Listas de controle de acesso e fragmentos IP

Índice

Introdução

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 o fragmento IP que filtra e destaca dois ataques nos anfitriões que envolvem fragmentos IP dos pacotes de TCP, do ataque de fragmento minúsculo e do ataque de fragmento de sobreposição. Obstruir estes ataques é desejável porque podem comprometer um host, ou amarra acima todos seus recursos internos.

O RFC 1858 igualmente descreve dois métodos da defesa contra estes ataques, o direto e o indireto. No método direto, os fragmentos iniciais que são menores do que um comprimento mínimo são rejeitados. O método indireto envolve o descarte do segundo fragmento de um conjunto de fragmento, se ele inicia 8 bytes no datagrama de IP original. Veja por favor o RFC 1858 para mais detalhes.

Tradicionalmente, os filtros de pacote como ACL são aplicados aos não-fragmentos e ao fragmento inicial de um pacote IP porque contêm a camada 3 e a informação 4 que os ACL podem combinar contra para uma decisão do permit or deny. Os fragmentos não iniciais são permitidos tradicionalmente com o ACL porque podem ser obstruídos com base na informação da camada 3 nos pacotes; contudo, porque estes pacotes não contêm a informação da camada 4, não combinam a informação da camada 4 na entrada ACL, se existe. Permitir os fragmentos não iniciais de um IP datagram é completamente aceitável porque o host que recebe os fragmentos não pode remontar a datagrama de IP original sem o fragmento inicial.

Os Firewall podem igualmente ser usados aos bloqueares pacote mantendo uma tabela dos fragmentos de pacote posicionados pelo endereço IP de origem e de destino, pelo protocolo, e pelo IP ID. O Cisco PIX Firewall e o Firewall do ® do Cisco IOS podem filtrar todos os fragmentos de um fluxo particular mantendo esta tabela da informação, mas é demasiado caro fazer isto em

uma funcionalidade ACL do roteador para básico. O trabalho principal de um Firewall é aos bloqueares pacote, e seu papel secundário é aos pacotes de rota; 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 no RFC 1858 , foi executado como parte da verificação de sanidade do pacote de entrada do padrão TCP/IP. As mudanças foram feitas igualmente à funcionalidade ACL no que diz respeito 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 seguinte lista, o FO = 0 indica um não-fragmento ou um fragmento inicial em um fluxo de TCP, o FO > 0 indica que o pacote é um fragmento não inicial, L3 significa a camada 3, e o L4 significa a camada 4.

Nota: Quando há informações da Camada 3 e da Camada 4 na linha ACL, e a palavra-chave fragments está presente, a ação do ACL é conservativa para as ações de permissão e rejeição. 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 exemplo da negação, em vez de negar um fragmento não inicial, a entrada ACL seguinte é processada. No exemplo da licença, supõe-se que a informação da camada 4 no pacote, se disponível, combina a informação da camada 4 na linha ACL.

Permitir linha ACL somente com informações de L3

1. Se a informação L3 de um pacote combina a informação L3 na linha ACL, está permitida.
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.

Permita a linha ACL com a informação L3 somente, e a palavra-chave dos fragmentos esta presente

Se a informação L3 de um pacote combina a informação L3 na linha ACL, o deslocamento de fragmento do pacote está 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.

Negue a linha ACL com a informação L3 somente, e a palavra-chave dos fragmentos esta

presente

Se a informação L3 de um pacote combina a informação L3 na linha ACL, o deslocamento de fragmento do pacote está 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 de um pacote a informação o L3 e o L4 combina a linha ACL e o FO = 0, o pacote está 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 de um pacote a informação o L3 e o L4 combina a entrada ACL e o FO = 0, o pacote está negado.
2. Se a informação L3 de um pacote combina a linha ACL e o FO > 0, a entrada ACL seguinte está 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.

Nota: Os próprios fragmentos não iniciais contêm somente informações da Camada 3, nunca da Camada 4, embora o ACL possa conter informações das Camadas 3 e 4.

Como os pacotes podem corresponder a um ACL

Exemplo 1

Os seguintes cinco cenários possíveis envolvem tipos diferentes de pacotes que encontram o ACL 100. Refira por favor a tabela e o fluxograma como 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 do ACL contém a informação de ambas camadas 3 e 4, que combina a informação de camada 3 e 4 no pacote, assim que o pacote é permitido.

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

1. A primeira linha do ACL contém a informação de ambas camadas 3 e 4, mas a informação da camada 4 no ACL não combina o pacote, assim que a linha ACL seguinte 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 seguintes os mesmos cinco cenários possíveis envolvem tipos diferentes de pacotes que encontram o ACL 101. Refira além disso, por favor a tabela e o fluxograma como 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 um destinado não-fragmento para o server 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 ACL é negar, mas porque a palavra-chave dos **fragmentos** esta presente, a entrada ACL seguinte 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 um destinado não-fragmento para o server na porta 21:

1. A primeira linha do ACL contém a informação da camada 3, que combina o pacote, mas a entrada ACL igualmente tem a palavra-chave dos **fragmentos**, que não combina o pacote porque FO = 0, assim que a entrada ACL seguinte é processada.
2. A segunda linha do ACL contém as informações da camada 3 e da camada 4. Neste caso, a informação da camada 4 não combina, assim que a entrada ACL seguinte 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 a camada 3 fósforos da informação.

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. A informação da camada 4 e da camada 3 no pacote não combina aquela do ACL, assim que a linha ACL seguinte é processada.
3. A terceira linha do ACL nega este pacote

fragmenta cenários com palavras-chave

Cenário 1

O roteador B conecta a um servidor de Web, e o administrador de rede não quer permitir que nenhuns fragmentos alcancem o server. Esta encenação mostra o que acontece se o administrador de rede executa o ACL 100 contra o ACL 101. O ACL é de entrada aplicado na relação do serial0 do Roteadores (S0) e deve permitir que somente os pacotes NON-fragmentados alcancem o servidor de 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. Permite estes pacotes porque os fragmentos não iniciais não contêm a informação da camada 4, e o ACL logic supõe aquele se os fósforos da informação da camada 3, a seguir a informação da camada 4 igualmente combinaria, se estava disponível. A segunda linha está implícita e nega todos os outros tráfegos.

Éimportante notar que, até à data dos Cisco IOS Software Releases 12.1(2) e 12.0(11), o código novo ACL deixa cair os fragmentos que não combinam nenhuma outra linha no ACL. As versões

anterior permitem fragmentos não iniciais completamente se não combinam nenhuma outra linha do 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
```

O ACL 101 não permite fragmentos não iniciais completamente ao server devido à primeira linha. Um fragmento não inicial ao server é negado quando encontra a primeira linha ACL porque a informação da camada 3 no pacote combina a informação da camada 3 na linha ACL.

A inicial ou os não-fragmentos à porta 80 no server igualmente combinam a primeira linha do ACL para a informação da camada 3, mas porque a palavra-chave dos fragmentos esta presente, a entrada ACL seguinte (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 anfitriões na rede de 171.16.23.0 são obstruídos por este 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 a conectividade de Internet em dois locais diferentes, e há igualmente uma conexão de porta traseira entre os dois locais. A política do administrador de rede é permitir que o grupo A no local 1 alcance o Server do HTTP no local 2. O Roteadores em ambos os locais está usando endereços privados (RFC 1918) e Network Address Translation (NAT) para traduzir os pacotes que são distribuídos através do Internet.

O administrador de rede no local 1 é roteamento de política os endereços privados atribuídos para agrupar A, de modo que usem a porta traseira com o serial0 do roteador a (S0) ao alcançar o Server do HTTP no local 2. O roteador no local 2 tem uma rota estática a 172.16.10.0, de modo que o tráfego de retorno para agrupar A seja distribuído igualmente com a porta traseira. Todo tráfego restante é processado pelo NAT e distribuído através do Internet. O administrador da rede nesse cenário tem que decidir que aplicativo ou fluxo funcionará caso os pacotes se fragmentem. Não é possível fazer ao mesmo tempo o HTTP e o trabalho dos fluxos do File Transfer Protocol (FTP) porque um ou o outro quebra.

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 seguinte, o mapa de rota chamado FOO no roteador A envia os pacotes que combinam o ACL 100 transversalmente ao roteador B com o S0. Todos os pacotes que não

combinam são processados pelo NAT e para tomar a rota padrão através do Internet.

Nota: Se um pacote cai a parte inferior do ACL, ou é negado por ele, a seguir não é política-roteado.

O seguinte é uma configuração parcial do roteador A, mostrando que um mapa de rotas da política chamado FOO está aplicado para conectar o E0, onde o tráfego do grupo A inscreve o 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
```

O ACL 100 permite a roteamento de política em ambos a inicial, não-fragmentos e os fragmentos não iniciais do HTTP fluem ao server. A inicial e os não-fragmentos de fluxos HTTP ao server são permitidos pelo ACL e pela política distribuído porque combina a informação de camada 3 e 4 na primeira linha ACL. Os fragmentos não iniciais são permitidos pelo ACL e pela política distribuídos porque a informação da camada 3 no pacote igualmente combina a primeira linha ACL; o ACL logic supõe que a informação da camada 4 no pacote igualmente combinaria se estava disponível.

Nota: O ACL 100 quebra outros tipos de fluxos de TCP fragmentados entre o grupo A e o server porque a inicial e os fragmentos não iniciais obtêm ao server através dos trajetos diferentes; os fragmentos iniciais são processados pelo NAT e distribuídos através do Internet, mas os fragmentos não iniciais do mesmo fluxo são política distribuídos.

As ajudas fragmentadas de um FTPftp ilustram o problema nesta encenação. 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 fósforo do FTPftp a informação da camada 3 na primeira linha ACL, e o ACL logic supõem um fósforo positivo na informação 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.

O ACL 100 na configuração abaixo fixa o problema com FTP. A primeira linha de ACL 100 nega fragmentos iniciais e NON-iniciais FTP do grupo A ao server.

```
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 combinam na informação da camada 3 na primeira linha ACL, mas a presença da palavra-chave dos **fragmentos** faz com que a linha ACL seguinte seja processada. O fragmento inicial não combina a segunda linha ACL para a informação da camada 4, e assim que a linha implícita seguinte do ACL é processada, que nega o pacote. Os fragmentos não iniciais combinam a informação da camada 3 na primeira linha do ACL, assim que são negados. Rubrique e os fragmentos não iniciais são processados pelo NAT e distribuídos através do Internet, assim que o server não tem nenhum problema com remontagem.

Fixar os FTPftps HTTP fragmentado rupturas flui porque os fragmentos de HTTP iniciais são

agora política distribuídos, mas os fragmentos não iniciais são processados pelo NAT e distribuídos através do 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.

O primeiro ACL nesta encenação permite fluxos fragmentados HTTP e quebra FTPftps 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