IPv6 ACLが使用されている場合の完全なIPv6パケットドロップの解決

内容

はじめに

このドキュメントでは、ACE内のすべてのプレフィクスがゼロのIPv6 ACLがすべてのIPv6パケットに一致する可能性があることと、その回避策について説明します。

前提条件

要件

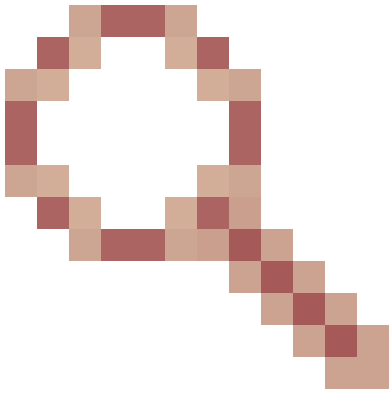
次の項目に関する知識があることが推奨されます。

- Cisco IOS® XRルータでのIPv6 ACL（アクセスコントロールリスト）の設定
- Cisco IOS® XRルータでのACLハードウェアプログラミング

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IPv6 ACLは圧縮レベル2または3で適用される



- Cisco IOS® XRリリース(Cisco Bug ID CSCwe08250の修正なし)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

IPv6アドレス：:/128は、RFC(Request For Comments)4291で未指定アドレス用に予約されています。このアドレスはどのノードにも割り当ててはならないため、IPv6 Bogonフィルタリングでこのアドレスを拒否することがベストプラクティスです。

問題

::/128のアクセスコントロールエントリ(ACE)を含むIPv6 ACLは、それが適用されたインターフェイス上の任意のIPv6パケットと一致できます。

ラボでの観察例を次に示します。

IPv6送信元アドレスと宛先アドレスにそれぞれ一致する：:/128を使用してIPv6 ACLを設定します。

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

ゼロ以外のIPv6宛先アドレスにPING(パケットインターネットまたはインターネットワーク探索機)トラフィックを送信しています：

```
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)
```

パケットがACE11によってドロップされました：

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

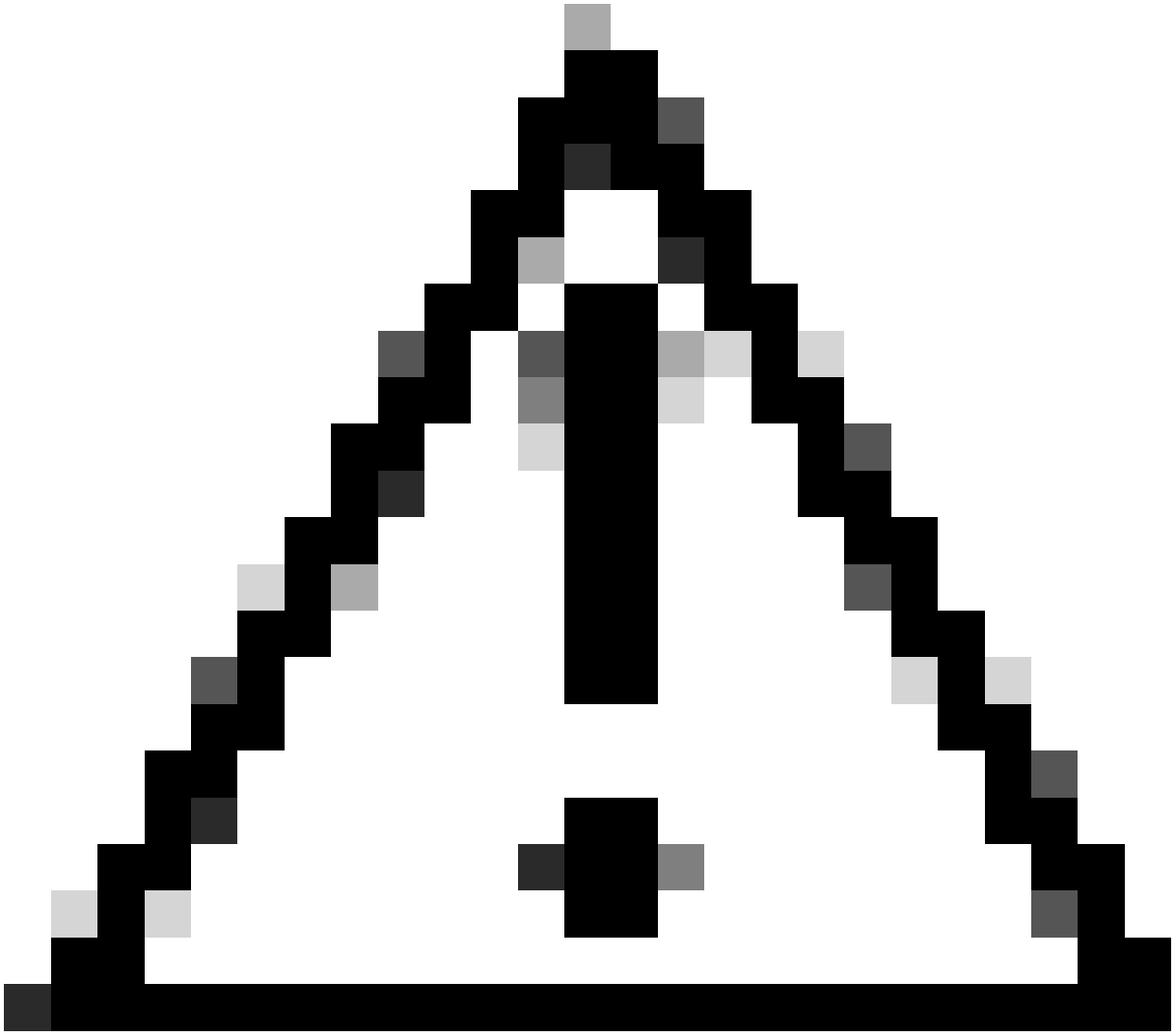
ACE 11を取り外すと、ドロップはACE 12に移動します。

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)

これらのACEでは、送信元アドレスまたは宛先アドレスがすべて0のパケットだけが廃棄されます。
ただし、送信元または宛先がすべてゼロでなくても、すべてのトラフィックがドロップされていました。



注意：このミスマッチ動作は、例の/128だけでなく、ACEの/1から/128までのIPv6サブネットマーク長に適用されます。

解決方法

Cisco IOS® XRリリース(Cisco Bug ID CSCwe08250の修正を含む)では、この誤った動作が修正されています。

この修正が適用されていない状態で稼働しているCisco IOS® XRルータには、次の回避策があります。

- ハイブリッドACLを使用し、ACLからネットワークオブジェクトグループに：:/<x>を移動して、すべて0の送信元アドレスまたは宛先アドレスと照合します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。