存取控制清單和IP片段

目錄

簡介

本白皮書介紹了各種不同的訪問控制清單(ACL)條目，以及當不同型別的資料包遇到這些各種條目時會發生的情況。ACL用於阻止路由器轉發IP資料包。

RFC 1858 ，涵蓋IP分段過濾的安全注意事項，並著重說明對TCP資料包IP分段的兩種主機攻擊：微片段攻擊和重疊分段攻擊。阻止這些攻擊是理想的，因為它們可能會危及主機，或者會佔用主機的所有內部資源。

RFC 1858 還介紹了兩種防禦這些攻擊的方法：直接方法和間接方法。在直接方法中，丟棄小於最小長度的初始片段。間接方法涉及丟棄片段集的第二個片段（如果它從原始IP資料包中開始8位元組）。如需詳細資訊，請參閱RFC 1858 。

傳統上，封包過濾器（例如ACL）會套用到IP封包的未片段和初始片段，因為這些封包過濾器包含ACL可以相符作出允許或拒絕決定的第3層和第4層資訊。傳統上允許非初始片段通過ACL，因為可以基於封包中的第3層資訊來封鎖這些片段；但是，由於這些資料包不包含第4層資訊，因此它們與ACL條目中的第4層資訊（如果存在）不匹配。允許IP資料包的非初始片段通過的做法是可接受的，因為接收片段的主機無法重組沒有初始片段的原始IP資料包。

防火牆也可以用於通過維護按源和目標IP地址、協定和IP ID索引的資料包片段表來阻止資料包。Cisco PIX防火牆和Cisco IOS®防火牆都可以通過維護此資訊表來過濾特定流的所有片段，但是在路由器上執行此操作對於基本ACL功能來說成本太高。防火牆的主要工作是阻止資料包，其次要角色是路由資料包；路由器的主要工作是路由封包，而其次要角色是封鎖封包。

在Cisco IOS軟體版本12.1(2)和12.0(11)中進行了兩項變更，以解決圍繞TCP片段的一些安全問題。間接方法(如RFC 1858)是標準TCP/IP輸入封包健全性檢查的一部分。還針對非初始片段更改了ACL功能。

ACL專案的型別

有六種不同型別的ACL行，如果資料包匹配或不匹配，則每種行都會產生後果。在以下清單中，FO = 0表示TCP流中的非分段或初始分段，FO > 0表示資料包為非初始分段，L3表示第3層，L4表示第4層。

注意：當ACL行中同時存在第3層和第4層資訊且存在**fragments**關鍵字時，ACL操作對於permit和deny操作都是保守的。這些操作是保守的，因為您不希望意外拒絕流的碎片部分，因為這些片段不包含足以匹配所有過濾器屬性的資訊。在deny案例中，系統不會拒絕非初始片段，而是會處理下一個ACL專案。在允許的情況下，假設封包中的第4層資訊（如果可用）與ACL行中的第4層資訊相符。

僅允許包含L3資訊的ACL行

1. 如果封包的L3資訊與ACL行中的L3資訊相符，則允許通過。
2. 如果封包的L3資訊與ACL行中的L3資訊不匹配，則會處理下一個ACL專案。

僅包含L3資訊的拒絕ACL行

1. 如果封包的L3資訊與ACL行中的L3資訊相符，就會遭到拒絕。
2. 如果封包的L3資訊與ACL行中的L3資訊不匹配，則會處理下一個ACL專案。

僅允許含有L3資訊的ACL行，且存在fragments關鍵字

如果封包的L3資訊與ACL行中的L3資訊相符，則會檢查封包的片段位移。

1. 如果資料包的FO > 0，則允許該資料包。
2. 如果資料包的FO = 0 ，則會處理下一個ACL條目。

僅包含L3資訊的Deny ACL行，且存在fragments關鍵字

如果封包的L3資訊與ACL行中的L3資訊相符，則會檢查封包的片段位移。

1. 如果資料包的FO大於0，則該資料包將被拒絕。
2. 如果封包的FO = 0，則會處理下一個ACL行。

允許ACL行包含L3和L4資訊

1. 如果封包的L3和L4資訊與ACL行相符，且FO = 0，則允許該封包。
2. 如果封包的L3資訊與ACL行和FO > 0相符，則允許該封包。

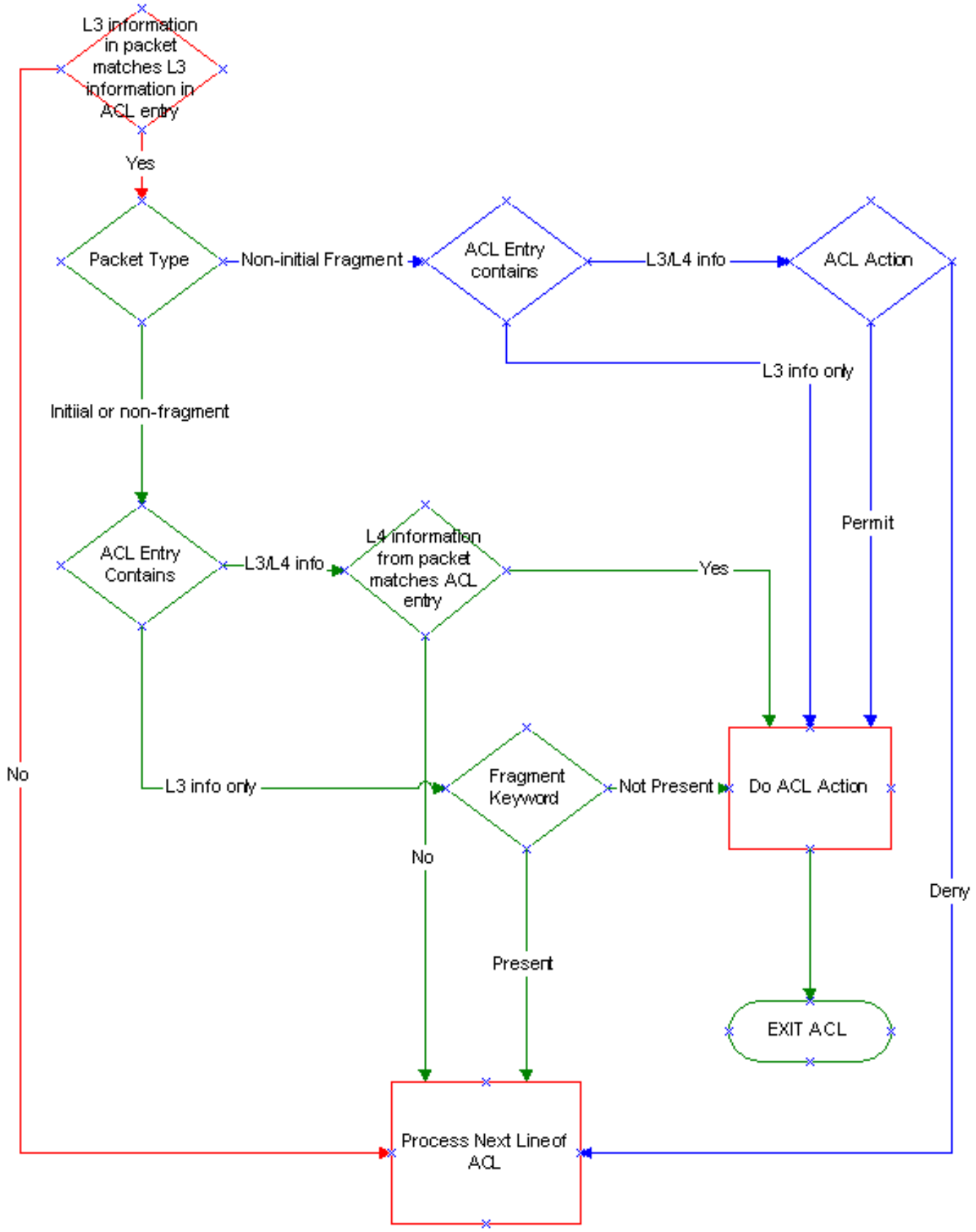
拒絕包含L3和L4資訊的ACL行

1. 如果封包的L3和L4資訊與ACL專案相符，且FO = 0，則封包將遭拒絕。
2. 如果封包的L3資訊與ACL行和FO > 0相符，則處理下一個ACL專案。

ACL規則流程圖

以下流程圖說明了根據ACL檢查非片段、初始片段和非初始片段時的ACL規則。

注意：非初始片段本身僅包含第3層資訊，不包含第4層資訊，儘管ACL可能同時包含第3層和第4層資訊。



封包如何與ACL相符

範例 1

以下五種可能的情況涉及遇到ACL 100的不同型別的資料包。請參閱表和流程圖，瞭解每種情況下會發生的情況。Web伺服器的IP地址是171.16.23.1。

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

access-list 100 deny ip any any
```

封包是目的地為連線埠80上伺服器的初始片段或非片段：

ACL的第一行包含第3層和第4層資訊，它們與資料包中的第3層和第4層資訊匹配，因此允許該資料包。

封包是目的地為連線埠21上伺服器的初始片段或非片段：

1. ACL的第一行包含第3層和第4層資訊，但ACL中的第4層資訊與資料包不匹配，因此會處理下一個ACL行。
2. ACL的第二行拒絕所有資料包，因此資料包被拒絕。

封包是連線埠80流量中傳至伺服器的非初始片段：

ACL的第一行包含第3層和第4層資訊，ACL中的第3層資訊與資料包匹配，且ACL操作為permit，因此允許該資料包。

封包是連線埠21流量中傳至伺服器的非初始片段：

ACL的第一行包含第3層和第4層資訊。ACL中的第3層資訊與資料包匹配，資料包中沒有第4層資訊，且ACL操作是允許的，因此允許該資料包。

封包是到伺服器子網中另一個主機的初始片段、非片段或非初始片段：

1. ACL的第一行包含的第3層資訊與資料包中的第3層資訊（目的地址）不匹配，因此會處理下一個ACL行。
2. ACL的第二行拒絕所有資料包，因此資料包被拒絕。

範例 2

以下五種可能的情況涉及遇到ACL 101的不同型別的資料包。同樣地，請參考表和流程圖，以便您瞭解每種情況下會發生的情況。Web伺服器的IP地址是171.16.23.1。

```
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
```

封包是目的地為連線埠80上伺服器的初始分段或非分段：

1. ACL的第一行包含與資料包中的第3層資訊匹配的第3層資訊。ACL操作是拒絕，但由於存在fragments關鍵字，因此會處理下一個ACL專案。
2. ACL的第二行包含與資料包匹配的第3層和第4層資訊，因此允許該資料包。

封包是目的地為連線埠21上伺服器的初始分段或非分段：

1. ACL的第一行包含與封包相符的第3層資訊，但ACL專案也包含fragments關鍵字，此關鍵字與封包不匹配，因為FO = 0，因此會處理下一個ACL專案。
2. ACL的第二行包含第3層和第4層資訊。在這種情況下，第4層資訊不匹配，因此會處理下一個ACL條目。
3. ACL的第三行拒絕所有封包，因此封包將遭拒絕

封包是連線埠80流量中傳至伺服器的非初始片段：

ACL的第一行包含與資料包中的第3層資訊匹配的第3層資訊。請記住，即使這是連線埠80流量的一部分，非初始片段中也沒有第4層資訊。封包將遭拒絕，因為第3層資訊相符。

封包是連線埠21流量中傳至伺服器的非初始片段：

ACL的第一行僅包含第3層資訊，且它與封包相符，因此封包將遭拒絕。

封包是到伺服器子網中另一個主機的初始片段、非片段或非初始片段：

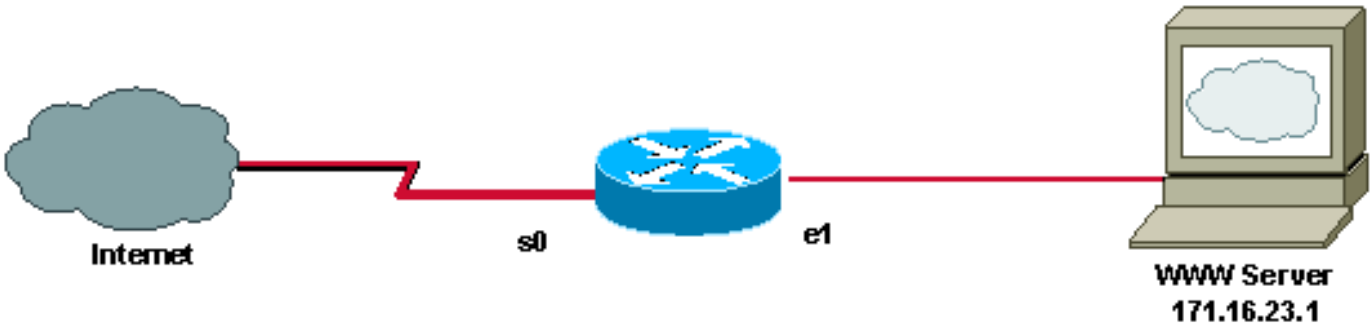
1. ACL的第一行僅包含第3層資訊，但它與資料包不匹配，因此會處理下一個ACL行。
2. ACL的第二行包含第3層和第4層資訊。封包中的第4層和第3層資訊與ACL的資訊不匹配，因此會處理下一個ACL線路。
3. ACL的第三行拒絕此封包

fragments關鍵字方案

案例 1

路由器B連線到Web伺服器，網路管理員不希望允許任何片段到達伺服器。此案例顯示如果網路管理員實作ACL 100而不是ACL 101會發生什麼情況。ACL套用到路由器Serial0(s0)介面的傳入，且應僅允許未分段封包到達Web伺服器。按照場景操作，請參閱ACL規則流程圖和資料包如何匹配ACL部分。

使用fragments關鍵字的後果



以下是ACL 100:

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

access-list 100 deny ip any any
```

ACL 100的第一行只允許對伺服器執行HTTP，但它也允許對伺服器上的任何TCP埠執行非初始分段。它允許這些封包，因為非初始片段不包含第4層資訊，而ACL邏輯會假設如果第3層資訊相符，則第4層資訊也會相符（如果可用）。第二行是隱式的，拒絕所有其他流量。

必須注意的是，自Cisco IOS軟體版本12.1(2)和12.0(11)起，新ACL代碼會捨棄與ACL中任何其他行不符的片段。如果非初始片段與ACL的任何其他行都不匹配，則早期版本允許它們通過。

以下是ACL 101:

```
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
```

由於第一行，ACL 101不允許非初始片段通過到伺服器。當伺服器遇到第一個ACL行時，其非初始片段會被拒絕，因為封包中的第3層資訊與ACL行中的第3層資訊相符。

連線到伺服器上連線埠80的初始分段或非分段也與ACL中第3層資訊的第一行相符，但由於存在fragments關鍵字，因此會處理下一個ACL專案（第二行）。ACL的第二行允許初始片段或非片段，因為它們與第3層和第4層資訊的ACL行相符。

此ACL會封鎖目的地為171.16.23.0網路上其他主機的TCP連線埠的非初始片段。這些封包中的第3層資訊與第一行ACL中的第3層資訊不匹配，因此會處理下一個ACL行。這些封包中的第3層資訊與第二個ACL行中的第3層資訊也不相符，因此會處理第三個ACL行。第三行是隱式的，拒絕所有流量。

在此案例中，網路管理員決定實作ACL 101，因為它僅允許到伺服器的非分段HTTP流量。

案例 2

一個客戶在兩個不同的站點有Internet連線，並且兩個站點之間也有後門連線。網路管理員的策略是允許站點1中的組A訪問站點2的HTTP伺服器。兩個站點的路由器都使用私有地址(RFC 1918)和網路地址轉換(NAT)來轉換通過網際網路路由的資料包。

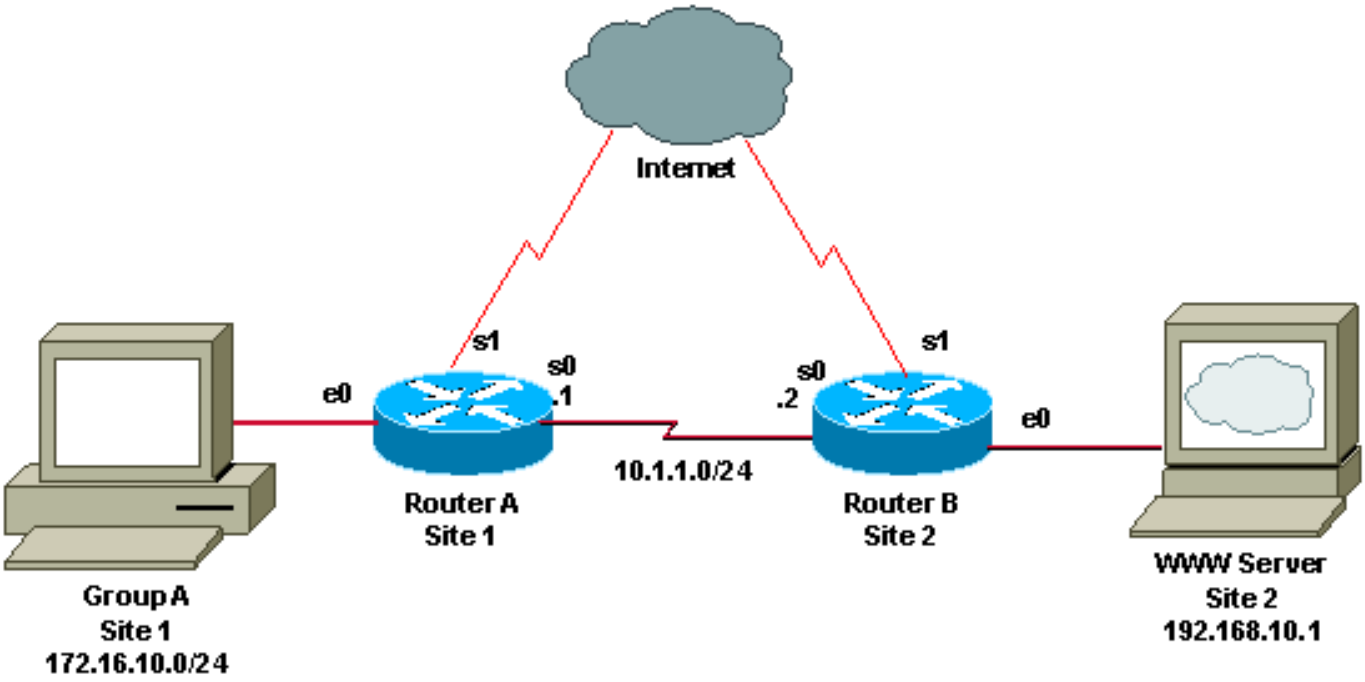
站點1的網路管理員對分配給組A的私有地址執行策略路由，以便在訪問站點2的HTTP伺服器時通過路由器A的Serial0(s0)使用後門。站點2的路由器具有到172.16.10.0的靜態路由，因此返回組A的流量也通過後門路由。所有其他流量都由NAT處理並通過Internet路由。在此案例中，網路管理員必須決定如果資料包被分段，哪個應用程式或流將正常工作。無法使HTTP和檔案傳輸通訊協定(FTP)流量同時運作，因為其中一個或另一個會中斷。

按照場景操作，請參閱ACL規則流程圖和資料包如何匹配ACL部分。

網路管理員選項的說明

在以下示例中，路由器A上名為FOO的路由對映將匹配ACL 100的資料包通過s0傳送到路由器B。所有不匹配的資料包都由NAT處理，並採用Internet的預設路由。

註：如果封包從ACL的底部跌落或遭到拒絕，則不會進行原則路由。



以下是路由器A的部分配置，其中顯示名為FOO的策略路由對映應用於介面e0，來自組A的流量在此進入路由器：

```
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允許HTTP流的初始片段、非片段和非初始片段到伺服器的策略路由。ACL和路由的策略允許到達伺服器的初始HTTP流和非片段，因為它們與第一個ACL行中的第3層和第4層資訊匹配。ACL和路由的策略允許非初始片段，因為封包中的第3層資訊也與第一個ACL行相符；acl邏輯會假設封包中的第4層資訊如果可用，也會相符。

注意：ACL 100會中斷組A和伺服器之間的其他型別的分段TCP資料流，因為初始片段和非初始片段會透過不同的路徑到達伺服器；初始片段由NAT處理並通過Internet路由，但同一流中的非初始片段會被策略路由。

分段的FTP流量有助於說明此案例中的問題。FTP流量的初始片段與第一行ACL的第3層資訊（而非第4層資訊）相符，但接著遭到第二行的拒絕。這些資料包由NAT處理並通過Internet路由。

FTP流量的非初始片段與第一行ACL中的第3層資訊相符，而ACL邏輯會假設第4層資訊為正相符。這些資料包是策略路由的，並且重組這些資料包的主機不會將初始片段識別為與策略路由的非初始片段相同的流的一部分，因為NAT已更改了初始片段的源地址。

下面配置中的ACL 100修復了FTP問題。ACL 100的第一行拒絕將初始和非初始FTP片段從組A傳送到伺服器。

```
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
```

初始片段在第一個ACL行中的第3層資訊上相符，但若存在**fragments**關鍵字，則會處理下一個ACL行。初始片段與第4層資訊的第二個ACL行不相符，因此會處理ACL的下一個隱含行，這會拒絕封包。非初始片段與ACL第一行中的第3層資訊相符，因此會遭到拒絕。初始片段和非初始片段都由NAT處理並通過Internet路由，因此伺服器不存在重組問題。

修復FTP流會中斷分段的HTTP流，因為現在對初始HTTP片段進行策略路由，但非初始片段由NAT處理並通過Internet路由。

從組A到伺服器的HTTP資料流的初始片段遇到該ACL的第一行時，會與ACL中的第3層資訊相符，但由於**fragments**關鍵字，因此會處理ACL的下一行。ACL的第二行允許並將資料包路由到伺服器。

當從組A傳送到伺服器的非初始HTTP片段遇到ACL的第一行時，封包中的第3層資訊會與ACL行相符，且封包會遭到拒絕。這些資料包由NAT處理並通過Internet到達伺服器。

此案例中的第一個ACL允許分段的HTTP流量，並中斷分段的FTP流量。第二個ACL允許分段的FTP流量並中斷分段的HTTP流量。由於初始片段和非初始片段通向伺服器的路徑不同，每種情況下的TCP流都會中斷。無法重組，因為NAT已更改了非初始片段的源地址。

無法構建允許兩種分段流到達伺服器的ACL，因此網路管理員必須選擇要使用的流。

相關資訊

- IP 路由支援頁面
- 技術支援與文件 - Cisco Systems