访问控制列表与 IP 分段

目录

简介

此白皮书解释了不同类型的访问控制列表 (ACL) 条目，以及在不同类型的数据包遇到这些条目时会发生的情况。ACL 用于阻止路由器转发 IP 数据包。

RFC 1858 涵盖IP分段过滤的安全注意事项，并重点介绍对主机的两种攻击，这两种攻击涉及TCP数据包的IP分段，即微分段攻击和重叠分段攻击。必须阻止这些攻击，因为这些攻击会破坏主机，或者占用其所有内部资源。

RFC 1858 还介绍了两种防止这些攻击的方法，即，直接方法和间接方法。 在直接方法中，小于最小长度的初始分段将被丢弃。在间接方法中，如果分段集在原始 IP 数据报中初始为 8 个字节，则该分段集的第二个分段将被丢弃。有关详细信息，请参阅 RFC 1858。

在过去，将数据包过滤器（如 ACL）应用于 IP 数据包的非分段和初始分段，因为 ACL 可以匹配这些分段中包含的第 3 层和第 4 层信息，以决定是允许还是拒绝分段。由于可以根据数据包中的第 3 层信息来阻止非初始分段，因此通常允许此类分段通过 ACL。但是，由于这些数据包不包含第 4 层信息，因此它们不能匹配 ACL 条目中的第 4 层信息（如果存在）。允许 IP 数据报的非初始分段通过是可以接受的，因为在没有初始分段的情况下，收到分段的主机将无法重组原始 IP 数据报。

此外，也可以使用防火墙来阻止数据包，但需要维护一个按源和目标 IP 地址、协议以及 IP ID 编制索引的数据包分段表。Cisco PIX防火墙和Cisco IOS®防火墙都可以通过维护此信息表来过滤特定流的所有分段，但在路由器上执行此操作对于基本ACL功能而言太昂贵。防火墙的主要工作是阻止数据包，其辅助角色是路由数据包。路由器的主要工作是路由数据包，其辅助角色是阻止数据包。

Cisco IOS 软件版本 12.1(2) 和 12.0(11) 中进行了两处更改，以解决与 TCP 分段相关的一些安全问题。在标准 TCP/IP 输入数据包健全性检查中实施了 RFC 1858 中介绍的间接方法。 对于 ACL 功能，也进行了与非初始分段相关的更改。

ACL 条目的类型

有六种不同类型的 ACL 行，每种类型的 ACL 行在数据包匹配或不匹配时都有相应的结果。在以下列表中，FO = 0 表示 TCP 流中的非分段或初始分段，FO > 0 表示数据包是一个非初始分段，L3 表示第 3 层，L4 表示第 4 层。

注意：当ACL行中同时包含第3层和第4层信息且存在**fragments**关键字时，ACL操作对于允许和拒绝操作都是保守的。操作比较保守是因为当分段未包含足够的信息来匹配所有过滤器属性时，您不希望无意中拒绝数据流中的已分段部分。在拒绝情况下，将处理下一个 ACL 条目，而不是拒绝非初始分段。在允许情况下，假定数据包中的第 4 层信息（如果存在）与 ACL 行中的第 4 层信息匹配。

仅包含 L3 信息的允许 ACL 行

1. 如果数据包的 L3 信息与 ACL 行中的 L3 信息匹配，将允许该数据包。
2. 如果数据包的 L3 信息与 ACL 行中的 L3 信息不匹配，将处理下一个 ACL 条目。

仅包含 L3 信息的拒绝 ACL 行

1. 如果数据包的 L3 信息与 ACL 行中的 L3 信息匹配，将拒绝该数据包。
2. 如果数据包的 L3 信息与 ACL 行中的 L3 信息不匹配，将处理下一个 ACL 条目。

仅包含 L3 信息并且出现 fragments 关键字的允许 ACL 行

如果数据包的 L3 信息与 ACL 行中的 L3 信息匹配，将检查数据包的分段偏移。

1. 如果数据包的 FO > 0，将允许该数据包。
2. 如果数据包的 FO = 0，将处理下一个 ACL 条目。

仅包含 L3 信息并且出现 fragments 关键字的拒绝 ACL 行

如果数据包的 L3 信息与 ACL 行中的 L3 信息匹配，将检查数据包的分段偏移。

1. 如果数据包的 FO > 0，将拒绝该数据包。
2. 如果数据包的 FO = 0，将处理下一个 ACL 行。

包含 L3 和 L4 信息的允许 ACL 行

1. 如果数据包的 L3 和 L4 信息与 ACL 行匹配并且 FO = 0，将允许该数据包。
2. 如果数据包的 L3 信息与 ACL 行匹配并且 FO > 0，将允许该数据包。

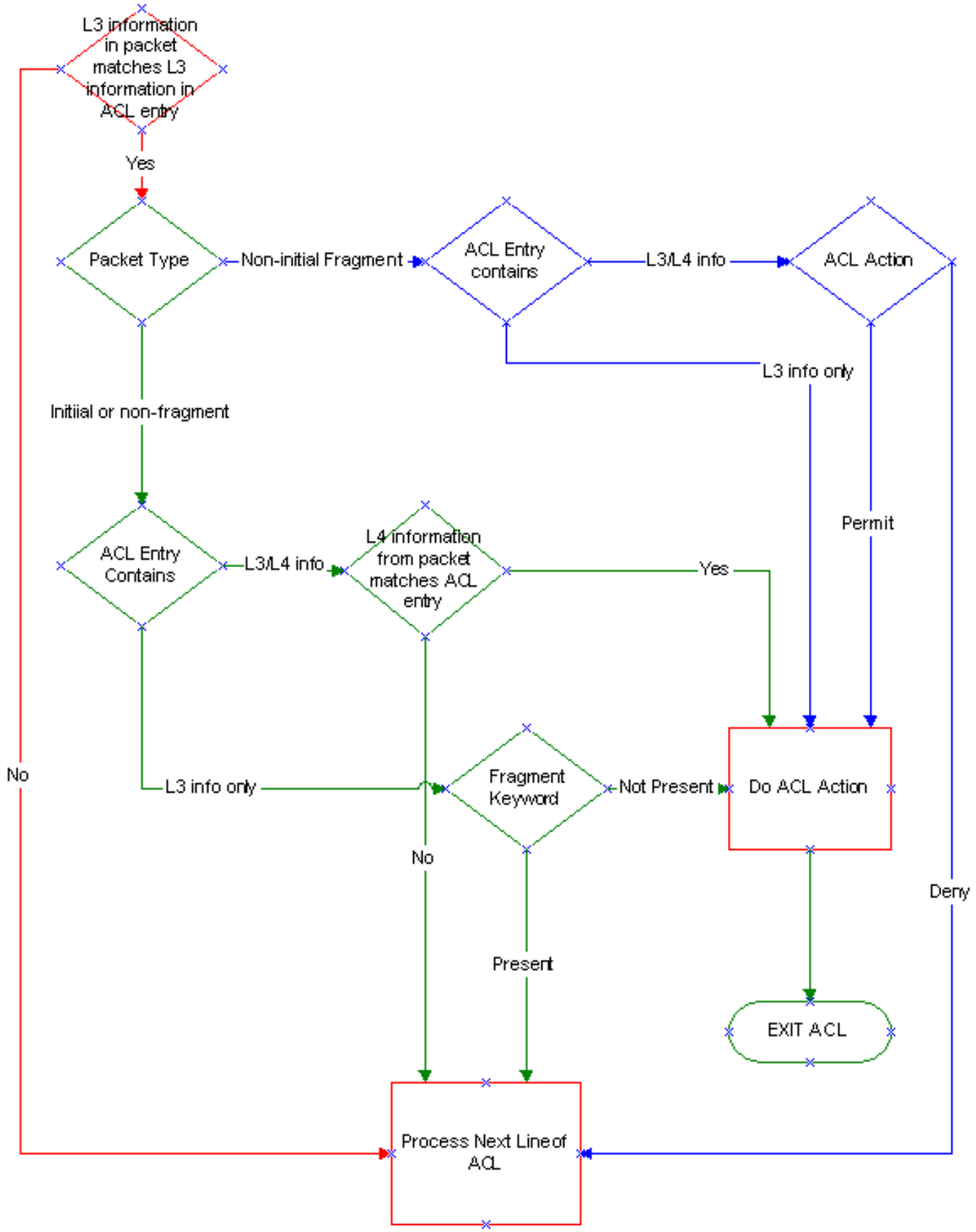
包含 L3 和 L4 信息的拒绝 ACL 行

1. 如果数据包的 L3 和 L4 信息与 ACL 条目匹配并且 FO = 0，将拒绝该数据包。
2. 如果数据包的 L3 信息与 ACL 行匹配并且 FO > 0，将处理下一个 ACL 条目。

ACL 规则流程图

以下流程图说明了针对 ACL 检查非分段、初始分段和非初始分段时的 ACL 规则。

注意：非初始分段本身仅包含第3层信息，而不包含第4层信息，尽管ACL可能同时包含第3层和第4层信息。



数据包怎样才能匹配 ACL

示例 1

以下五种可能的场景涉及不同类型的数据包遇到ACL 100。请参阅表和流程图，了解每种情况下发生的情况。Web 服务器的 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
```

数据包是一个通过端口 80 发送至服务器的初始分段或非分段：

ACL 的第一行同时包含第 3 层和第 4 层信息，并且这些信息与数据包中的第 3 层和第 4 层信息匹配，因此允许该数据包。

数据包是一个通过端口 21 发送至服务器的初始分段或非分段：

1. ACL 的第一行同时包含第 3 层和第 4 层信息，但其中第 4 层信息与数据包不匹配，因此将处理下一个 ACL 行。
2. ACL 的第二行拒绝所有数据包，因此该数据包被拒绝。

数据包是端口 80 数据流中一个流向服务器的非初始分段：

ACL 的第一行同时包含第 3 层和第 4 层信息，其中第 3 层信息与数据包匹配，并且 ACL 操作为允许，因此允许该数据包。

数据包是端口 21 数据流中一个流向服务器的非初始分段：

ACL 的第一行同时包含第 3 层和第 4 层信息。ACL 中的第 3 层信息与数据包匹配，该数据包中没有第 4 层信息，并且 ACL 操作为允许，因此允许该数据包。

数据包是一个发送至服务器子网中的另一台主机的初始分段、非分段或非初始分段：

1. ACL 的第一行中包含的第 3 层信息与数据包中的第 3 层信息（目标地址）不匹配，因此将处理下一个 ACL 行。
2. ACL 的第二行拒绝所有数据包，因此该数据包被拒绝。

示例 2

以下五个可能的场景涉及不同类型的数据包遇到ACL 101。同样，请参考表和流程图，了解每种情况下发生的情况。Web 服务器的 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
```

数据包是一个通过端口 80 发送至服务器的初始分段或非分段：

1. ACL 的第一行中包含的第 3 层信息与数据包中的第 3 层信息匹配。ACL 操作为拒绝，但因为出现 **fragments 关键字，因此将处理下一个 ACL 条目。**
2. ACL 的第二行包含第 3 层和第 4 层信息，这些信息与数据包匹配，因此允许该数据包。

数据包是一个通过端口 21 发送至服务器的初始分段或非分段：

1. ACL 的第一行中包含的第 3 层信息与数据包匹配，但 ACL 条目还包含 **fragments 关键字，这与数据包不匹配（因为 FO = 0），因此将处理下一个 ACL 条目。**
2. ACL 的第二行包含第 3 层和第 4 层信息。在这种情况下，第 4 层信息不匹配，因此将处理下一个 ACL 条目。
3. ACL 的第三行拒绝所有数据包，因此该数据包被拒绝。

数据包是端口 80 数据流中一个流向服务器的非初始分段：

ACL 的第一行中包含的第 3 层信息与数据包中的第 3 层信息匹配。请记住，尽管该非初始分段是端口 80 数据流的一部分，但该分段中没有第 4 层信息。由于第 3 层信息匹配，因此该数据包被拒绝。

数据包是端口 21 数据流中一个流向服务器的非初始分段：

ACL 的第一行仅包含第 3 层信息，并且该信息与数据包匹配，因此该数据包被拒绝。

数据包是一个发送至服务器子网中的另一台主机的初始分段、非分段或非初始分段：

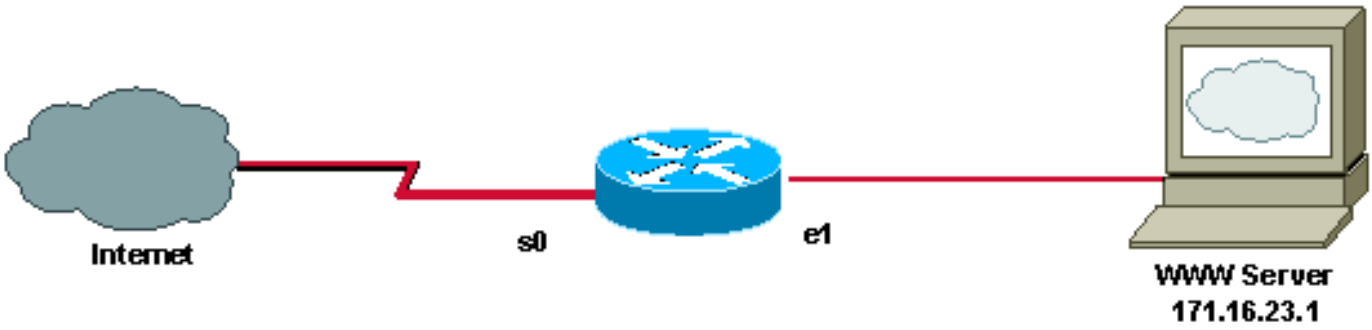
1. ACL 的第一行仅包含第 3 层信息，并且该信息与数据包不匹配，因此将处理下一个 ACL 行。
2. ACL 的第二行包含第 3 层和第 4 层信息。数据包中的第4层和第3层信息与ACL的信息不匹配，因此将处理下一个ACL行。
3. ACL 的第三行拒绝此数据包。

使用 fragments 关键字的各种方案

场景 1

路由器 B 连接到 Web 服务器，但网络管理员不希望任何分段到达该服务器。此场景显示如果网络管理员实施ACL 100而非ACL 101，会发生什么情况。ACL应用于路由器Serial0(s0)接口的入站流量，并且应仅允许非分段数据包到达Web服务器。在您按此方案操作时，请参阅 ACL 规则流程图和数据包怎样才能匹配 ACL 部分。

使用 fragments 关键字的结果



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 的第一行仅允许 HTTP 流量到达服务器，但它同时允许非初始分段到达服务器上的任何 TCP 端口。ACL 允许这些数据包通过是因为非初始分段不包含第 4 层信息，并且 ACL 逻辑认为在第 3 层信息匹配时，第 4 层信息（如果存在）也将匹配。第二行是隐式的，它拒绝所有其他流量。

请务必注意，从 Cisco IOS 软件版本 12.1(2) 和 12.0(11) 开始，新的 ACL 代码将丢弃与 ACL 中的任何其他行不匹配的分段。在较早版本中，即使非初始分段不匹配 ACL 中的任何其他行，也允许这些分段通过。

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
```

ACL 101 的第一行不允许非初始分段通过到达服务器。因为数据包中的第 3 层信息与第一个 ACL 行中的第 3 层信息匹配，所以当发送至服务器的非初始分段遇到该 ACL 行时，该分段被拒绝。

发送至服务器的端口 80 的初始分段或非分段也与 ACL 第一行中的第 3 层信息匹配，但由于出现 fragments 关键字，因此将处理下一个 ACL 条目（第二行）。因为初始分段或非分段与 ACL 行中的第 3 层和第 4 层信息匹配，所以 ACL 的第二行允许该初始分段或非分段。

发送至 171.16.23.0 网络上其他主机的 TCP 端口的非初始分段被此 ACL 阻止。这些数据包中的第 3 层信息与第一个 ACL 行中的第 3 层信息不匹配，因此将处理下一个 ACL 行。这些数据包中的第 3 层信息也与第二个 ACL 行中的第 3 层信息不匹配，因此处理第三个 ACL 行。第三行是隐式的，它拒绝所有流量。

此方案中的网络管理员决定实施 ACL 101，因为 ACL 101 仅允许未分段的 HTTP 数据流到达服务器。

场景 2

客户在两个不同的站点具有 Internet 连接，并且这两个站点之间还有一个后门连接。网络管理员的

策略是允许站点1中的组A访问站点2的HTTP服务器。两个站点的路由器都使用私有地址(RFC 1918)和网络地址转换(NAT)来转换通过Internet路由的数据包。

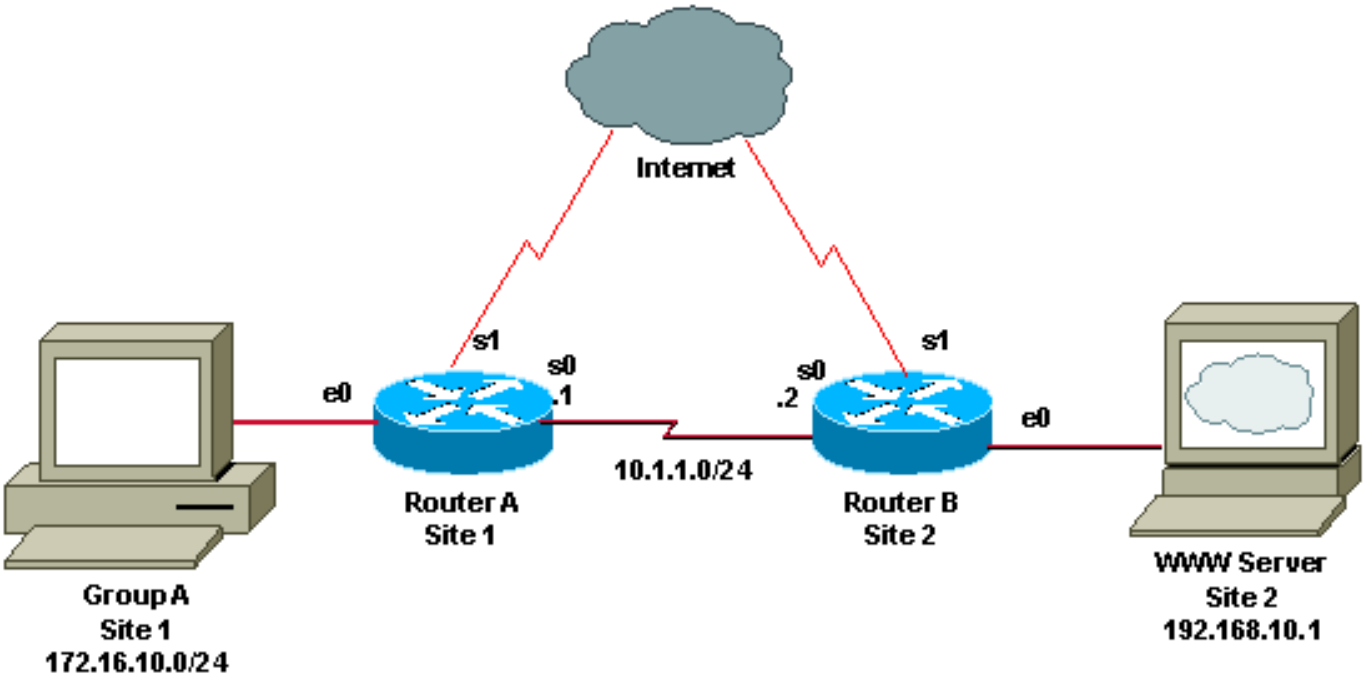
站点1的网络管理员策略性地路由分配给组A的私有地址，以便他们在访问站点2的HTTP服务器时通过路由器A的Serial0(s0)使用后门。站点2的路由器具有到172.16.10.0的静态路由，因此返回到组A的流量也通过后门路由。所有其他流量由 NAT 处理并通过 Internet 路由。此方案中的网络管理员必须决定当数据包被分段时哪个应用程序或数据流将工作。由于 HTTP 数据流和文件传输协议 (FTP) 数据流中有一个数据流中断，因此不可能使这两个数据流同时工作。

在您按此方案操作时，请参阅 ACL 规则流程图和数据包怎样才能匹配 ACL 部分。

对网络管理员所做选择的说明

在以下示例中，路由器A上名为FOO的路由映射通过s0将匹配ACL 100的数据包发送到路由器B。所有不匹配的数据包都由NAT处理，并通过Internet采用默认路由。

注意：如果数据包从ACL底部掉落或被ACL拒绝，则它不是策略路由的。



以下是路由器 A 的部分配置，该配置表明对接口 e0 应用了称为 FOO 的策略路由映射，其中来自组 A 的流量进入该路由器：

```
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 允许对流向服务器的 HTTP 数据流中的初始分段、非分段和非初始分段进行策略路由。由于流向服务器的 HTTP 数据流中的初始分段和非分段与第一个 ACL 行中的第 3 层和第 4 层信息匹

配，因此 ACL 允许这些分段并对它们进行策略路由。由于数据包中的第 3 层信息也与第一个 ACL 行匹配，因此 ACL 允许非初始分段并对它们进行策略路由；ACL 逻辑认为数据包中的第 4 层信息（如果存在）也匹配。

注意：ACL 100会中断组A和服务器之间其他类型的分段TCP流，因为初始分段和非初始分段通过不同路径到达服务器；初始分段由 NAT 处理并通过 Internet 路由，但相同数据流中的非初始分段将进行策略路由。

分段的 FTP 数据流有助于说明此方案中存在的问题。FTP 数据流的初始分段与第一个 ACL 行中的第 3 层信息匹配，但不与第 4 层信息匹配，因此它们被第二行拒绝。这些数据包由 NAT 处理并通过 Internet 路由。

FTP 数据流中的非初始分段与第一个 ACL 行中的第 3 层信息匹配，并且 ACL 逻辑认为第 4 层信息肯定匹配。这些数据包将进行策略路由，但由于 NAT 更改了初始分段的源地址，因此重组这些数据包的主机无法识别与进行策略路由的非初始分段包含在相同数据流中的初始分段。

以下配置中的 ACL 100 将解决 FTP 问题。ACL 100 的第一行拒绝从组 A 发送至服务器的初始和非初始 FTP 分段。

```
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
```

初始分段与第一个 ACL 行中的第 3 层信息匹配，但由于出现 **fragments 关键字，导致将处理下一个 ACL 行。**初始分段与第二个 ACL 行中的第 4 层信息不匹配，因此将处理 ACL 的下一个隐式行，该行拒绝数据包。非初始分段与 ACL 的第一行中的第 3 层信息匹配，因此这些非初始分段被拒绝。初始分段和非初始分段都由 NAT 处理并通过 Internet 路由，因此服务器在重组时不会存在任何问题。

修正 FTP 数据流将中断分段的 HTTP 数据流，这是因为现在初始 HTTP 分段将进行策略路由，但非初始分段由 NAT 处理并通过 Internet 路由。

当从组 A 发送至服务器的 HTTP 数据流中的初始分段遇到 ACL 的第一行时，它与 ACL 中的第 3 层信息匹配，但由于出现 **fragments 关键字，因此处理 ACL 的下一行。**ACL 的第二行允许该数据包并将它策略路由到服务器。

当从组 A 发送至服务器的非初始 HTTP 分段遇到 ACL 的第一行时，数据包中的第 3 层信息与 ACL 行匹配，因此该数据包被拒绝。这些数据包由 NAT 处理并通过 Internet 到达服务器。

此方案中的第一个 ACL 允许分段的 HTTP 数据流并中断分段的 FTP 数据流。第二个 ACL 允许分段的 FTP 数据流并中断分段的 HTTP 数据流。每种情况下 TCP 数据流之所以中断是因为初始和非初始分段采用不同的路径到达服务器。此时，不能进行重组，因为 NAT 更改了非初始分段的源地址。

不可能构造出允许这两种分段的数据流到达服务器的 ACL，因此网络管理员必须选择要工作的数据

流。

相关信息

- IP 路由 支持页
- 技术支持和文档 - Cisco Systems