思科安全管理设备(SMA)的“开拓者”CLI命令的管理详细信息

目录

简介

从AsyncOS 11.4开始，到AsyncOS 12.x for Security Management Appliance(SMA),Web用户界面(UI)经过重新设计，并对数据进行内部处理。本文重点介绍浏览新重新设计的Web用户界面的功能变化。 在实施技术更先进的设计后，思科努力改善用户体验。

作者：思科TAC工程师Chris Arellano。

先决条件

注意：“管理”接口是默认接口，在SMA的第一次配置期间显示。在“网**络”>“IP接**口”中，不允许删除。 因此，它始终是要验证服务的默认接口。

在启用trailzerconfig之前，请确保已验证以**下项目**:

1. SMA已升级，且正在运行AsyncOS版本12.x（或更高版本）
2. 在“**网络”>“IP接口**”中，管理接口启**用了“设备管理”> 必须在防火墙上**打开“设备管理”(Appliance Management)> HTTPS端口
3. 在**Network > IP Interfaces**中，管理接口**已启用AsyncOS API > HTTP**和**AsyncOS > HTTPS。必须在防火墙上打**开AsyncOS API **> HTTP和**AsyncOS API > HTTPS端口
4. 必须通过防火墙打开“开拓者”端口 默认值为 4431
5. 确保DNS可解析管理接口“主机名”
   即，nslookup sma.hostname**返*回IP***地址
6. 确保DNS可以解析“*这是垃圾邮件隔离区的默认接口*”主机名/URL，该主机名/URL配置为访问垃圾邮件隔离区

为什么

12.x下一代SMA(NGSMA)GUI已重新实施为单页应用(SPA)，下载到客户端(IE、Chrome、Firefox)，以改善用户体验。 SPA与SMA的多台内部服务器通信，每台服务器执行不同的服务。

SPA与SMA通信中的CORS（跨源资源共享）限制会对多个模块之间的通信造成一些障碍。

- CORS是一种安全功能，旨在防止恶意命令在已建立的与其他内部服务的通信线路内执行。

内部服务器可通过NGSMA通过不同编号的TCP端口访问。每个TCP端口都需要单独的证书批准才能与客户端通信。 无法与NGSMA的内部服务器通信会带来问题。

影响

下一代Web界面，包括“/euq-login”和“ng-login”。

AMP思科威胁响应(CTR)集成报告。

解决方案

TCP端口代表不同模块的简单示例要求每个端口接受证书。 如果SMA上不存在受信任签名证书，则当浏览器启动与模块的透明通信时，需要接受多个证书。 如果用户可能不理解TCP端口6443、443、4431的需求，这种体验可能会造成混淆。

为了克服这些挑战，思科实施了Nginx，以在客户端（浏览器客户端）和服务器（可通过特定端口访问的服务）之间执行代理功能。 Nginx（以NGINX或nginx格式表示）是Web服务器，也可用作反向代理、负载均衡器、邮件代理和HTTP缓存。

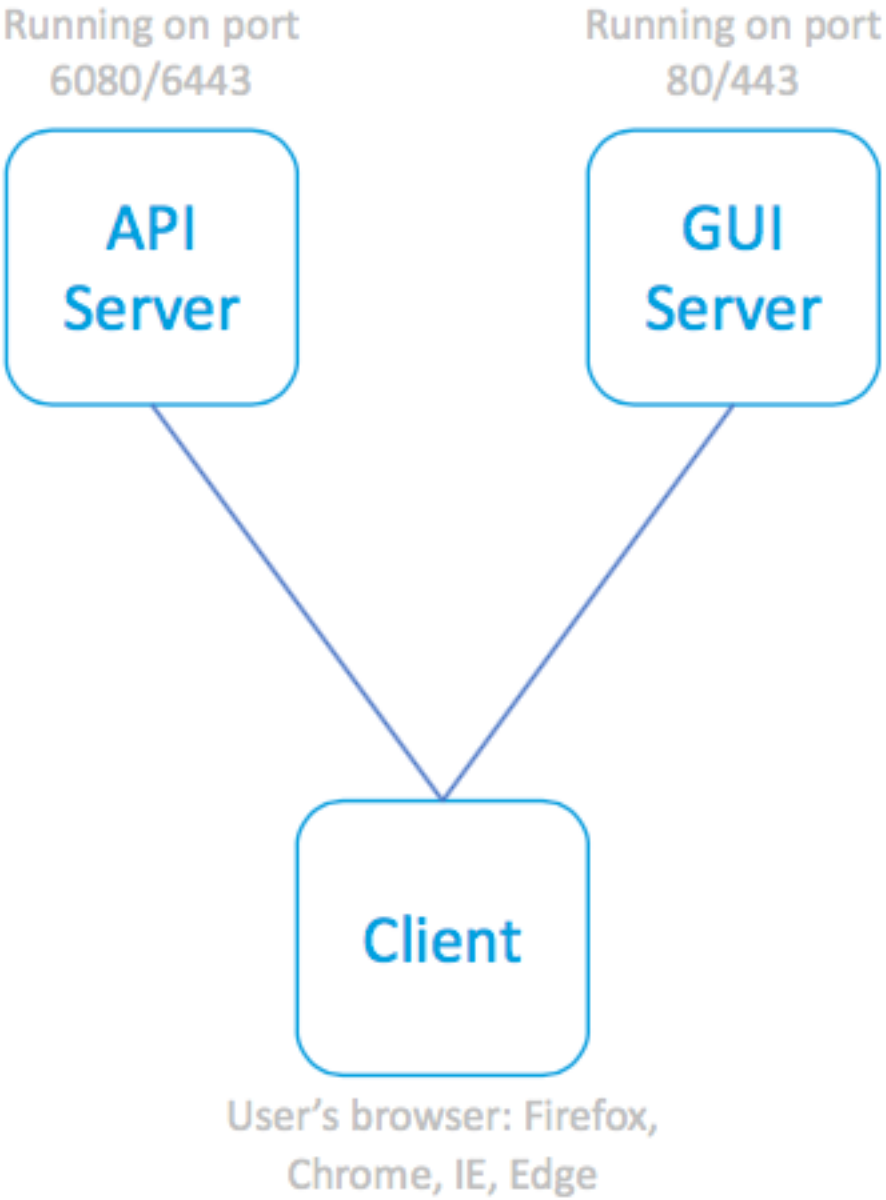
这将通信简化为单个通信流和证书接受。

思科已将CLI命令标记为**trailzerconfig**。

第一个图显示了两个当前服务器的示例：

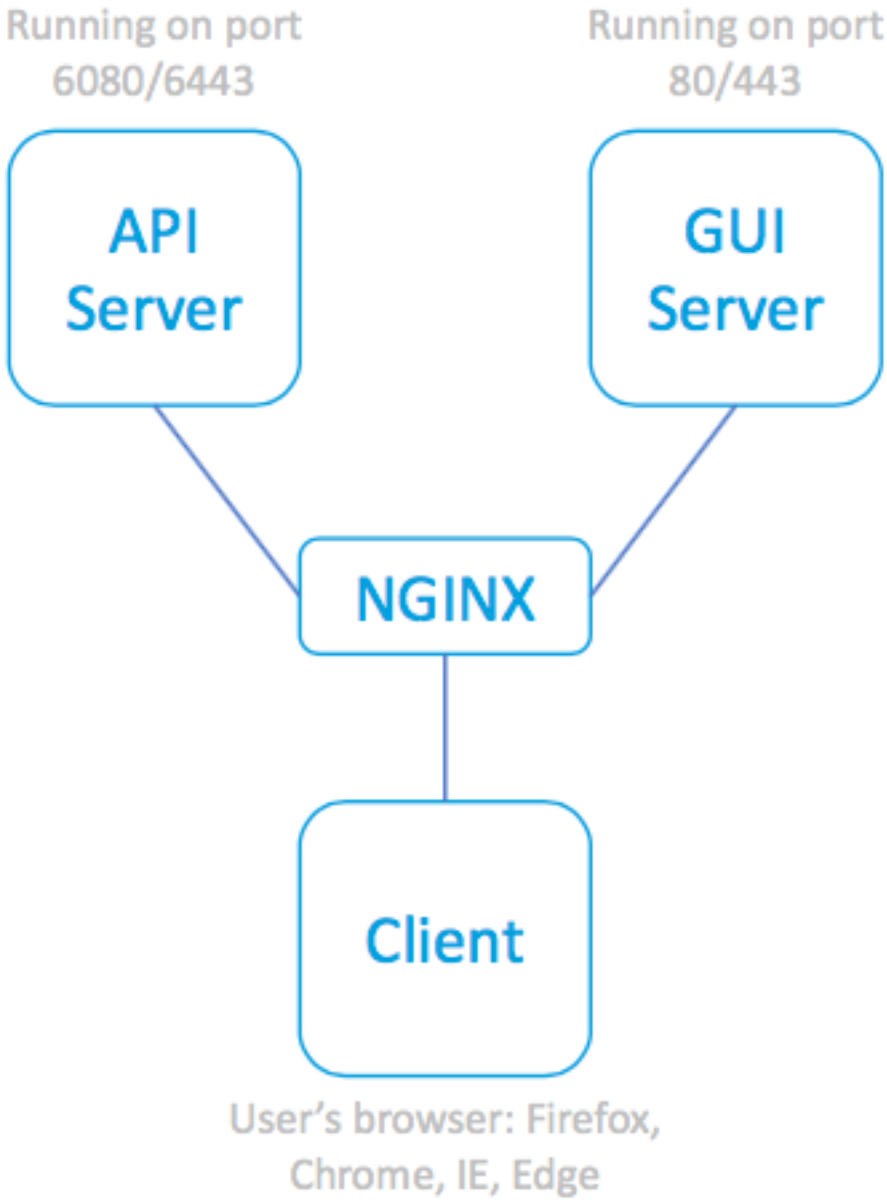
- API服务器HTTP:6080和HTTPS:6443
- GUI服务器HTTP:80和HTTPS:443

从GUI向API批准通信需要批准和端口访问。



SPA和相关服务器

下图在API和GUI进程前加入了Nginx代理，消除了对受限通信的顾虑。



SPA，利用NGINX代理访问

相关服务器

命令行示例

完整帮助：

```
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
```

检查状态：

```
sma.local> trailblazerconfig status

trailblazer is not running
```

启用:

```
sma.local> trailblazerconfig enable

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

启用后，检查状态：

```
sma.local> trailblazerconfig status

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

命名语法示例

启用开拓性的Web访问将包括URL地址中的开拓性端口：

- NGSMA管理门户显示为：https://hostname:4431/ng-login
- NGSMA最终用户隔离（或ISQ）门户显示为：https://hostname:4431/euq-login

故障排除

一些实施侧重于垃圾邮件通知的辅助界面。如果管理接口“主机名”在DNS中无法解析(即**nslookup *hostname***)，则开拓者将无法初始化。

立即确认和恢复服务的一个操作是向管理接口添加可解析的主机名。（然后创建A记录以正确解析指定的主机名。）

用户端安全限制阻止从用户环境访问SMA 4431 TCP端口：

1. 测试以确保该端口对浏览器可用
2. 将主机名和端口输入为：
   https://hostname:4431

TCP端口443未打开

- **IE11:无法显示此页**
- **Chrome:无法访问此站点。拒绝连接**
- **Firefox:无法连接**

TCP端口4431打开且已接受证书

- **IE:HTTP 406**
- **Chrome:{"error":{"消息":"未授权。","代码":“40**
  “解释”："401 =无权限 — 请参阅授权方案。"}

- **Firefox:证书提示(ACCEPT)。 Firefox:post certificate acception > "unauthorized"。 401**

正确的URL语法：

- 启用非开拓性的系统不会在名称中使用端口4431: https://hostname/ng-login

  — 或 — https:// *hostname*/euq-login

- 启用开拓性的系统名称中将包含端口号4431: https://hostname:4431/ng-login

  — 或 — https:// *hostname*:4431/euq-login