アクセス コントロール リスト(ACL)と IP フラグメント

目次

概要

このホワイト ペーパーでは、各種の Access Control List (ACL; アクセス コントロール リスト) エントリについて、また各種のパケットがそれらのさまざまなエントリとどのように照合されるかについて説明します。 ルータは、ACL を使用して、IP パケットをブロックします。

RFC 1858 は IP断片フィルタリングおよび強調表示するのためのセキュリティ 考察を TCP パケット、小さいフラグメント攻撃およびオーバーラップ フラグメント攻撃の IP フラグメントを含むホストの 2 つの不正侵入カバーします。 これらの不正侵入は、ホストの信頼性を低下させたり、ホスト内部の全リソースを妨害したりする可能性があるため、ブロックすることが求められます。

RFC 1858 は またこれらの不正侵入、直接および間接に対して防御の 2 つのメソッドを記述します。 直接方式では、先頭フラグメントが最小長よりも短いと、廃棄されます。 間接方式では、フラグメント セットの 2 番目のフラグメントが元の IP データグラムの 8 バイトで始まる場合に廃棄されます。 RFC 1858 を詳細については 参照して下さい。

通常、ACL のようなパケット フィルタは、IP パケットが非フラグメント パケットや先頭フラグメントである場合に使用されます。この 2 つのフラグメントには、許可または拒否の決定の際に ACL と照合するためのレイヤ 3 と 4 の両方の情報が含まれているからです。 先頭以外のフラグメントは、通常、パケットのレイヤ 3 情報に基づいてブロックできるので、ACL によって許可されます。 ただし、これらのパケットにはレイヤ 4 の情報が含まれないため、ACL エントリのレイヤ 4 情報が存在していても、その情報と照合できません。 IP データグラムの先頭以外のフラグメントが許可されるのは、ホストがフラグメントを受信しても、先頭フラグメントがないと、元の IP データグラムを再構成できないからです。

また、ファイアウォールを使用すると、発信元と送信先の IP アドレス、プロトコル、および IP ID などでインデックスされたパケット フラグメントのテーブルを整備しておくことにより、パケ

ットをブロックできます。 Cisco PIX ファイアウォールと Cisco IOS® ファイアウォールでは、この情報を備えたテーブルを維持管理することにより、特定のフローの全フラグメントをフィルタリングできます。同じ処理をルータで ACL の基本機能として実行しようとすると、非常にコストがかかります。 ファイアウォールの主要な役割は、パケットのブロックです。副次的な役割として、パケットのルーティングがあります。 一方、ルータの場合は、主要な役割は、パケットのルーティングであり、副次的な役割がパケットのブロックになります。

Cisco IOS ソフトウェア リリース 12.1(2) および 12.0(11) では、TCP フラグメント関連のセキュリティ問題に対処するために、 2 つの変更が加えられました。 間接的方法は、RFC 1858 に記述されているように 、標準 TCP/IP インプットパケット サニティ チェックの一部として設定されていました。 また、先頭以外のフラグメントに関連する ACL の機能も変更されています。

ACL エントリのタイプ

ACL 行には、異なる 6 つのタイプがあり、各タイプにはパケットが一致した場合と不一致の場合の処理内容が定義されています。 次のリストでは、FO = 0 は、TCP フローの非フラグメント パケットまたは先頭フラグメント パケットであることを示しており、FO > 0 は、パケットが先頭以外のフラグメントであることを示しています。また、L3 はレイヤ 3、L4 はレイヤ 4 をそれぞれ表しています。

注: ACL 行にレイヤ 3 とレイヤ 4 の両方の情報が存在しており、さらに **fragments** キーワードが含まれている場合には、ACL の動作では、許可および拒否のどちらについても保守的なアプローチが取られます。 ACL の動作が慎重になるのは、フラグメントにフィルタのアトリビュートすべてを照合するための情報が十分に含まれていないためであり、フローのフラグメント部分を誤って拒否しないようにするためです。 拒否の場合には、先頭以外のフラグメントを拒否せずに、次の ACL エントリが処理されます。 パケットを許可する場合は、パケットにレイヤ 4 情報が存在すればその情報と、ACL 行の レイヤ 4 情報とが一致するという前提で処理されます。

L3 情報のみによる ACL 行の許可

1. パケットの L3 情報が ACL 行の L3 情報と一致すると、パケットは許可されます。
2. パケットの L3 情報がその ACL 行の L3 情報と一致しない場合は、次の ACL エントリが処理されます。

L3 情報のみによる ACL 行の拒否

1. パケットの L3 情報が ACL 行の L3 情報と一致すると、パケットは拒否されます。
2. パケットの L3 情報がその ACL 行の L3 情報と一致しない場合は、次の ACL エントリが処理されます。

L3 情報だけによって ACL 行が許可され、fragments キーワードが存在する場合

パケットの L3 情報が ACL 行の L3 情報と一致すると、パケットのフラグメント オフセットがチェックされます。

1. パケットが FO > 0 の場合、そのパケットは許可されます。
2. パケットが FO = 0 の場合、次の ACL エントリが処理されます。

L3 情報だけによって ACL 行が拒否され、fragments キーワードが存在する場合

パケットの L3 情報が ACL 行の L3 情報と一致すると、パケットのフラグメント オフセットがチェックされます。

1. パケットが FO > 0 の場合、パケットは拒否されます。
2. パケットが FO = 0 の場合、次の ACL 行が処理されます。

L3 および L4 情報による ACL 行の許可

1. パケットの L3 および L4 の情報が ACL 行と一致しており、さらに FO = 0 の場合、パケットは許可されます。
2. パケットの L3 の情報が ACL 行と一致しており、さらに FO > 0 の場合、パケットは許可されます。

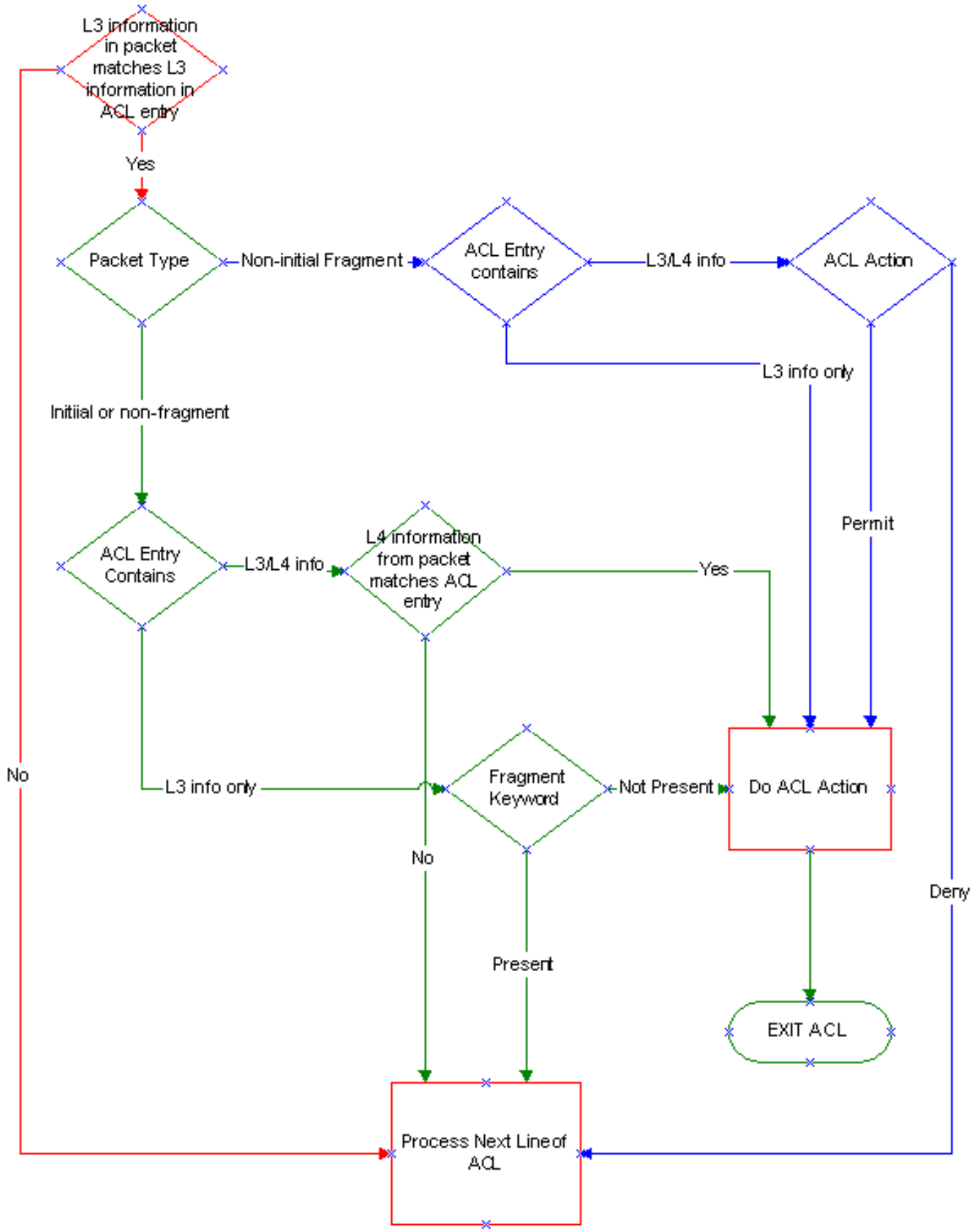
L3 および L4 情報による ACL 行の拒否

1. パケットの L3 および L4 の情報が ACL エントリと一致しており、さらに FO = 0 の場合、パケットは拒否されます。
2. パケットの L3 の情報が ACL 行と一致しており、さらに FO > 0 の場合、次の ACL エントリが処理されます。

ACL 規則のフローチャート

次のフローチャートでは、非フラグメント パケット、先頭フラグメント、および先頭以外のフラグメントが ACL に対してチェックされるときに使用される ACL 規則を示します。

注: 先頭以外のフラグメント自体には、レイヤ 3 の情報だけが含まれ、レイヤ 4 の情報は含まれません。ただし、ACL には、レイヤ 3 とレイヤ 4 の両方の情報が含まれる場合があります。



パケットと ACL の照合方法

例 1

各種のパケットが ACL 100 によって処理される場合には、次の 5 つのシナリオが考えられます。

それぞれの状況でどのように処理が進められるのかを確認しながら、表およびフローチャートを参照してください。 Web サーバの IP アドレスは 171.16.23.1 です。

```
access-list 100 permit tcp any host 171.16.23.1 eq 80 access-list 100 deny ip any any
```

パケットが先頭フラグメントまたは非フラグメント パケットで、送信先がポート 80 のサーバである場合：

ACL の最初の行には、レイヤ 3 およびレイヤ 4 の情報が含まれており、パケットの レイヤ 3 およびレイヤ 4 の情報と一致するので、パケットは許可されます。

パケットが先頭フラグメントまたはフラグメント以外で、送信先がポート 21 のサーバである場合：

1. ACL の最初の行にレイヤ 3 およびレイヤ 4 の情報が含まれますが、ACL のレイヤ 4 情報がパケットの情報と異なるため、次の ACL 行が処理されます。
2. ACL の 2 行目で全パケットを拒否しているため、このパケットは拒否されます。

パケットが先頭以外のフラグメントで、送信先がポート 80 フローのサーバである場合：

ACL の最初の行にはレイヤ 3 およびレイヤ 4 の情報が含まれています。ACL のレイヤ 3 情報はパケットの情報と一致し、ACL が許可しているので、パケットが許可されます。

パケットが先頭以外のフラグメントで、送信先がポート 21 フローのサーバである場合：

ACL の最初の行には、レイヤ 3 およびレイヤ 4 の情報が含まれています。 ACL のレイヤ 3 情報はパケットの情報と一致し、パケットにはレイヤ 4 情報は存在しません。ACL が許可しているので、パケットが許可されます。

パケットが先頭フラグメント、非フラグメント パケット、または先頭以外のフラグメントのいずれかで、送信先がサーバ サブネット上の別のホストである場合：

1. ACL の最初の行に含まれるレイヤ 3 情報が、パケットのレイヤ 3 情報 (送信先アドレス) と一致しないので、次の ACL 行が処理されます。
2. ACL の 2 行目で全パケットを拒否しているため、このパケットは拒否されます。

例 2

各種のパケットが ACL 101 によって処理される場合には、次の 5 つのシナリオが考えられます。例 1 と同じように、それぞれの状況でどのように処理が進められるのかを確認しながら、表およびフローチャートを参照してください。 Web サーバの IP アドレスは 171.16.23.1 です。

```
access-list 101 deny ip any host 171.16.23.1 fragments access-list 101 permit tcp any host 171.16.23.1 eq 80 access-list 101 deny ip any any
```

パケットは先頭フラグメントまたはフラグメント以外で、送信先がポート 80 のサーバの場合：

1. ACL の最初の行にはレイヤ 3 情報が含まれており、パケットのレイヤ 3 情報と一致します。 ACL の動作は拒否ですが、**fragments** キーワードが存在するので、次の ACL エントリが

処理されます。
2. ACL の 2 行目に含まれるレイヤ 3 およびレイヤ 4 の情報がパケットの情報と一致するので、パケットが許可されます。

パケットは先頭フラグメントまたはフラグメント以外で、送信先がポート 21 のサーバの場合：

1. ACL の最初の行にはレイヤ 3 情報が含まれており、パケットの情報と一致します。ただし、ACL エントリには fragments キーワードが存在しており、FO = 0 のパケットとは一致しないため、次の ACL エントリが処理されます。
2. ACL の 2 行目には、レイヤ 3 およびレイヤ 4 の情報が含まれます。 この場合には、レイヤ 4 の情報は一致しないため、次の ACL 項目が処理されます。
3. ACL の 3 行目で全パケットを拒否しているので、このパケットは拒否されます。

パケットが先頭以外のフラグメントで、送信先がポート 80 フローのサーバである場合：

ACL の最初の行にはレイヤ 3 情報が含まれており、パケットのレイヤ 3 情報と一致します。 これは、ポート 80 フローの一部ですが、先頭以外のフラグメントにはレイヤ 4 情報がないことに注意してください。 レイヤ 3 情報が一致するので、パケットは拒否されます。

パケットが先頭以外のフラグメントで、送信先がポート 21 フローのサーバである場合：

ACL の 1 行目には、レイヤ 3 情報だけが含まれており、その情報はパケットと一致するので、パケットは拒否されます。

パケットが先頭フラグメント、非フラグメント パケット、または先頭以外のフラグメントのいずれかで、送信先がサーバ サブネット上の別のホストである場合：

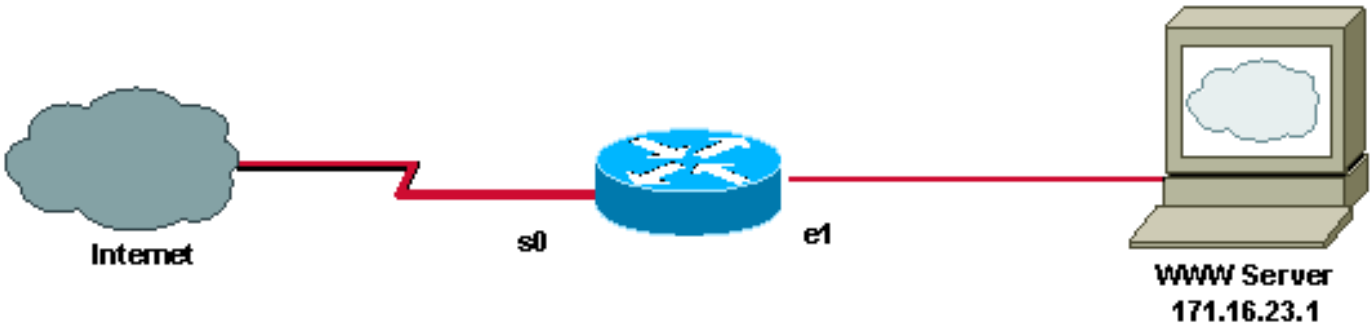
1. ACL の 1 行目にはレイヤ 3 情報だけが含まれており、その情報はパケットの情報と一致しないので、次の ACL 行が処理されます。
2. ACL の 2 行目には、レイヤ 3 およびレイヤ 4 の情報が含まれます。 パケットのレイヤ4 およびレイヤ3 情報は ACL のそれを一致する、従って次の ACL行は処理されます。
3. ACL の 3 行目で、パケットは拒否されます。

fragments キーワードのシナリオ

シナリオ 1

ルータ B は Web サーバと接続しているため、サーバにフラグメントが到達することは望ましくありません。 このシナリオでは、ネットワーク管理者が ACL 100 と ACL 101 を実装した場合に、それぞれの経過の違いを示しています。 ACL はルータの Serial0（s0）インターフェイスの着信に適用されており、フラグメント化していないパケットのみが Web サーバに到達できるようにします。 シナリオを確認しながら、「ACL 規則のフローチャート」および「パケットと ACL の照合方法」のセクションを参照してください。

fragments キーワードを使用した場合の動作



次に示すのは、ACL 100 の例です。

```
access-list 100 permit tcp any host 171.16.23.1 eq 80 access-list 100 deny ip any any
```

ACL 100 の最初の行では、サーバに対して HTTP のみを許可していますが、サーバ上の任意の TCP ポートには、先頭以外のフラグメントも許可しています。 これらのパケットが許可されるのは、ACL ロジックによって、先頭以外のフラグメントにレイヤ 4 情報が含まれなくても、レイヤ 3 情報が一致した場合には、レイヤ 4 も (存在する場合) 一致するものと想定されているからです。 2 行目は、暗黙的にその他すべてのトラフィックを拒否しています。

Cisco IOS ソフトウェア リリース 12.1(2) および 12.0(11) の場合、新しい ACL コードによって、ACL のその他の行と一致しないフラグメントについては、破棄されることに注意してください。 それ以前のリリースでは、ACL のその他の行と一致しなくても、先頭以外のフラグメントが許可されます。

次は ACL 101 の例です。

```
access-list 101 deny ip any host 171.16.23.1 fragments access-list 101 permit tcp any host 171.16.23.1 eq 80 access-list 101 deny ip any any
```

ACL 101 では、最初の行の設定により、サーバへの先頭以外のフラグメントを許可しません。 サーバへの先頭以外のフラグメントは、ACL の最初の行で処理されるときに、拒否されます。パケットのレイヤ 3 情報が、ACL 行のレイヤ 3 情報と一致するためです。

サーバ上のポート 80 への先頭フラグメントや非フラグメント パケットのレイヤ 3 情報は、ACL の最初の行のレイヤ 3 情報とも一致しますが、fragments キーワードが存在するので、次の ACL エントリ (2 行目) が処理されます。 ACL の 2 行目で、レイヤ 3 情報およびレイヤ 4 情報の ACL 行に一致するため、先頭フラグメントや非フラグメント パケットが許可されます。

171.16.23.0 ネットワーク上の他のホストの TCP ポートに送信される先頭以外のフラグメントは、この ACL によってブロックされます。 これらのパケットのレイヤ 3 情報は、ACL の最初の行のレイヤ 3 情報と一致しないので、次の ACL 行が処理されます。 これらのパケットのレイヤ 3 情報は、ACL の 2 行目のレイヤ 3 情報とも一致しないので、ACL の 3 行目が処理されます。 3 行目は、暗黙的にすべてのトラフィックを拒否しています。

ACL 101 はサーバに対して非フラグメント HTTP フローだけを許可するため、このシナリオのネットワーク管理者は、ACL 101 を実装することに決めました。

シナリオ 2

ある顧客の環境では、2 つのサイトがインターネットと接続しており、この 2 つのサイトの間にはバックドア接続も存在します。 ネットワーク管理者のポリシーは、サイト 1 のグループ A が、サイト 2 の HTTP サーバにアクセスできるようにすることです。 両方のサイトのルータはイン

ターネットを通して ルーティングされるパケットを変換するのにプライベートアドレス（RFC 1918）およびネットワーク アドレス変換（NAT）を使用しています。

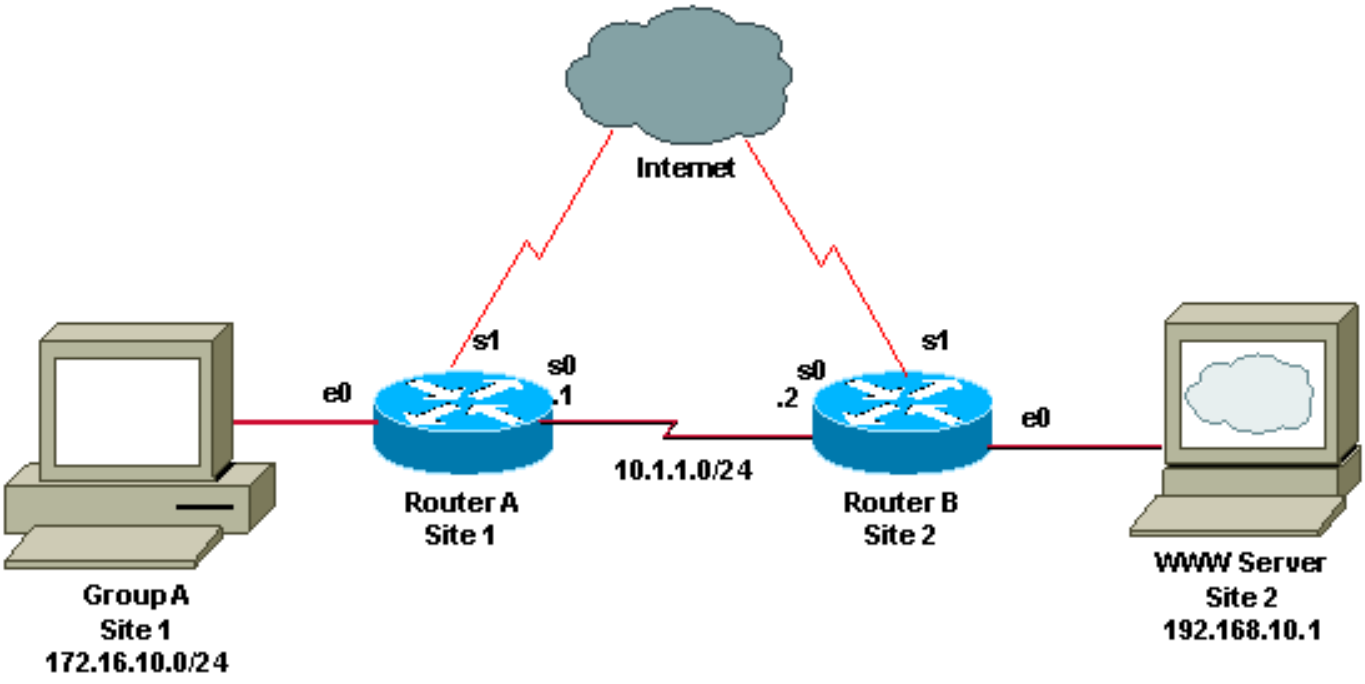
サイト 1 のネットワーク管理者は、グループ A に割り当てられたプライベート アドレスをポリシー ルーティングしています。そのため、サイト 2 の HTTP サーバにアクセスするときに、ルータ A の Serial0 (s0) 経由でバックドアが使用されます。 サイト 2 のルータには、172.16.10.0 宛てのスタティック ルートが設定されています。そのため、グループ A へのリターン トラフィックもバックドア経由でルーティングされます。 その他のトラフィックは、NAT によって処理され、インターネット経由でルーティングされます。 このシナリオのネットワーク管理者は、パケットが分割された場合に、どのアプリケーションまたはフローが動作するかを確認する必要があります。 HTTP と File Transfer Protocol（FTP; ファイル転送プロトコル）の両方のフローを同時に動作させることはできません。

シナリオを確認しながら、「ACL 規則のフローチャート」および「パケットと ACL の照合方法」のセクションを参照してください。

ネットワーク管理者の選択肢に関する説明

次の例では、ルータ A のルート マップ（FOO）が、ACL 100 と一致するパケットを s0 経由でルータ B に送信しています。 一致しないパケットはすべて NAT によって処理され、インターネット経由でデフォルト ルートを通過します。

注: パケットが ACL の最後で破棄されたり、ACL によって拒否された場合、そのパケットはポリシー ルーティングされません。



以下は、ルータ A の構成の一部で、ポリシー ルートマップ（FOO）がインターフェイス e0 に適用されており、そのインターフェイスを通じてグループ A からのトラフィックがルータに着信することを示しています。

```
hostname Router_A int e0 ip policy route-map FOO route-map FOO permit 10 match ip address 100
set ip next-hop 10.1.1.2 access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq
80 access-list 100 deny ip any any
```

ACL 100 を使用する場合、サーバへの HTTP フローの先頭フラグメントと非フラグメント パケ

ット、および先頭以外のフラグメントの両方をポリシー ルーティングできます。 サーバに送信される HTTP フローの先頭フラグメントおよび非フラグメント パケットは、ACL の最初の行に含まれるレイヤ 3 および レイヤ 4 情報と一致するので、ACL によって許可され、ポリシー ルーティングされます。 先頭以外のフラグメントの場合も、ACL によって許可され、ポリシー ルーティングされます。これは、パケットのレイヤ 3 情報が ACL 最初の行と一致した場合、 ACL ロジックでは、パケットのレイヤ 4 情報も（存在する場合）一致するものと想定されているからです。

注: 先頭フラグメントと先頭以外のフラグメントは、異なるパスを経由してサーバに到着するため、ACL 100 では、グループ A とサーバ間のその他のタイプのフラグメント TCP フローが区別されます。 先頭フラグメントは、NAT で処理されて、インターネット経由でルーティングされますが、同じフローの先頭以外のフラグメントは、ポリシー ルーティングされます。

フラグメント化 FTP フローは、このシナリオの問題を具体的に説明するのに役立ちます。 FTP フローの最初のフラグメントは、ACL の最初の行に示されるレイヤ 3 情報と一致しますが、レイヤ 4 情報とは一致しないため、それに続く 2 行目によって拒否されます。 これらのパケットは NAT によって処理され、インターネット経由でルーティングされます。

FTP フローの先頭以外のフラグメントは、ACL の最初の行のレイヤ 3 情報と一致するため、ACL ロジックでは、レイヤ 4 情報も一致するものと想定されます。 これらのパケットはポリシー ルーティングされます。これらのパケットを再構成するホストは、NAT によって先頭フラグメントの発信元アドレスが変更されているため、先頭フラグメントをポリシー ルーティングされた先頭以外のフラグメントと同じフローの一部としては認識しません。

次の構成では、ACL 100 によって FTP の問題を修正しています。 ACL 100 の最初の行で、グループ A からサーバに送られる先頭および先頭以外の FTP フラグメントを拒否しています。

```
hostname Router_A int e0 ip policy route-map FOO route-map FOO permit 10 match ip address 100
set ip next-hop 10.1.1.2 access-list 100 deny tcp 172.16.10.0 0.0.0.255 host 192.168.10.1
fragments access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80 access-list
100 deny ip any any
```

先頭フラグメントは、ACL の最初の行のレイヤ 3 情報と一致しますが、**fragments** キーワードが存在するため、次の ACL 行が処理されます。 先頭フラグメントは、2 行目のレイヤ 4 情報と一致しないため、次の暗黙的な ACL 行が処理され、パケットは拒否されます。 先頭以外のフラグメントは、ACL の 1 行目のレイヤ 3 情報と一致するため、拒否されます。 先頭フラグメントと先頭以外のフラグメントは、そちらも NAT によって処理され、インターネット経由でルーティングされます。そのため、サーバでは再構成に関する問題は発生しません。

FTP フローを修正すると、フラグメント HTTP フローが中断します。これは、HTTP の先頭フラグメントはポリシー ルーティングされていても、先頭以外のフラグメントが NAT によって処理されており、インターネット経由でルーティングされるためです。

グループ A からサーバ宛ての HTTP フローの最初のフラグメントが、ACL の最初の行と遭遇する際、ACL のレイヤ 3 情報とは一致しますが、 **fragments** キーワードが存在するために ACL の次の行が処理されます。 ACL の 2 行目で、パケットは許可されてサーバにポリシー ルーティングされます。

グループ A からサーバへの先頭以外の HTTP フラグメントが ACL の最初の行で処理されると、パケットのレイヤ 3 情報が ACL 行の情報と一致して、パケットは拒否されます。 これらのパケットは NAT によって処理され、インターネット経由でサーバに到着します。

このシナリオでは、ACL の最初の行で、フラグメント HTTP フローについては許可しますが、フラグメント FTP フローは中断します。 ACL の 2 行目では、フラグメント化 FTP フローを許可し

、フラグメント化 HTTP フローは中断します。 いずれの場合も、TCP フローが中断するのは、先頭フラグメントと先頭以外のフラグメントが異なるパスを経由してサーバに送信されるためです。 NAT が先頭以外のフラグメントの発信元アドレスを変更したので、再構成は不可能となります。

両タイプのフラグメント フローがサーバにアクセスできるように ACL を構築することはできません。そのため、ネットワーク管理者はどちらのフローを動作させるのかを選択する必要があります。

関連情報

- IP ルーティングに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems