使用访问列表过滤发往Cisco IOS XE设备WebUI的流量

目录

简介

本文档介绍如何在Cisco IOS XE设备上配置访问列表(ACL)，以过滤发往Web服务的流量。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档针对运行Cisco IOS® XE软件的企业设备编写。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

当需要启用HTTP Web服务以具有WebUI访问权限来管理IOS XE设备或进行Web身份验证/访客用户访问时，可以实施流量过滤功能，以确保只有必要的IP地址可以访问WebUI，并且访客用户可以继续加入网络。

配置

HTTP服务访问类配置

定义访问的最简单方法可以通过HTTP Web服务器上的IP访问类支持来完成。 在此配置示例中，允许ipv4子网192.168.10.0/24，允许ipv6子网fd00::/64，并且拒绝其他所有内容。 访问列表末尾有一个隐式deny any any，但如果您愿意，还可以添加一个显式deny any any。对于C9800无线局域网控制器，请务必考虑对无线管理接口(WMI)和带外管理/服务端口的HTTP/HTTPS访问。

IPv4 示例

步骤1:配置标准ACL并包括允许通过HTTP/HTTPS访问Cisco IOS XE设备的受信任设备/子网

```
ip access-list standard restrict_ipv4_webui
permit 192.168.10.0 0.0.0.255
```

注意：此ACL必须仅包含受信任的子网，以便对IOS XE设备具有Web管理员访问权限。也就是说，此ACL中不得包含任何访客子网。不包括访客子网不会中断Web身份验证、访客访问或Web重定向。

第二步：将标准ACL分配给HTTP Web服务access-class。

```
ip http access-class ipv4 restrict_ipv4_webui
```

IPv6 示例

步骤1:配置IPv6 ACL包括允许通过HTTP/HTTPS访问Cisco IOS XE设备的受信任设备/子网

```
ipv6 access-list restrict_ipv6_webui
permit fd00::/64 any
```

第二步：将标准ACL分配给HTTP Web服务功能。

```
ip http access-class ipv6 restrict_ipv6_webui
```

验证

检查IPv4 ACL条目

```
show ip access-list restrict_ipv4_webui
Standard IP access list restrict_ipv4_webui
10 permit 192.168.10.0 0.0.0.255
```

检查IPv6 ACL条目

```
show ipv6 access restrict_ipv4_webui
IPv6 access list restrict_ipv6_webui
permit ipv6 FD00::/64 any sequence 10
```

问：应用访问列表后，我获得403响应，而不是无响应。 为什么？

答：这是预期行为。 access-list用于限制允许哪些人访问http/https进程。 403响应表示您被禁止访问此资源，并且是此场景中的正确响应，因为访问列表应用到HTTP/HTTPS进程，而不是接口级别访问列表。 如果访问列表应用于接口而不是HTTP/HTTPS进程，则没有适当的响应

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。