Cisco IOS ファイアウォール設定のトラブルシューティング

目次

概要

このドキュメントでは、Cisco IOS® Firewall 設定をトラブルシューティングするために使用できる情報を提供します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

トラブルシューティング

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- アクセス リストの内容を反転（削除）するには、インターフェイス コンフィギュレーション モードで **access-group コマンド**の先頭に「no」を付けます。

```
int <interface>
no ip access-group # in|out
```

- 非常に大量のトラフィックが拒否されている場合は、定義しているリストのロジックを調べるか、より許可対象範囲の広い別のリストを定義して、代わりに適用してみてください。 次に、例を示します。

```
access-list # permit tcp any any
access-list # permit udp any any
access-list # permit icmp any any
int <interface>
ip access-group # in|out
```

- **show ip access-lists コマンド**では、割り当てられているアクセス リストと、拒否されているトラフィックを表示します。 操作に失敗した前後で拒否されたパケットの数を、送信元と送信先の IP アドレスについて調べている場合、アクセス リストがトラフィックをブロックしていると、パケット数は増加します。
- ルータの負荷が高くない場合は、拡張アクセス リストまたは IP 検査のアクセス リストに対してパケット レベルでのデバッグを行うことができます。 ルータの負荷が高い場合、トラフィックはルータ経由で遅くなります。 デバッグ コマンドは慎重に使用してください。一時的にインターフェイスに **no ip route-cache コマンド**を追加します。

```
int <interface>
no ip route-cache
```

次に、イネーブル モード (設定モードではなく) に入ります。

```
term mon
debug ip packet # det
```

次のような出力が表示されます。

```
term mon
debug ip packet # det
```

- 拡張したアクセス リストは、さまざまな文の末尾に「log」オプションを付けて使用する場合もあります。

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

これにより、許可および拒否されたトラフィックに関するメッセージが画面上に表示されるようになります。

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

- IP 検査リストが疑わしい場合、**debug ip inspect <type_of_traffic>** コマンドを実行すると、次のような出力が表示されます。

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

これらのコマンド、およびその他のトラブルシューティング情報については、認証プロキシのトラブルシューティングを参照してください。

関連情報

- Cisco IOS Firewall 製品のサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems