アクセス コントロール リストの概要

アクセス リストは、パケットをデバイスのインターフェイスで転送するかブロックするかを制御して、ネットワーク トラフィックをフィルタリングします。デバイスは各パケットを調べ、アクセス リスト内で指定されている基準に基づいて、そのパケットの転送またはドロップを決定します。

アクセス リストで指定できる条件には、トラフィックの発信元アドレス、トラフィックの宛先アドレス、または上位層のプロトコルなどが含まれます。

（注） これらのリストは認証を必要としないため、一部のユーザは基本的なアクセス リストを回避できる可能性があります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

アクセス コントロール リストについて

アクセス リストの定義

アクセス リストとは、少なくとも 1 つの **permit** ステートメント、および任意の 1 つまたは複数の **deny** ステートメントで構成される順次リストです。IP アドレス リストの場合、ステートメントは IP アドレス、上位層の IP プロトコルなどの IP パケットのフィールドに適用できます。アクセス リストは名前または番号で識別および参照されます。アクセスリストはパケット フィルタとして動作し、アクセス リストに定義されている条件に基づいてパケットのフィルタ処理を行います。

アクセスリストを設定しても、アクセスリストがインターフェイスまたは仮想端末回線（VTY）に適用されるか、アクセス リストを受け入れるコマンドで参照されるまでは、有効になりません。複数のコマンドから同じアクセス リストを参照できます。

次に、branchoffices という名前の IP アクセス リストを作成するための設定例を示します。ACL は着信パケットのシリアル インターフェイス 0 に適用されます。このインターフェイスにアクセスできるのは、個々の各送信元アドレスとマスク ペアで指定されているネットワーク上の送信元のみです。ネットワーク 172.20.7.0 上の送信元から発信されるパケットの宛先に、制限はありません。ネットワーク 172.29.2.0 上の送信元から発信されるパケットの宛先は、172.25.5.4 にする必要があります。

```
ip access-list extended branchoffices
 10 permit 172.20.7.0 0.0.0.3 any
 20 permit 172.29.2.0 0.0.0.255 host 172.25.5.4
!
interface serial 0
 ip access-group branchoffices in
```

アクセス コントロール リストの機能

アクセス リストを設定する理由は多数あります。たとえば、ルーティング アップデートのコンテンツの制限や、トラフィック フローの制御などです。アクセスリストを設定する最も重要な理由の 1 つは、このモジュールの要であるネットワークにセキュリティを提供することです。

アクセスリストを使用することで、ネットワークにアクセスするための基本的なセキュリティ レベルが実現します。デバイスでアクセス リストを設定しないと、デバイスを通過するすべてのパケットに、ネットワーク全体へのアクセスが許可されます。

アクセス リストでは、あるホストにはネットワークの一部へのアクセスを許可する一方、別のホストにはそれと同じ領域へのアクセスを禁止するという定が可能です。次の図では、ホスト A にはヒューマン リソース ネットワークへのアクセスが許可されていますが、ホスト B にはヒューマン リソース ネットワークへのアクセスが禁止されています。

また、アクセス リストを使用して、デバイス インターフェイスで転送またはブロックするトラフィックの種類を定義することもできます。たとえば、電子メール トラフィックのルーティングを許可し、同時にすべての Telnet トラフィックをブロックすることができます。

IP アクセス リストの目的

アクセスリストは、パケットフィルタリングを実行して、ネットワークを介して移動するパケットとその場所を制御します。この処理は、ネットワーク トラフィックを制限し、ユーザやデバイスによるネットワークへのアクセスを制限するのに役立ちます。アクセス リストの用途は多様なので、多くのコマンドの構文でアクセスリストが参照されます。アクセスリストを使用して、次のようなことを実行できます。

- インターフェイスでの着信パケットのフィルタリング
- インターフェイスでの発信パケットのフィルタリング
- アドレスまたはプロトコルに基づくデバッグ出力の制限
- 仮想端末回線アクセスの制御
- 輻輳回避、輻輳管理、プライオリティおよびカスタム キューイングなどの高度な機能に使用されるトラフィックの特定または分類

ACL を設定する理由

アクセスリストを設定する理由は多数あります。たとえば、アクセスリストを使用して、スイッチングアップデートのコンテンツを制限したり、トラフィック フローを制御したりできます。アクセス リストを設定する最も重要な理由の 1 つは、ネットワークに対するアクセスを制御することで、ネットワークに基本レベルのセキュリティを提供することです。デバイスでアクセス リストを設定しない場合、デバイスを通過するすべてのパケットは、ネットワークのすべての部分で許可される可能性があります。

アクセス リストで、ネットワークの一部に対してアクセスを許可するホストと、同じ領域に対してアクセスを禁止するホストを設定できます。たとえば、適切なアクセス リストをデバイスのインターフェイスに適用することで、ホスト A にはヒューマン リソース ネットワークへのアクセスが許可され、ホスト B にはヒューマン リソース ネットワークへのアクセスが禁止されます。

ネットワークの 2 つの部分の間に配置されたデバイスにアクセス リストを使用して、内部ネットワークの特定の部分で発着信するトラフィックを制御できます。

アクセス リストのセキュリティ上の利点を実現するために、少なくとも境界デバイスでアクセス リストを設定する必要があります。境界デバイスとは、ネットワークのエッジにあるデバイスです。このようなアクセス リストは、外部ネットワークから、または内部ネットワークのあまり制御されていない領域から、内部ネットワークの機密性が高い領域に対する基本的なバッファとして機能します。このような境界デバイスでは、デバイスのインターフェイスに設定されている各ネットワーク プロトコルに合わせてアクセス リストを設定する必要があります。インバウンド トラフィック、アウトバウンド トラフィック、またはその両方がインターフェイスでフィルタされるように、アクセス リストを設定できます。

アクセスリストは個々のプロトコルベースで定義されます。つまり、各プロトコルのトラフィック フローを制御する場合、インターフェイスでイネーブルにするプロトコルごとにアクセスリストを定義する必要があります。

アクセス リストのソフトウェア処理

アクセス リストがインターフェイス、vty に適用されるとき、あるいはコマンドで参照されるときの処理方法を説明した一般的な手順を次に示します。この手順は、アクセスリストエントリが 13 以下のアクセス リストに適用されます。

- ソフトウェアが IP パケットや各パケットのテスト部分を受け取ります。これらは、アクセスリストの条件に一度に 1 つずつ（**permit** または **deny** ステートメント）照らし合わせてフィルタリングされます。たとえば、ソフトウェアは、**permit** あるいは **deny** ステートメントの送信元アドレスおよび宛先アドレスに照らし合わせてパケットの送信元アドレスおよび宛先アドレスをテストします。
- パケットがアクセスリストのステートメントに一致しないと、そのパケットはリスト内の次のステートメントに対してテストされます。
- パケットとアクセス リスト ステートメントが一致すると、リスト内の残りのステートメントはスキップされ、パケットは一致したステートメントに指定されたとおりに許可または拒否されます。パケットが許可されるか拒否されるかは、パケットが一致する最初のエントリによって決まります。つまり、一致すると、それ以降のエントリは考慮されません。
- いずれの条件とも一致しなかった場合、パケットは廃棄されます。これは、各アクセスリストが暗黙の **deny** ステートメントで終了するためです。言い換えると、パケットが各ステートメントに対してテストされたときまでに許可されないと、このパケットは拒否されます。

13 を超えるエントリが含まれるアクセス リストは、trie ベースのルックアップ アルゴリズムを使用して処理されます。このプロセスは自動的に行われます。設定する必要はありません。

アクセス リストのルール

アクセス コントロール リスト（ACL）には、次のルールが適用されます。

- 1 つのインターフェイス、1 つのプロトコル、1 つの方向につき、許可されるアクセス リストは 1 つだけです。
- アクセス リストには少なくとも 1 つの **permit** ステートメントが含まれる必要があります。そうしないと、ネットワークに入るすべてのパケットが拒否されます。
- アクセスリスト条件または一致基準の構成順序は重要です。パケットを転送するかブロックするかを決定するときに、Cisco ソフトウェアは、それぞれの条件ステートメントに対してステートメントの作成順にパケットをテストします。一致が見つかると、条件ステートメントはそれ以上チェックされません。同じ **permit** または **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- アクセスリストを名前によって参照したときに、そのアクセスリストが存在しない場合は、すべてのパケットが通過します。インターフェイスまたはコマンドに空のアクセスリストを適用すると、ネットワークに対するすべてのトラフィックが許可されます。

- 標準のアクセス リストと拡張のアクセス リストの名前は同じにできません。
- パケットがアウトバウンド インターフェイスに送信される前に、インバウンド アクセス リストがパケットを処理します。ネットワークへのパケット アクセスを拒否するフィルタ条件があるインバウンド アクセス リストは、ルート ルックアップ時のオーバーヘッドを削減します。構成されたフィルタ基準に基づいてネットワークへのアクセスを許可されたパケットはルーティング処理されます。着信アクセス リストの場合、**permit** ステートメントを構成するとパケットは受信後に処理され、**deny** ステートメントを構成するとパケットは破棄されます。
- 発信アクセス リストの場合、パケットの処理後にデバイスから送信されます。着信パケットは発信インターフェイスにルーティングされてから、発信アクセス リストで処理されます。発信アクセス リストの場合、**permit** ステートメントを構成するとパケットは出力バッファに送信され、**deny** ステートメントを構成するとパケットは破棄されます。

（注）

- アクセス リストで、デバイスに到達するトラフィック、またはデバイス経由で送信されるトラフィックは制御できますが、デバイスが送信元のトラフィックは制御できません。

IP アクセス リストを作成する際に役立つヒント

意図しない結果を回避し、より効率的なアクセス リストを作成するために役立つヒントを紹介します。

- アクセス リストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙の **deny** ステートメントによって即時のアクセスに問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。そうでない場合、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- 最初に（**permit** または **deny** ステートメントに対する）一致が見つかった後は条件のテストが終了するため、パケットが一致する可能性の高いステートメントをアクセス リストの先頭に配置すると処理にかかる時間とリソースが削減されます。最も頻繁に発生する条件を発生頻度の低い条件より前に配置します。
- ネットワークまたはサブネットのより具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。
- まだ拒否されていないその他のパケットすべてを許可する場合、ステートメント **permit any any** を使用します。ステートメント **permit any any** を使用すると、実質的に、アクセス リストの末尾にある暗黙の deny ステートメントでその他すべてのパケットが拒否されることを防

ぎます。最初のアクセス リスト エントリは、**permit any any** にしないでください。すべてのトラフィックが通過し、以降のテストに到達するパケットがなくなります。**permit any any** を指定すると、まだ拒否されていないすべてのトラフィックが通過します。

- すべてのアクセス リストは、暗黙の **deny** ステートメントで終わりますが、明示的な **deny** ステートメント（たとえば、**deny ip any any** など）を使用することを推奨します。ほとんどのプラットフォームでは、**show access-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny** ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。
- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。
  - 番号付きアクセス リストからはエントリを削除できません。削除しようとすると、アクセス リスト全体が削除されます。エントリを削除する必要がある場合、アクセス リスト全体を削除してから最初から作り直す必要があります。
  - 名前付きアクセス リストからはエントリを削除できます。**no permit** または **no deny** コマンドを使用して、該当するエントリを削除します。
- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。
- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **log** ステートメントを指定した **deny** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセス リストの配置に適用されます。リソースを保存しようとすると、着信アクセス リストでは常にフィルタ条件を適用した後に、ルーティング テーブルの検索を行います。発信アクセス リストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

アクセスを制御するためにフィルタできる IP パケット フィールド

拡張アクセス リストを使用すると、IP パケットに含まれる次の任意のフィールドについてフィルタできます。送信元アドレスおよび宛先アドレスは、アクセス リストの基礎として最もよく指定される 2 つのフィールドです。

- 送信元アドレス - 特定のネットワーキング デバイスまたはホストから送信されるパケットを制御するために、送信元アドレスを指定します。
- 宛先アドレス - 特定のネットワーキング デバイスまたはホストに対して送信されるパケットを制御するために、宛先アドレスを指定します。
-

送信元アドレスと宛先アドレス

IP パケットの送信元アドレスと宛先アドレスのフィールドは、アクセス リストの基礎となる典型的な 2 つのフィールドです。送信元アドレスを指定して、特定のネットワーキング デバイスまたはホストから送信されるパケットを制御します。宛先アドレスを指定して、特定のネットワーキング デバイスまたはホストに送信されるパケットを制御します。

アクセス リストのアドレスに対するワイルドカード マスク

アドレス フィルタリングでは、アクセス リスト エントリ内のアドレス ビットとアクセス リストに送信されるパケットを比較するときに、対応する IP アドレスを確認するか無視するかをソフトウェアに示すために、ワイルドカードマスクを使用します。注意してワイルドカードマスクを設定することで、許可または拒否テストのために 1 つまたは複数の IP アドレスを指定できます。

IP アドレス ビット用のワイルドカード マスクでは、数値 1 と数値 0 を使用して、対応する IP アドレス ビットをどのように扱うかを指定します。1 と 0 は、サブネット（ネットワーク）マスクで意味する内容が対照的なため、ワイルドカード マスクは逆マスクとも呼ばれます。

- ワイルドカード マスク ビット 0 は、対応するビット値を確認することを示します。ビット値は一致する必要があります。
- ワイルドカード マスク ビット 1 は、対応するビット値を無視することを示します。ビット値が一致する必要はありません。

アクセス リスト ステートメントの送信元アドレスまたは宛先アドレスでワイルドカード マスクを指定しない場合、0.0.0.0（すべての値が一致する必要があることを示します）という暗黙的なワイルドカード マスクが想定されます。

サブネット マスクでは、ネットワークとサブネットを示す隣接ビットをマスクにする必要がありますが、それとは異なり、ワイルドカード マスクではマスクに非隣接ビットを使用できます。

次の表に、アクセス リストの IP アドレスおよびマスクと、それに一致すると見なされる対応するアドレスの例を示します。

表 *1*：*IP* アドレス、ワイルドカード マスク、および一致する結果の例

アドレス	Wildcard Mask	一致する結果
0.0.0.0	255.255.255.255	すべてのアドレスはアクセス リスト条件に一致します
172.18.0.0/16	0.0.255.255	ネットワーク 172.18.0.0
172.18.5.2/16	0.0.0.0	ホスト 172.18.5.2 のみが一致します

アドレス	Wildcard Mask	一致する結果
172.18.8.0	0.0.0.7	サブネット 172.18.8.0/29 のみが一致します
172.18.8.8	0.0.0.7	サブネット 172.18.8.8/29 のみが一致します
172.18.8.15	0.0.0.3	サブネット 172.18.8.15/30 のみが一致します
10.1.2.0	0.0.254.255（マスクの非隣接ビット）	10.1.2.0 ～ 10.1.254.0 に含まれる偶数のネットワークに一致します

アクセス リストのシーケンス番号

IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。IP アクセス リスト エントリ シーケンス番号機能の前には、アクセス リスト内のエントリの位置を指定する方法はありませんでした。以前は、既存のリストの途中にエントリを挿入する場合、目的の位置の後にあるすべてのエントリを削除してから、新しいエントリを追加し、削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

この新しい機能を使用すると、アクセスリストエントリにシーケンス番号を追加し、順序を変更することができます。新しいエントリを追加する場合、アクセス リストの目的の位置に挿入されるようにシーケンス番号を指定します。必要に応じて、アクセス リストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。

ACL でサポートされるタイプ

スイッチは、IP ACL とイーサネット（MAC）ACL をサポートしています。

- IP ACL は、TCP、ユーザ データグラム プロトコル（UDP）、インターネット グループ管理プロトコル（IGMP）、およびインターネット制御メッセージ プロトコル（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

サポートされる ACL

スイッチでは、トラフィックをフィルタリングするために、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。レイヤ 2 インターフェイスに適用できるのは IP アクセス リストを 1 つと MAC アドレス リストを 1 つだけです。

ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL を使用できるのは、物理インターフェイスだけです。EtherChannel インターフェイスでは使用できません。ポート ACL は、インバウンド方向のインターフェイスにのみ適用できます。次のアクセス リストがサポートされています。

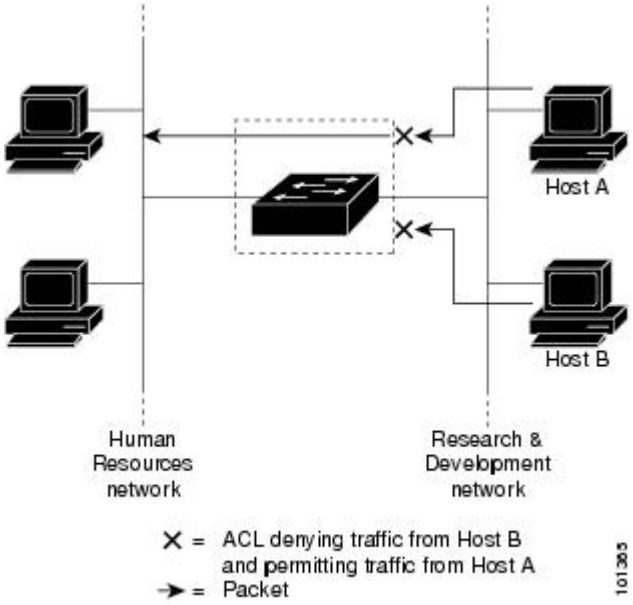
- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。

次に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマン リソース ネットワークにアクセスすることを許可しますが、ホスト B が同一のネッ

トワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2 インターフェイスだけに適用できます。

図 *2*：*ACL* によるネットワーク内のトラフィックの制御



ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。

（注） レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

アクセス コントロール エントリ

ACL には、アクセス コントロール エントリ（ACE）の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

ACE およびフラグメント化されるトラフィックとフラグメント化されていないトラフィック

IPパケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

アクセス コントロール エントリ（ACE）には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報（TCP や UDP などのプロトコル タイプを含む）をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。
- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```

（注） 最初の 2 つの ACE には宛先アドレスの後に *eq* キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれシンプル メール転送プロトコル（SMTP）および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE（permit）と一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ 3 情報だけをチェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。
- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて

揃っているため、最初のフラグメントが 2 つめの ACE（deny）と一致します。残りのフラグメントは、レイヤ 4 情報が含まれていないため、2 つめの ACE と一致しません。残りのフラグメントは 3 つめの ACE（permit）と一致します。

最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。

- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE（deny）と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。