome, Firefox)에 다운로드되는 SPA(Single Page Application)로 다시 구현되었습니다. SPA는 SMA의 여러 내부 서버와 통신하며 각각 다른 서비스를 수행합니다.

SMA에 대한 SPA 통신 내에서 CORS(Cross-Origin Resource Sharing) 제한으로 인해 여러 모듈 간의 통신에 몇 가지 장애가 발생합니다.

- CORS는 악의적인 명령이 다른 내부 서비스와의 설정된 통신 라인 내에서 실행되지 않도록 설계된 보안 기능입니다.

내부 서버는 NGSMA를 통해 서로 다른 번호가 지정된 TCP 포트를 통해 연결할 수 있습니다. 각 TCP 포트에는 클라이언트와 통신하려면 별도의 인증서 승인이 필요합니다. NGSMA의 내부 서버와 통신할 수 없는 경우 문제가 발생합니다.

영향

"/euq-login" 및 "ng-login"을 포함하는 차세대 웹 인터페이스.

AMP CTR(Cisco Threat Response) 통합을 위한 보고서

솔루션

서로 다른 모듈을 나타내는 TCP 포트의 간단한 예는 각 포트에 대해 인증서를 승인해야 합니다. 신뢰할 수 있는 서명 인증서가 SMA에 없는 경우 브라우저가 모듈과의 투명한 통신을 시작하기 때문에 여러 인증서 수락을 필요로 합니다. TCP 포트 6443, 443, 4431의 필요성을 이해하지 못하는 사용자에게 이러한 경험이 혼란을 일으킬 수 있습니다.

이러한 문제를 해결하기 위해 Cisco는 클라이언트(브라우저 클라이언트)와 서버(특정 포트를 통해 연결 가능한 서비스) 간에 프록시 기능을 수행하기 위해 Nginx를 구현했습니다. Nginx(NGINX 또는 nginx로 구분)는 리버스 프록시, 로드 밸런서, 메일 프록시 및 HTTP 캐시로 사용할 수 있는 웹 서버입니다.

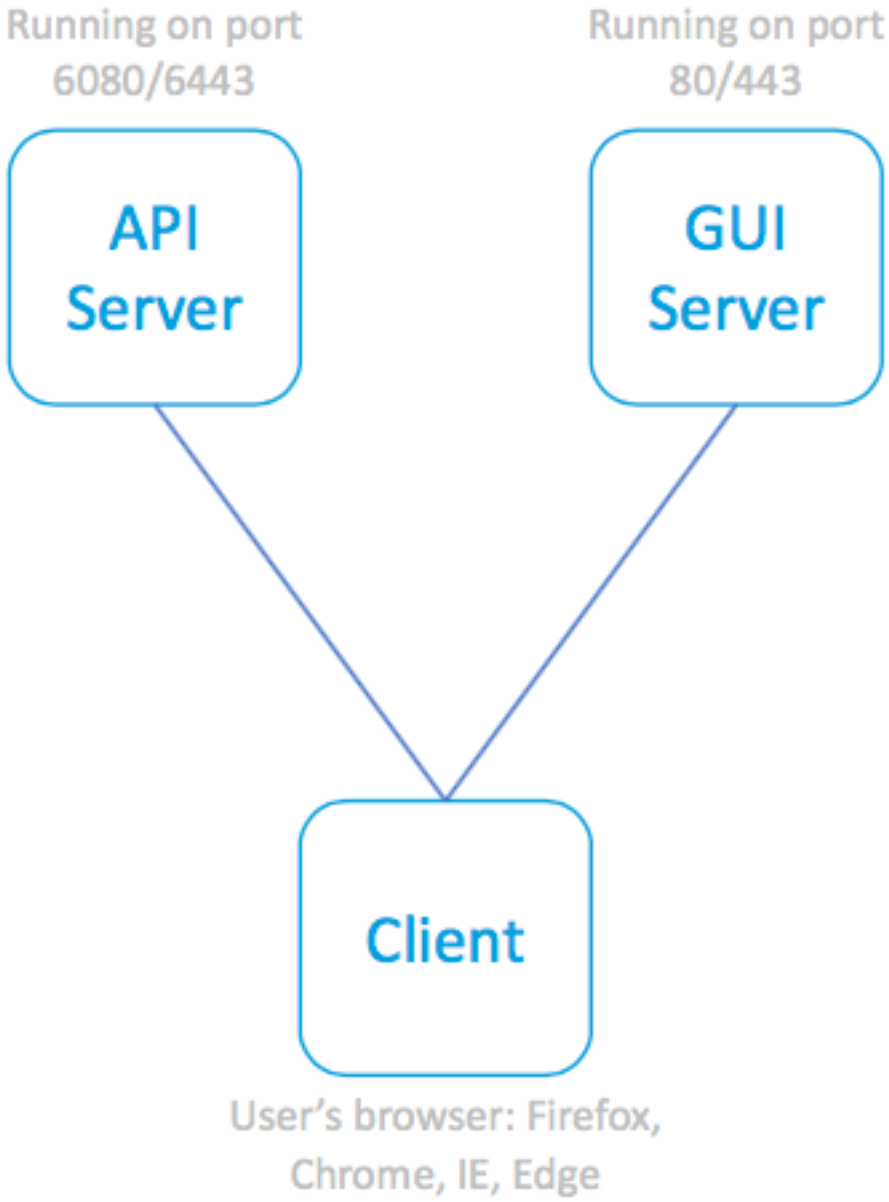
이렇게 하면 단일 통신 스트림 및 인증서 수락으로 통신이 압축됩니다.

Cisco는 이 기능을 trainblabzerconfig로 활성화하기 위해 CLI 명령**에 레이블을 지정했습니다**.

첫 번째 그림은 두 개의 현재 서버의 예를 보여줍니다.

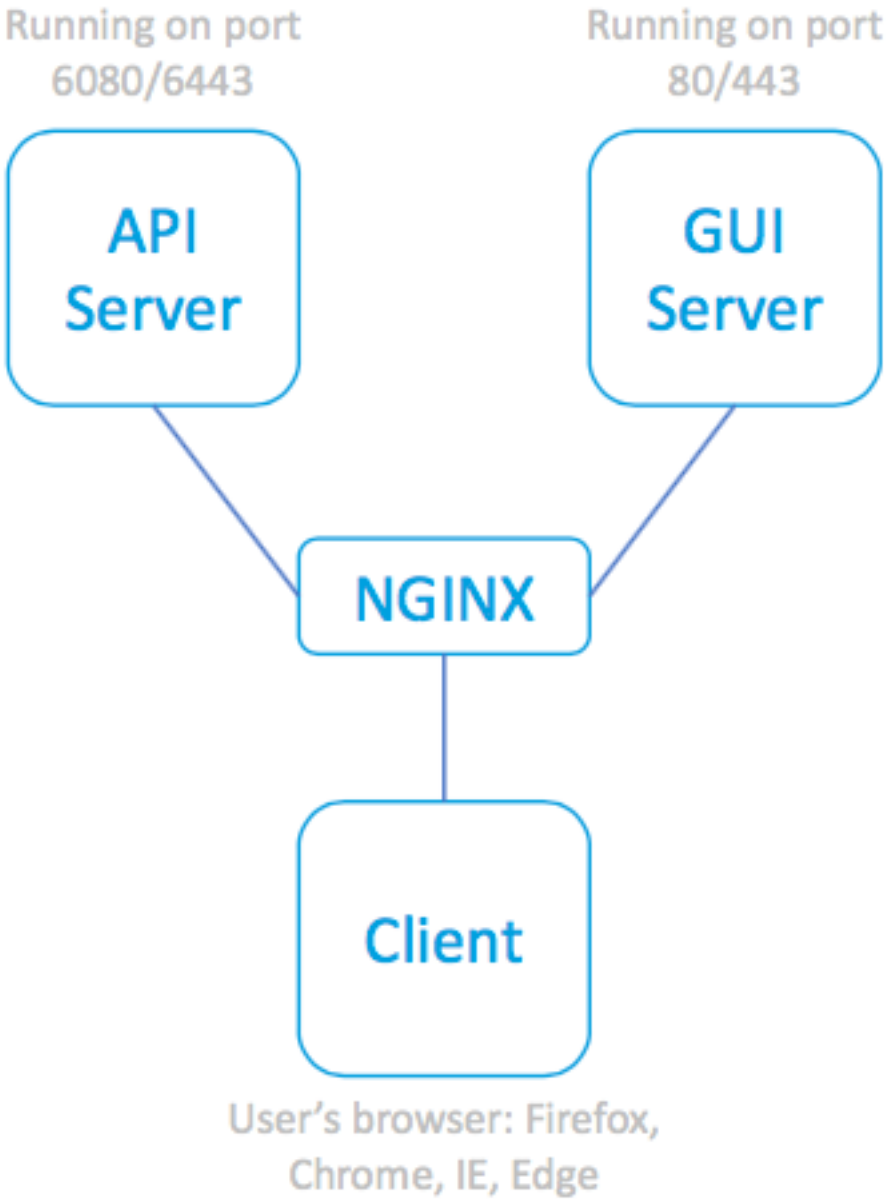
- API 서버 HTTP:6080 및 HTTPS:6443
- GUI 서버 HTTP:80 및 HTTPS:443

GUI에서 API로의 통신을 승인하려면 승인 및 포트 액세스가 필요합니다.



SPA 및 관련 서버

다음 그림은 API 및 GUI 프로세스 앞에 Nginx 프록시를 통합하여 제한된 커뮤니케이션의 우려를 해소합니다.



SPA, NGINX Proxy를 활용하여 연결된 서버에 연결

명령줄 예

전체 도움말:

```
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
```

상태 확인:

```
sma.local> trailblazerconfig status

trailblazer is not running
```

사용:

```
sma.local> trailblazerconfig enable

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

사후 활성화, 상태 확인:

```
sma.local> trailblazerconfig status

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

샘플 명명 구문

트레일블레이저 지원 웹 액세스는 URL 주소 내에 트레일블레이저 포트를 포함합니다.

- NGSMA 관리 포털은 다음과 같이 표시됩니다.https://hostname:4431/ng-login
- NGSMA 최종 사용자 쿼런틴(또는 ISQ) 포털은 다음과 같이 표시됩니다 .https://hostname:4431/euq-login

문제 해결

일부 구현에서는 스팸 알림을 위한 보조 인터페이스에 중점을 둡니다.DNS에서 관리 인터페이스 "hostname"을(를) 확인할 수 없는 경우(예: nslookup 호스트 이름) 트레일블레이저를 초기화하지 못합니다.

서비스를 즉시 확인하고 복원하는 한 가지 작업은 확인 가능한 호스트 이름을 관리 인터페이스에 추가하는 것입니다.(그런 다음 지정된 호스트 이름을 올바르게 확인하기 위해 A 레코드를 만듭니다 .)

사용자 측 보안 제한 사항으로 인해 사용자 환경에서 SMA 4431 TCP 포트로의 액세스가 차단됩니다.

1. 브라우저에서 포트를 사용할 수 있는지 테스트
2. 다음과 같이 호스트 이름 및 포트를 입력합니다.
   https://hostname:4431

TCP 포트 443이 열리지 않음

- **IE11:이 페이지를 표시할 수 없습니다.**
- **Chrome:이 사이트에 연결할 수 없습니다.연결 거부됨**
- **Firefox:연결할 수 없음**

TCP 포트 4431 열기 및 인증서 수락됨

- **IE:HTTP 406**
- **Chrome:{"error":{"메시지":"인증되지 않음.", "**
  ":"401", "설명":"401 = 권한 없음 — 권한 부여 마를 참조하십시오."}
- **Firefox:인증서 프롬프트(ACCEPT). Firefox:p certificate acceptance(인증서 승인 후) > "Unauthorized(승인되지 않음)" 401**

올바른 URL 구문:

- 비 트레일블레이저 지원 시스템은 이름에 포트 4431을 사용하지 않습니다.
  https://hostname/ng-login

  -또는- https:// *hostname*/euq-login

- Trailabzer가 활성화된 시스템은 이름에 포트 번호 4431을 포함합니다.
  https://hostname:4431/ng-login

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