在使用IPv6 ACL的情況下解決完整的IPv6資料包丟棄

目錄

簡介

本文檔介紹ACE中帶有全零字首的IPv6 ACL可以匹配所有IPv6資料包及其解決方法。

必要條件

需求

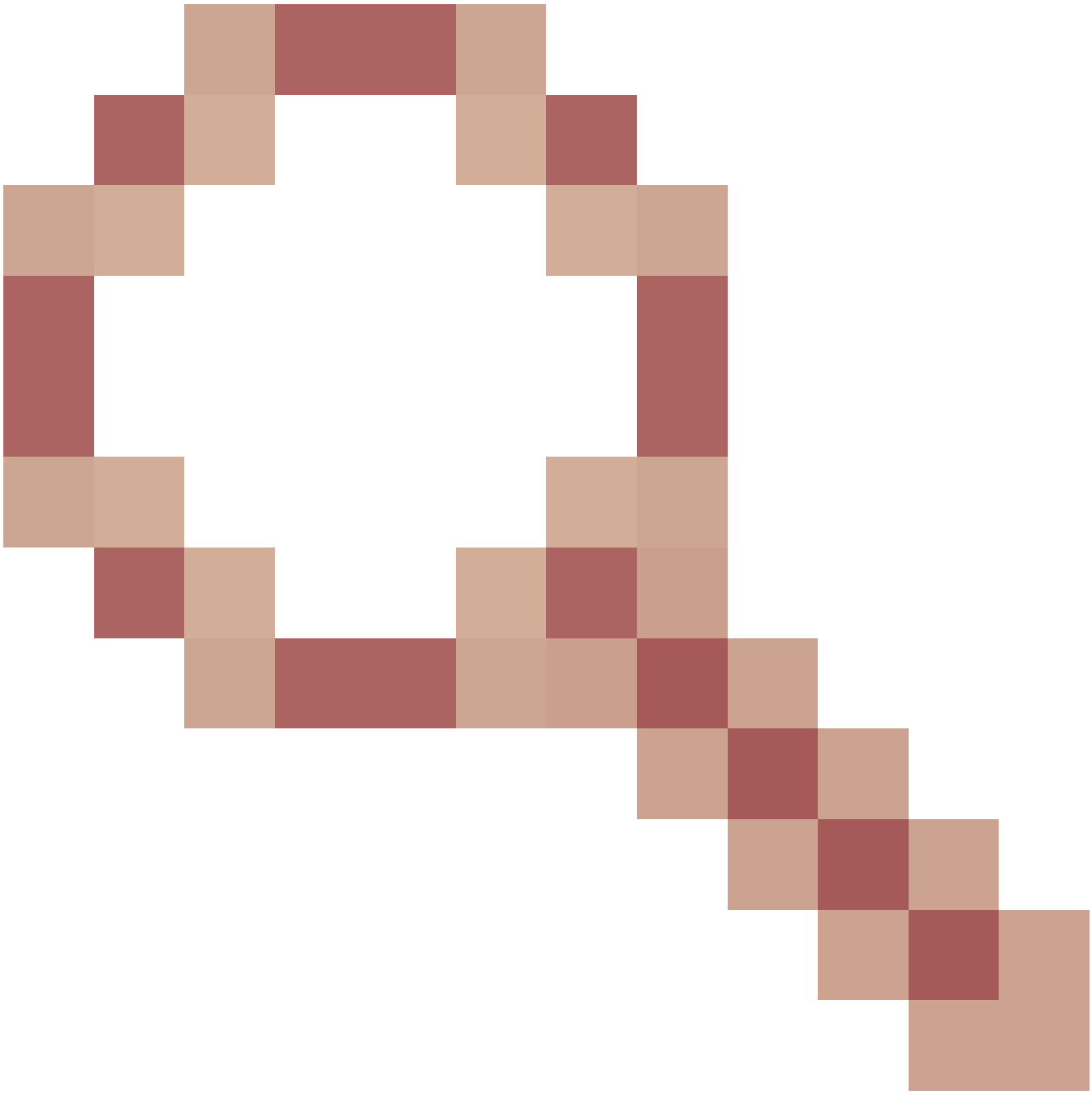
思科建議您瞭解以下主題：

- 思科IOS® XR路由器上的IPv6 ACL（訪問控制清單）配置
- Cisco IOS® XR路由器上的ACL硬體程式設計

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- IPv6 ACL應用壓縮級別2或3
- 思科IOS® XR版本，不修復思科漏洞ID CSCwe08250



本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

IPv6地址：：/128保留給RFC(請求註解) 4291中未指定的地址。它絕不能分配給任何節點，因此最佳做法是在IPv6 Bogon過濾中拒絕此地址。

問題

包含：：/128的ACE（訪問控制條目）的IPv6 ACL可以匹配其應用到的介面上的任何IPv6資料包。

下面是實驗中的觀察示例。

使用：：/128分別配置與IPv6源地址和目標地址匹配的IPv6 ACL：

```
ipv6 access-list PREFIX_ALL_ZERO
 10 remark ** HOST MASK **
 11 deny ipv6 any host :: log
 12 deny ipv6 host :: any log
```

將PING(資料包網際網路或網間分組器)流量傳送到非零IPv6目標地址：

```
RP/0/RP0/CPU0:router#ping fd00:4860:1:1::150 count 100 timeout 0
Thu Sep 14 12:30:23.412 UTC
pings with timeout=0 may result in system instability and
control protocol flaps resulting in traffic impact.
Do you really want to continue[confirm with only 'y' or 'n'] [y/n] :y
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to FD00:4860:1:1::150, timeout is 0 seconds:
....................................................................................................
Success rate is 0 percent (0/100)
```

ACE11丟棄了資料包：

```
RP/0/RP0/CPU0:router#show access-lists ipv6 PREFIX_ALL_ZERO hardware ingress lo
Thu Sep 14 12:30:46.346 UTC
ipv6 access-list PREFIX_ALL_ZERO
11 deny ipv6 any host :: log (100 matches)
12 deny ipv6 host :: any log
```

刪除ACE 11時，丟棄將移動到ACE 12：

```
RP/0/RP0/CPU0:router#clear access-list ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0
Thu Sep 14 12:31:34.899 UTC
```

RP/0/RP0/CPU0:router#ping fd00:4860:1:1::150 count 100 timeout 0

Thu Sep 14 12:31:39.482 UTC

pings with timeout=0 may result in system instability and

control protocol flaps resulting in traffic impact.

Do you really want to continue[confirm with only 'y' or 'n'] [y/n] :y

Type escape sequence to abort.

Sending 100, 100-byte ICMP Echos to FD00:4860:1:1::150, timeout is 0 seconds:

.....

Success rate is 0 percent (0/100)

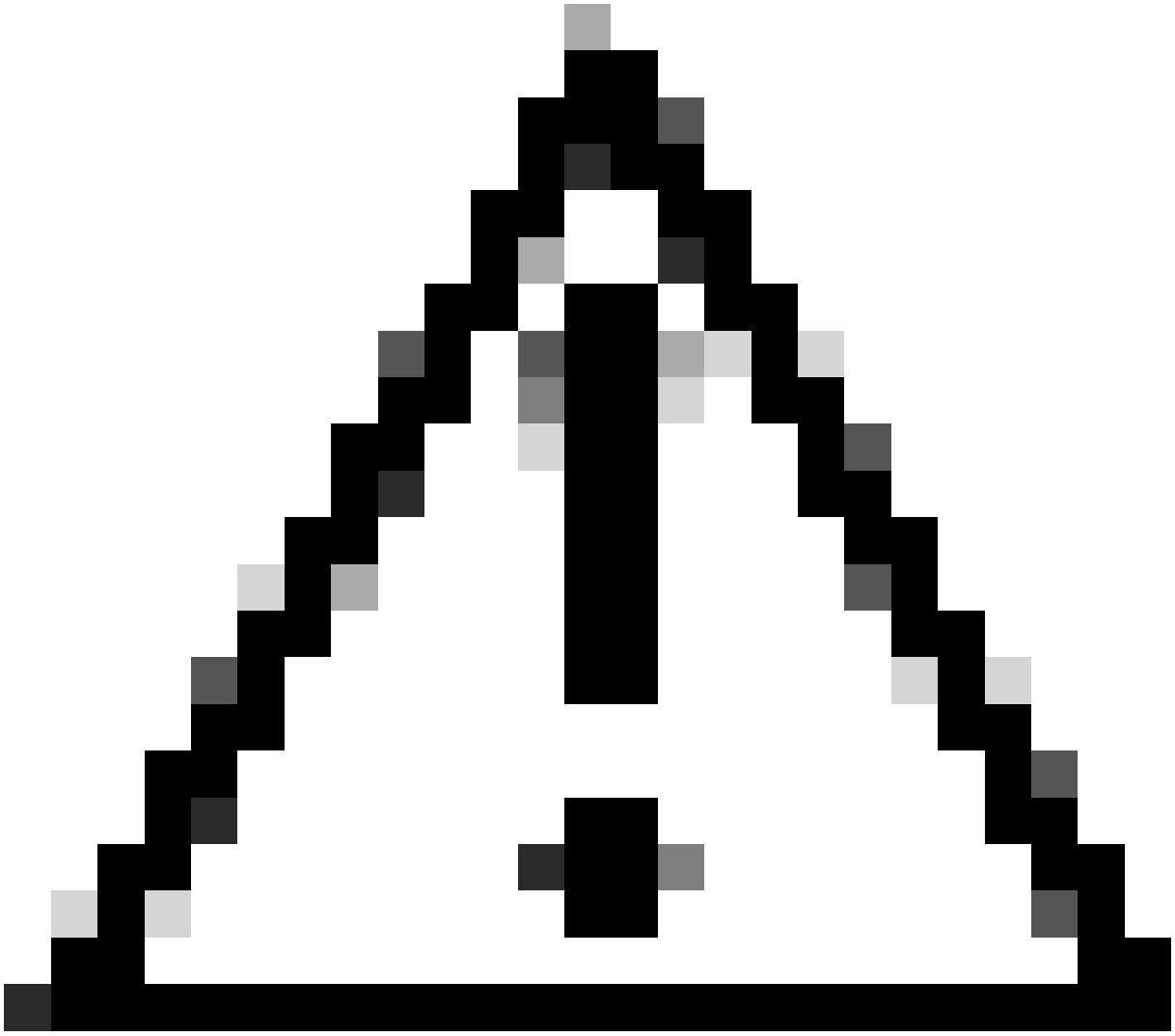
RP/0/RP0/CPU0:router#show access-lists ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0

Thu Sep 14 12:31:45.229 UTC

ipv6 access-list PREFIX_ALL_ZERO

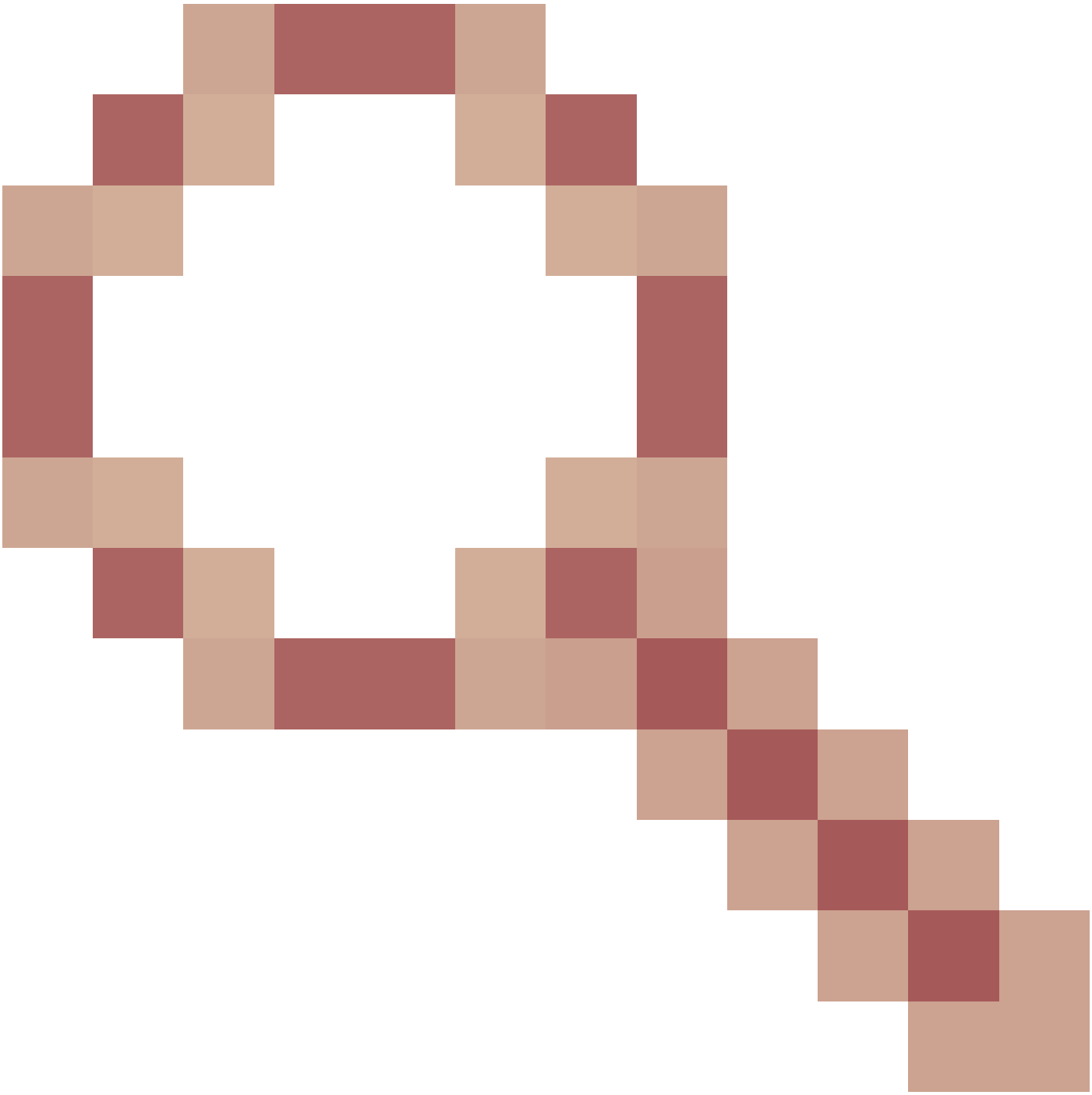
12 deny ipv6 host :: any log (100 matches)

這些ACE應該只丟棄源地址或目標地址全部為零的資料包。
但是，所有流量（即使源或目標不是全部為零）都將被丟棄。



注意：此不匹配行為適用於ACE的從/1到/128的IPv6子網標籤長度，而不只是示例中的/128。

解決方案



修正了Cisco Bug ID CSCwe08250的Cisco IOS® XR版本可更正此錯誤行為。

在運行沒有此修復程式的Cisco IOS® XR路由器上，存在一種解決方法：

- 使用混合ACL並將：：/<x>從ACL移動到網路object-group，以匹配全部為零的源地址或目標地址。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。