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する固有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。

- （取除く）アクセス リストを反転させるために、インターフェイス設定モードに **access-group コマンド**の前の「いいえ」置かないで下さい:`int <interface>no ip access-group # in|out`
- たくさんのトラフィックが拒否される場合、リストの口ジックを調査しか、または追加広範囲 の リストを定義することを試み次にそれを代りに加えて下さい。 次に、例を示します。`access-list # permit tcp any anyaccess-list # permit udp any anyaccess-list # permit icmp any anyint <interface>ip access-group # in|out`
- **show ip access-lists コマンドは**どのアクセス リストが適用し、どんなトラフィックがそれらによって拒否されるか示します。 送信元 および 宛先 IPアドレスの失敗した操作の前後に否定されるパケットカウントを検知 する場合アクセス リストがトラフィックをブロックする場

合この数増加。

- 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。 ルータが過剰にロードされる場合、トラフィックはルータを通して遅れます。 デバッギングコマンドで思慮分別を使用して下さい。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`それから、イネーブル（しかしない構成）モードで:`term mondebug ip packet # det`これと同じような出力を生成 します:`term mondebug 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 logaccess-list 101 permit ip any any`従って割り当てられるについては画面のメッセージが拒否されたトラフィック表示され、:`access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 logaccess-list 101 permit ip any any`
- ip inspect リストが疑わしい場合、**debug ip inspect <type_of_traffic>** コマンドはこの出力のような出力を生成 します:`access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 logaccess-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（英語）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