Listas de controle de acesso e fragmentos IP

Contents

Introduction

Esta documentação explica os diferentes tipos de entrada da Lista controle de acesso (ACL) e o que acontece quando diferentes tipos de pacote encontram essas várias entradas. Os ACL são usados para bloquear pacotes IP de serem encaminhados por um roteador.

O RFC 1858 cobre considerações de segurança para filtragem de fragmentos IP e destaca dois ataques em hosts que envolvem fragmentos IP de pacotes TCP, o Ataque de Fragmento Minúsculo e o Ataque de Fragmento Sobreposto. Bloquear esses ataques é desejável porque eles podem comprometer um host ou vincular todos os seus recursos internos.

O RFC 1858 também descreve dois métodos de defesa contra esses ataques, os diretos e os indiretos. No método direto, fragmentos iniciais menores que um comprimento mínimo são descartados. O método indireto envolve o descarte do segundo fragmento de um conjunto de fragmento, se ele inicia 8 bytes no datagrama de IP original. Consulte RFC 1858 para obter mais detalhes.

Tradicionalmente, filtros de pacote como ACLs são aplicados aos não fragmentos e ao fragmento inicial de um pacote IP porque contêm informações das camadas 3 e 4 que as ACLs podem comparar para uma decisão de permissão ou negação. Os fragmentos não iniciais são tradicionalmente permitidos através da ACL porque podem ser bloqueados com base nas informações da Camada 3 nos pacotes; no entanto, como esses pacotes não contêm informações da camada 4, eles não correspondem às informações da camada 4 na entrada da ACL, se houver. Permitir a passagem de fragmentos não iniciais de um datagrama IP é aceitável porque o host que recebe os fragmentos não pode remontar o datagrama IP original sem o fragmento inicial.

Os firewalls também podem ser usados para bloquear pacotes mantendo uma tabela de fragmentos de pacotes indexados por endereço IP de origem e destino, protocolo e ID IP. O Cisco PIX Firewall e o Cisco IOS® Firewall podem filtrar todos os fragmentos de um fluxo específico

mantendo esta tabela de informações, mas é muito caro fazer isso em um roteador para obter a funcionalidade básica da ACL. O principal trabalho de um firewall é bloquear pacotes, e sua função secundária é rotear pacotes; uma tarefa principal do roteador é rotear pacotes e a função secundária é bloqueá-los.

Foram feitas duas alterações nos Cisco IOS Software Releases 12.1(2) e 12.0(11) para resolver alguns problemas de segurança relacionados aos fragmentos de TCP. O método indireto, como descrito na RFC 1858 , foi implementado como parte da verificação de integridade do pacote de entrada TCP/IP padrão. Também foram feitas alterações na funcionalidade da ACL em relação aos fragmentos não iniciais.

Tipos de entradas de ACL

Existem seis tipos diferente de linhas de ACL e cada um tem uma conseqüência se um pacote corresponder ou não. Na lista a seguir, FO = 0 indica um não fragmento ou um fragmento inicial em um fluxo TCP, FO > 0 indica que o pacote é um fragmento não inicial, L3 significa Camada 3 e L4 significa Camada 4.

Observação: quando há informações das Camadas 3 e 4 na linha ACL e a palavra-chave **fragmentos** está presente, a ação ACL é conservadora para as ações de permissão e negação. As ações são conservadoras porque você não deseja recusar acidentalmente uma parte fragmentada de um fluxo, pois os fragmentos não contêm informações suficientes para criar correspondência com todos os atributos do filtro. No caso deny, em vez de negar um fragmento não inicial, a próxima entrada da ACL é processada. No caso de permissão, supõe-se que as informações da Camada 4 no pacote, se disponíveis, correspondam às informações da Camada 4 na linha da ACL.

Permitir linha ACL somente com informações de L3

1. Se as informações L3 de um pacote corresponderem às informações L3 na linha da ACL, elas serão permitidas.
2. Se as informações da L3 de um pacote não corresponderem às informações da L3 da linha da ACL, a próxima entrada da ACL será processada.

Negar a linha ACL apenas com informações de L3.

1. Se as informações de L3 do pacote coincidirem com as informações de L3 na linha ACL, elas serão recusadas.
2. Se as informações da L3 de um pacote não corresponderem às informações da L3 da linha da ACL, a próxima entrada da ACL será processada.

Permitir linha ACL somente com informações L3 e a palavra-chave fragments está presente

Se as informações de L3 de um pacote corresponderem às informações de L3 na linha da ACL, o deslocamento de fragmento do pacote será verificado.

1. Se em um pacote FO > 0, o pacote será permitido.
2. Se um pacote tiver F0 = 0, a próxima entrada de ACL é processada.

Negar linha ACL somente com informações L3, e a palavra-chave fragments está presente

Se as informações de L3 de um pacote coincidirem com as informações de L3 na linha ACL, o deslocamento de fragmento do pacote será verificado.

1. Se um FO > 0, o pacote é recusado.
2. Se o FO de um pacote = 0, a próxima linha da ACL é processada.

Permita a linha ACL com as informações L3 e L4

1. Se as informações L3 e L4 de um pacote corresponderem à linha da ACL e FO = 0, o pacote será permitido.
2. Se as informações L3 de um pacote corresponderem à linha do ACL e a FO > 0, o pacote será permitido.

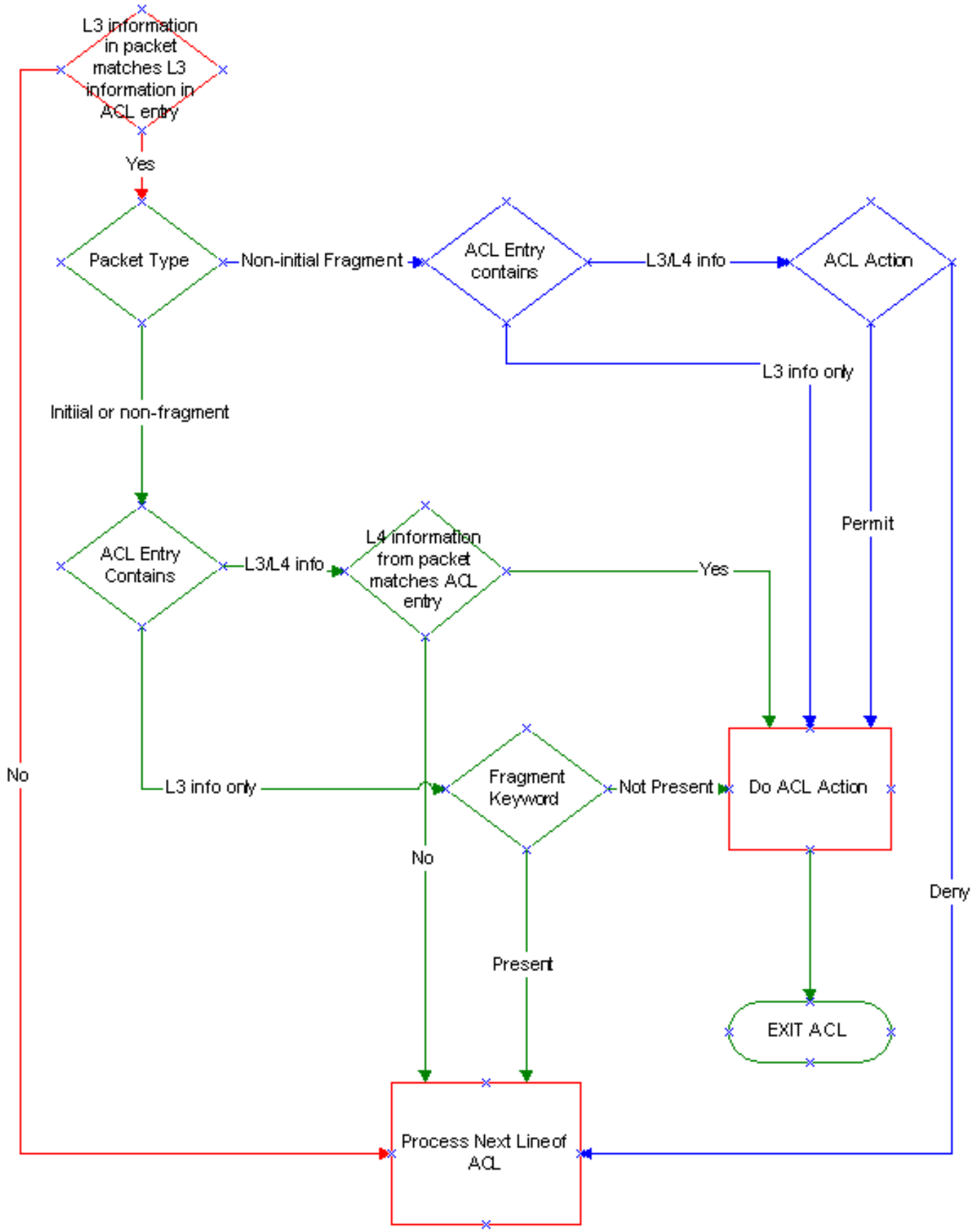
Recuse a linha ACL com informações L3 e L4

1. Se as informações L3 e L4 de um pacote corresponderem à entrada da ACL e FO = 0, o pacote será negado.
2. Se as informações L3 de um pacote corresponderem à linha da ACL e FO > 0, a próxima entrada da ACL será processada.

Fluxograna de regras de ACL

O fluxograma a seguir ilustra as regras ACL quando há uma verificação de ausência de fragmentos, fragmentos iniciais e fragmentos não iniciais em relação a ACL.

Observação: os próprios fragmentos não iniciais contêm apenas informações da Camada 3, nunca da Camada 4, embora a ACL possa conter informações das Camadas 3 e 4.



Como os pacotes podem corresponder a um ACL

Exemplo 1

Os cinco cenários possíveis a seguir envolvem diferentes tipos de pacotes que encontram a ACL

100. Consulte a tabela e o fluxograma à medida que você segue o que acontece em cada situação. O endereço IP do servidor da Web é 171.16.23.1.

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

access-list 100 deny ip any any
```

O pacote é um fragmento inicial ou não é um fragmento destinado ao servidor na porta 80:

A primeira linha da ACL contém informações das Camadas 3 e 4, que correspondem às informações das Camadas 3 e 4 no pacote, de modo que o pacote seja permitido.

O pacote é um fragmento inicial ou um não-fragmento destinado ao servidor na porta 21.

1. A primeira linha da ACL contém informações das Camadas 3 e 4, mas as informações da Camada 4 na ACL não correspondem ao pacote, portanto a próxima linha da ACL é processada.
2. A segunda linha do ACL recusa todos os pacotes, de modo que o pacote é recusado.

O pacote não é um fragmento inicial para o servidor em um fluxo da porta 80.

A primeira linha do ACL contém informações da Camada 3 e da Camada 4, as informações da Camada 3 do ACL correspondem ao pacote e a ação do ACL é para permissão, portanto o pacote é permitido.

O pacote é um fragmento não inicial ao servidor em um fluxo de porta 21:

A primeira linha do ACL contém informações da Camada 3 e da Camada 4. As informações da Camada 2 na ACL correspondem ao pacote, não há nenhuma informação da Camada 4 no pacote, e a ação da ACL é permitir, então o pacote é permitido.

O pacote é um fragmento inicial, um não-fragmento ou um fragmento não-inicial para outro host na sub-rede do servidor.

1. A primeira linha da ACL contém informações da Camada 3 que não correspondem às informações da Camada 3 no pacote (o endereço de destino), portanto a próxima linha ACL é processada.
2. A segunda linha do ACL recusa todos os pacotes, de modo que o pacote é recusado.

Exemplo 2

Os mesmos cinco cenários possíveis a seguir envolvem diferentes tipos de pacotes que encontram a ACL 101. Mais uma vez, consulte a tabela e o fluxograma à medida que você segue o que acontece em cada situação. O endereço IP do servidor da Web é 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
```

O pacote é um fragmento inicial ou não fragmento destinado ao servidor na porta 80:

1. A primeira linha da ACL contém informações sobre a Camada 3 que correspondem às informações da Camada 3 no pacote. A ação da ACL é negar, mas como a palavra-chave **fragments** está presente, a próxima entrada da ACL é processada.
2. A segunda linha da ACL contém informações das camadas 3 e 4 que correspondem ao pacote e, por isso, o pacote é permitido.

O pacote é um fragmento inicial ou não fragmento destinado ao servidor na porta 21:

1. A primeira linha da ACL contém informações da Camada 3, que correspondem ao pacote, mas a entrada da ACL também tem a palavra-chave **fragments**, que não corresponde ao pacote porque FO = 0, então a próxima entrada da ACL é processada.
2. A segunda linha do ACL contém as informações da camada 3 e da camada 4. Nesse caso, as informações da Camada 4 não correspondem, portanto, a próxima entrada da ACL é processada.
3. A terceira linha da ACL recusa todos os pacotes, de modo que o pacote foi recusado

O pacote não é um fragmento inicial para o servidor em um fluxo da porta 80.

A primeira linha da ACL contém informações sobre a Camada 3 que correspondem às informações da Camada 3 no pacote. Lembre-se de que, embora isso seja parte de um fluxo da porta 80, não há nenhuma informação da Camada 4 no fragmento não inicial. O pacote é negado porque as informações da Camada 3 correspondem.

O pacote é um fragmento não inicial ao servidor em um fluxo de porta 21:

A primeira linha da ACL contém apenas informações da Camada 3 e corresponde ao pacote; portanto, o pacote é negado.

O pacote é um fragmento inicial, um não-fragmento ou um fragmento não-inicial para outro host na sub-rede do servidor.

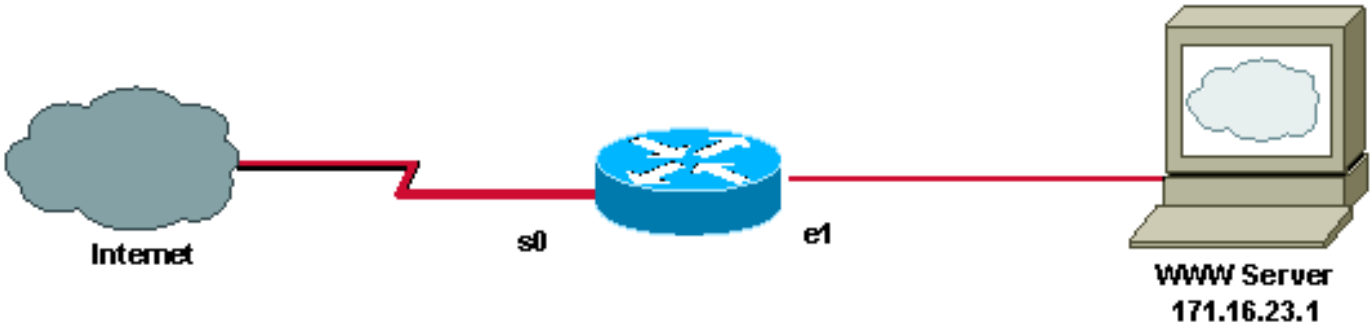
1. A primeira linha da ACL contém somente informações de camada 3, e não corresponde ao pacote, de modo que a próxima linha ACL é processada.
2. A segunda linha do ACL contém as informações da camada 3 e da camada 4. As informações da Camada 4 e da Camada 3 no pacote não correspondem às da ACL, então a próxima linha da ACL é processada.
3. A terceira linha da ACL nega esse pacote

fragmenta cenários com palavras-chave

Cenário 1

O Roteador B se conecta a um servidor Web e o administrador da rede não deseja permitir que nenhum fragmento acesse o servidor. Esse cenário mostra o que acontece se o administrador de rede implementar a ACL 100 versus a ACL 101. A ACL é aplicada na entrada da interface Serial0 (s0) dos roteadores e deve permitir que somente pacotes não fragmentados cheguem ao servidor Web. Consulte as seções Fluxograma de regras de ACL e Como os pacotes podem corresponder a um ACL à medida que prossegue no cenário.

Conseqüências do uso da palavra-chave fragments



O que segue é uma ACL 100:

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

access-list 100 deny ip any any
```

A primeira linha da ACL 100 permite somente HTTP para o servidor e também fragmentos não-iniciais para qualquer porta TCP no servidor. Ele permite esses pacotes porque os fragmentos não iniciais não contêm informações da Camada 4 e a lógica da ACL pressupõe que, se as informações da Camada 3 coincidirem, as informações da Camada 4 também corresponderão, se estiverem disponíveis. A segunda linha está implícita e nega todos os outros tráfegos.

Éimportante observar que, a partir das versões 12.1(2) e 12.0(11) do software Cisco IOS, o novo código ACL descarta fragmentos que não correspondem a nenhuma outra linha na ACL. Versões anteriores permitem a passagem de fragmentos não iniciais se não corresponderem a nenhuma outra linha da ACL.

O seguinte é 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
```

A ACL 101 não permite fragmentos não iniciais através do servidor devido à primeira linha. Um fragmento não inicial ao servidor é negado quando ele encontra a primeira linha da ACL porque as informações da Camada 3 no pacote correspondem às informações da Camada 3 na linha da

ACL.

Os fragmentos iniciais ou não na porta 80 no servidor também correspondem à primeira linha da ACL para informações da Camada 3, mas como a palavra-chave fragments está presente, a próxima entrada da ACL (a segunda linha) é processada. A segunda linha da ACL permite oS fragmentos iniciais ou nenhum fragmento, pois eles correspondem à linha da ACL das informações das Camadas 3 e 4.

Os fragmentos não-iniciais destinados às portas TCP de outros hosts na rede 171.16.23.0 são bloqueados por essa ACL. As informações da Camada 3 nesses pacotes não corresponde às constantes na primeira linha ACL, por isso a próxima linha ACL será processada. As informações da Camada 3 nesses pacotes também não correspondem as informações da Camada 3 na segunda linha da ACL; portanto, a terceira linha da ACL está sendo processada. A terceira linha é implícita e nega todo o tráfego.

Neste cenário, o administrador da rede decide implementar ACL 101 porque este permite somente fluxos HTTP não fragmentados ao servidor.

Cenário 2

Um cliente tem conectividade com a Internet em dois locais diferentes e também há uma conexão de backdoor entre os dois locais. A política do administrador de rede é permitir que o Grupo A no Site 1 acesse o servidor HTTP no Site 2. Os roteadores em ambos os sites estão usando endereços privados (RFC 1918) e Network Address Translation (NAT) para converter pacotes roteados pela Internet.

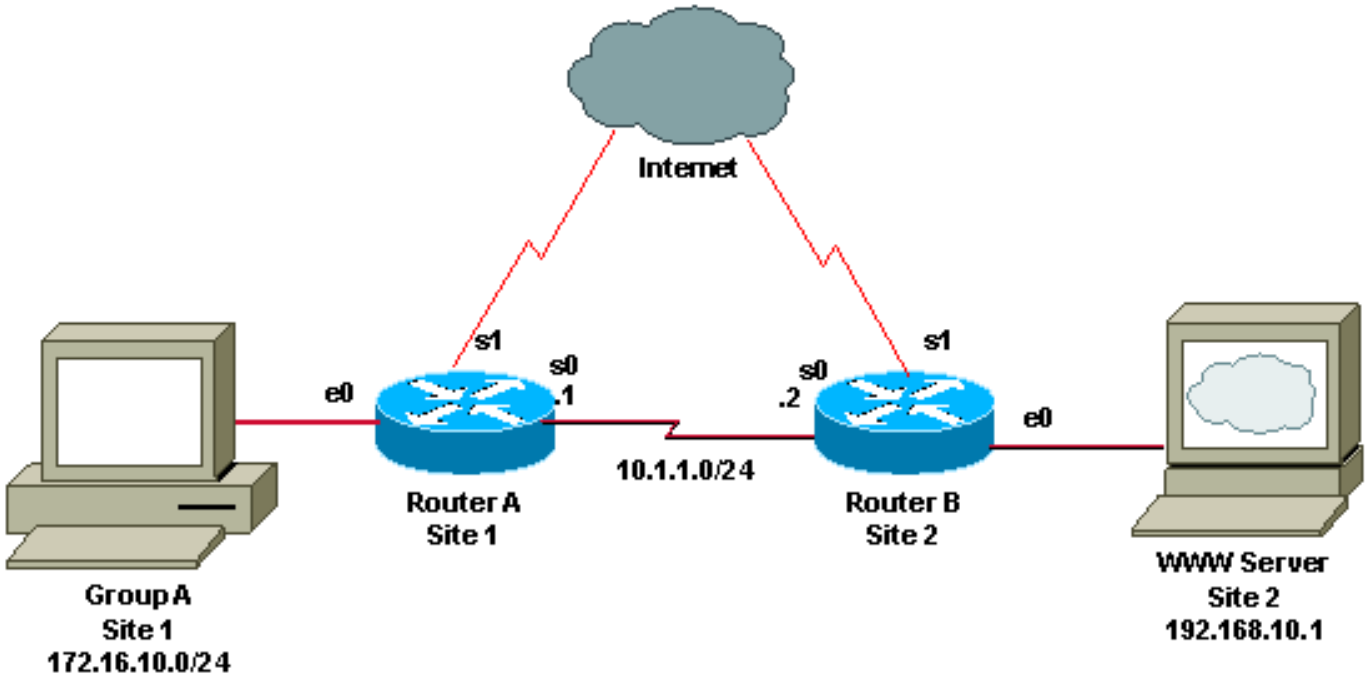
O administrador de rede no Site 1 está roteando por políticas os endereços privados atribuídos ao Grupo A, de modo que eles usem a porta traseira através da Serial0 (s0) do Roteador A ao acessar o servidor HTTP no Site 2. O roteador no local 2 tem uma rota estática para 172.16.10.0, de modo que o tráfego de retorno para o grupo A também é roteado pela porta traseira. Todo o tráfego restante é processado pelo NAT e roteado pela Internet. O administrador da rede nesse cenário tem que decidir que aplicativo ou fluxo funcionará caso os pacotes se fragmentem. Não é possível fazer com que os fluxos HTTP e FTP funcionem ao mesmo tempo porque um ou outro é interrompido.

Consulte as seções Fluxograma de regras de ACL e Como os pacotes podem corresponder a um ACL à medida que prossegue no cenário.

Explicação das opções do administrador de rede

No exemplo a seguir, o mapa de rota chamado FOO no Roteador A envia pacotes que correspondem à ACL 100 para o Roteador B através de s0. Todos os pacotes que não correspondem são processados pelo NAT e seguem a rota padrão através da Internet.

Observação: se um pacote cair da parte inferior da ACL ou for negado por ela, ele não será roteado por políticas.



A seguir está uma configuração parcial do Roteador A, mostrando que um mapa de rota de política chamado FOO é aplicado à interface e0, onde o tráfego do Grupo A entra no roteador:

```
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
```

A ACL 100 permite o roteamento de política em fragmentos iniciais, não fragmentos e não iniciais de fluxos HTTP para o servidor. A ACL e a política roteadas permitem os fluxos de HTTP iniciais e não-fragmentos para o servidor porque correspondem às informações da Camada 3 e da Camada 4 na primeira linha da ACL. Os fragmentos não iniciais são permitidos pela ACL e pela política roteada porque as informações da Camada 3 no pacote também correspondem à primeira linha da ACL; a lógica da ACL pressupõe que as informações da Camada 4 no pacote também corresponderiam se estivessem disponíveis.

Observação: a ACL 100 divide outros tipos de fluxos de TCP fragmentados entre o Grupo A e o servidor porque os fragmentos iniciais e não iniciais chegam ao servidor através de caminhos diferentes; os fragmentos iniciais são processados pelo NAT e roteados pela Internet, mas os fragmentos não iniciais do mesmo fluxo são roteados por política.

Um fluxo de FTP fragmentado ajuda a ilustrar o problema nesse cenário. Os fragmentos iniciais de um fluxo de FTP correspondem às informações da Camada 3, mas não às informações da Camada 4, da primeira linha de ACL, e são posteriormente negados pela segunda linha. Esses pacotes são processados pelo NAT e roteados pela Internet.

Os fragmentos não iniciais de um fluxo FTP correspondem às informações da Camada 3 na primeira linha da ACL, e a lógica da ACL pressupõe uma correspondência positiva nas

informações da Camada 4. Esses pacotes são roteados por políticas, e o host que está remontando esses pacotes não reconhece os fragmentos iniciais como parte do mesmo fluxo que os fragmentos não-iniciais roteados por política, pois a NAT alterou o endereço de origem dos fragmentos iniciais.

A ACL 100 na configuração abaixo corrige o problema de FTP. A primeira linha da ACL 100 nega fragmentos FTP iniciais e não iniciais do Grupo A para o servidor.

```
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
```

Os fragmentos iniciais correspondem às informações da Camada 3 na primeira linha da ACL, mas a presença da palavra-chave **fragments** faz com que a próxima linha da ACL seja processada. O fragmento inicial não corresponde à segunda linha da ACL para informações da Camada 4 e, portanto, a próxima linha implícita da ACL é processada, o que nega o pacote. Os fragmentos não iniciais correspondem às informações da Camada 3 na primeira linha da ACL, portanto, eles são negados. Os fragmentos iniciais e não iniciais são processados pelo NAT e roteados pela Internet, portanto, o servidor não tem problemas com a remontagem.

A correção de fluxos de FTP interrompe os fluxos de HTTP fragmentados porque os fragmentos de HTTP iniciais agora são roteados por política, mas os fragmentos não iniciais são processados pelo NAT e roteados pela Internet.

Quando um fragmento inicial de um fluxo HTTP do Grupo A para o servidor encontra a primeira linha do ACL, ele é correlacionado com as informações de Camada 3 no ACL, mas devido à palavra-chave dos fragmentos, a próxima linha do ACL é processada. A segunda linha das permissões de ACL e política direcionam o pacote para o servidor.

Quando fragmentos HTTP não-iniciais destinados ao Grupo A do servidor encontram a primeira linha do ACL, as informações da Camada 3 do pacote correspondem à linha ACL e o pacote é negado. Esses pacotes são processados pelo NAT e cruzam a Internet para chegar ao servidor.

A primeira ACL neste cenário permite fluxos HTTP fragmentados e interrompe fluxos FTP fragmentados. O segundo ACL permite fluxos de FTP fragmentado e interrompe fluxos de HTTP fragmentado. Os fluxos de TCP se interrompem em cada caso porque os fragmentos iniciais e não iniciais tomam caminhos diferentes para o servidor. A remontagem não é possível a NAT alterou o endereço de origem dos fragmentos não iniciais.

Não é possível construir uma ACL que permita dois tipos de fluxos fragmentados em direção ao servidor, portanto, o administrador de rede deve escolher o fluxo com o qual deseja trabalhar.

Informações Relacionadas

- Página de Suporte do IP Routing
- Suporte Técnico e Documentação - Cisco Systems