Zugriffskontrolllisten und IP-Fragmente

Inhalt

Einführung

In diesem Whitepaper werden die verschiedenen Arten von Zugriffskontrolllisten-Einträgen (Access Control List, ACL) erläutert. Außerdem wird erläutert, was geschieht, wenn verschiedene Pakettypen auf diese verschiedenen Einträge stoßen. ACLs blockieren die Weiterleitung von IP-Paketen durch einen Router.

RFC 1858 behandelt Sicherheitsaspekte bei der IP-Fragmentfilterung und hebt zwei Angriffe auf Hosts hervor, die IP-Fragmente von TCP-Paketen beinhalten: den Tiny Fragment Attack und den Overlapping Fragment Attack. Die Blockierung dieser Angriffe ist wünschenswert, da sie einen Host gefährden oder alle seine internen Ressourcen binden können.

RFC 1858 beschreibt auch zwei Methoden zur Abwehr dieser Angriffe: die direkte und die indirekte. Bei der Direktmethode werden anfängliche Fragmente, die kleiner als eine Mindestlänge sind, verworfen. Bei der indirekten Methode wird das zweite Fragment eines Fragmentsatzes verworfen, wenn es 8 Byte in das ursprüngliche IP-Datagramm einsetzt. Weitere Informationen finden Sie unter RFC 1858 .

Bisher werden Paketfilter wie ACLs auf die Nicht-Fragmente und das ursprüngliche Fragment eines IP-Pakets angewendet, da sie sowohl Layer-3- als auch Layer-4-Informationen enthalten, mit denen die ACLs bei einer Genehmigungsentscheidung oder Ablehnungsentscheidung übereinstimmen können. Nicht initiale Fragmente werden normalerweise durch die ACL zugelassen, da sie basierend auf Layer-3-Informationen in den Paketen blockiert werden können. Da diese Pakete jedoch keine Layer-4-Informationen enthalten, stimmen sie nicht mit den Layer-4-Informationen im ACL-Eintrag überein, sofern diese vorhanden sind. Das Zulassen der nicht initialen Fragmente eines IP-Datagramms durch ist akzeptabel, da der Host, der die Fragmente empfängt, das ursprüngliche IP-Datagramm ohne das ursprüngliche Fragment nicht reassemblieren kann.

Firewalls können auch verwendet werden, um Pakete zu blockieren, indem eine Tabelle mit

Paketerweiterungen verwaltet wird, die anhand der Quell- und Ziel-IP-Adresse, des Protokolls und der IP-ID indiziert sind. Sowohl die Cisco PIX-Firewall als auch die Cisco IOS® Firewall können alle Fragmente eines bestimmten Datenflusses filtern, indem sie diese Informationstabelle verwalten. Für die grundlegende ACL-Funktionalität auf einem Router ist dies jedoch zu kostspielig. Die primäre Aufgabe einer Firewall ist das Blockieren von Paketen, und die sekundäre Rolle besteht darin, Pakete weiterzuleiten. Die primäre Aufgabe eines Routers ist die Weiterleitung von Paketen. Die sekundäre Rolle besteht darin, diese zu blockieren.

In den Cisco IOS Software-Versionen 12.1(2) und 12.0(11) wurden zwei Änderungen vorgenommen, um einige Sicherheitsprobleme im Zusammenhang mit TCP-Fragmenten zu beheben. Die indirekte Methode, wie in RFC 1858 beschrieben, wurde im Rahmen der Standardprüfung der TCP/IP-Paketintegrität implementiert. Die ACL-Funktionalität wurde auch in Bezug auf nicht initiale Fragmente geändert.

Typen von ACL-Einträgen

Es gibt sechs verschiedene Arten von ACL-Leitungen, die jeweils eine Auswirkung haben, wenn ein Paket übereinstimmt oder nicht. In der folgenden Liste gibt FO = 0 ein Nicht-Fragment oder ein initiales Fragment in einem TCP-Fluss an. FO > 0 gibt an, dass es sich bei dem Paket um ein nicht initiales Fragment handelt, L3 bedeutet Layer 3, und L4 steht für Layer 4.

Hinweis: Wenn in der ACL-Zeile Layer-3- und Layer-4-Informationen vorhanden sind und das **fragments**-Schlüsselwort vorhanden ist, ist die ACL-Aktion sowohl für Zulassen- als auch für Ablehnungsaktionen konservativ. Die Aktionen sind konservativ, da Sie einen fragmentierten Teil eines Datenflusses nicht versehentlich verweigern möchten, da die Fragmente nicht genügend Informationen enthalten, um alle Filterattribute abzugleichen. Im Deny-Fall wird der nächste ACL-Eintrag verarbeitet, anstatt ein nicht initiales Fragment zu verweigern. Im Genehmigungsfall wird davon ausgegangen, dass die Layer-4-Informationen im Paket, sofern verfügbar, mit den Layer-4-Informationen in der ACL-Zeile übereinstimmen.

ACL-Leitung zulassen, nur mit L3-Informationen

1. Wenn die L3-Informationen eines Pakets mit den L3-Informationen in der ACL-Leitung übereinstimmen, ist dies zulässig.
2. Wenn die L3-Informationen eines Pakets nicht mit den L3-Informationen in der ACL-Zeile übereinstimmen, wird der nächste ACL-Eintrag verarbeitet.

ACL-Leitung nur mit L3-Informationen verweigern

1. Wenn die L3-Informationen eines Pakets mit den L3-Informationen in der ACL-Leitung übereinstimmen, wird diese verweigert.
2. Wenn die L3-Informationen eines Pakets nicht mit den L3-Informationen in der ACL-Zeile übereinstimmen, wird der nächste ACL-Eintrag verarbeitet.

ACL-Zeile nur mit L3-Informationen zulassen, und das fragments-Schlüsselwort ist vorhanden.

Wenn die L3-Informationen eines Pakets mit den L3-Informationen in der ACL-Zeile übereinstimmen, wird der Fragment-Offset des Pakets überprüft.

1. Wenn die FO > 0 eines Pakets lautet, ist das Paket zulässig.
2. Wenn der FO = 0 eines Pakets lautet, wird der nächste ACL-Eintrag verarbeitet.

ACL-Zeile nur mit L3-Informationen verweigern, und das fragments-Schlüsselwort ist vorhanden.

Wenn die L3-Informationen eines Pakets mit den L3-Informationen in der ACL-Zeile übereinstimmen, wird der Fragment-Offset des Pakets überprüft.

1. Wenn der FO > 0 eines Pakets lautet, wird das Paket abgelehnt.
2. Wenn der FO = 0 eines Pakets lautet, wird die nächste ACL-Zeile verarbeitet.

Zugriffsberechtigung für ACL-Leitung mit L3- und L4-Informationen

1. Wenn die L3- und L4-Informationen eines Pakets mit der ACL-Leitung und FO = 0 übereinstimmen, ist das Paket zulässig.
2. Wenn die L3-Informationen eines Pakets mit der ACL-Leitung und FO > 0 übereinstimmen, ist das Paket zulässig.

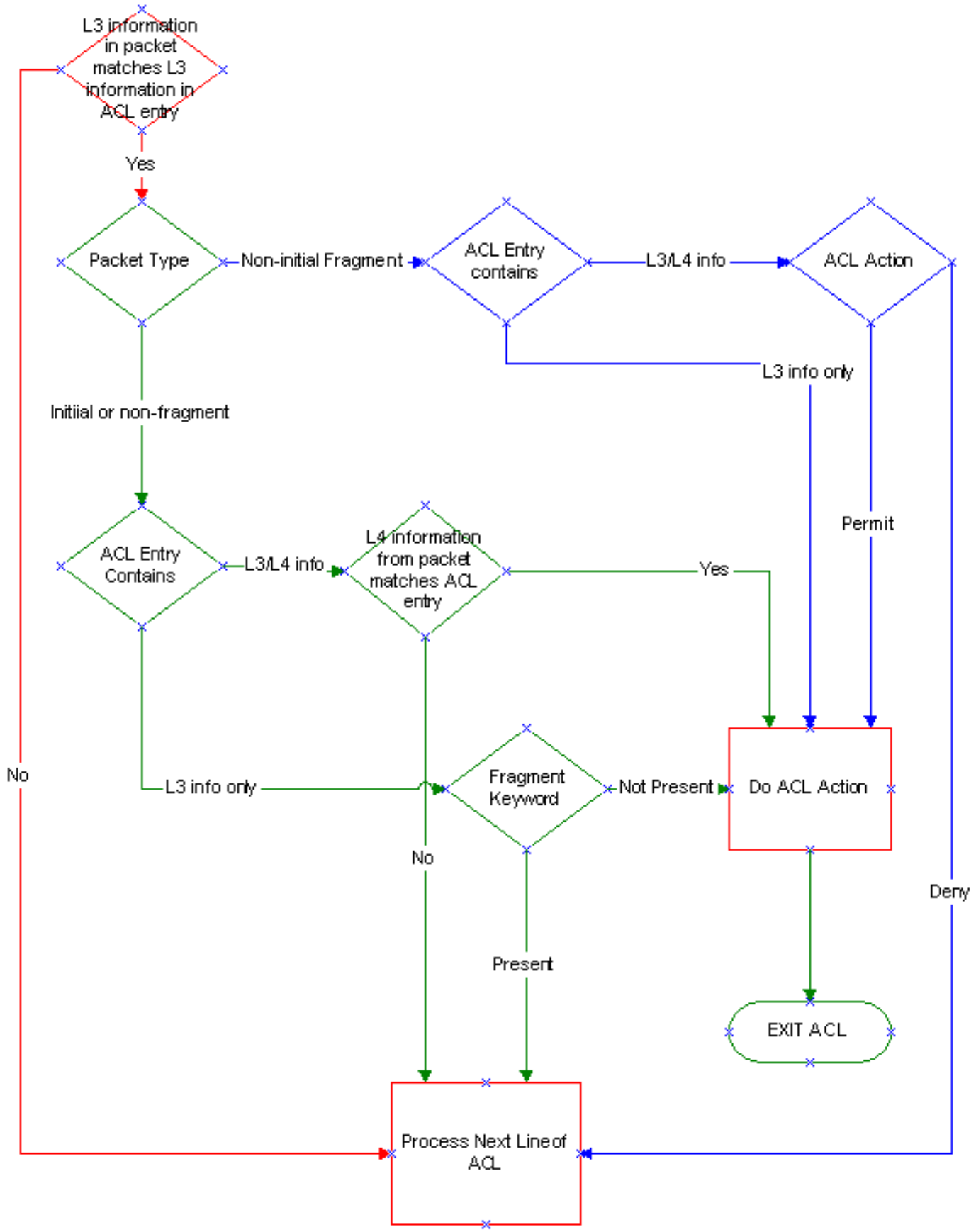
ACL-Leitung mit L3- und L4-Informationen verweigern

1. Wenn die L3- und L4-Informationen eines Pakets mit dem ACL-Eintrag und FO = 0 übereinstimmen, wird das Paket abgelehnt.
2. Wenn die L3-Informationen eines Pakets mit der ACL-Zeile und FO > 0 übereinstimmen, wird der nächste ACL-Eintrag verarbeitet.

Flussdiagramm der ACL-Regeln

Das folgende Flussdiagramm veranschaulicht die ACL-Regeln, wenn Nicht-Fragmente, ursprüngliche Fragmente und nicht-initiale Fragmente mit der ACL abgeglichen werden.

Hinweis: Die nicht initialen Fragmente selbst enthalten nur Layer-3- und niemals Layer-4-Informationen. Die ACL kann jedoch sowohl Layer-3- als auch Layer-4-Informationen enthalten.



Wie Pakete einer ACL zugeordnet werden können

Beispiel 1

Die folgenden fünf möglichen Szenarien beziehen sich auf verschiedene Pakettypen mit ACL 100.

Bitte beachten Sie die Tabelle und das Flussdiagramm, wenn Sie die Vorgänge in jeder Situation verfolgen. Die IP-Adresse des Webservers lautet 171.16.23.1.

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

access-list 100 deny ip any any
```

Das Paket ist ein initiales Fragment oder ein Nicht-Fragment, das für den Server an Port 80 bestimmt ist:

Die erste Zeile der ACL enthält Layer-3- und Layer-4-Informationen, die mit den Layer-3- und Layer-4-Informationen im Paket übereinstimmen, sodass das Paket zulässig ist.

Das Paket ist ein initiales Fragment oder ein Nicht-Fragment, das für den Server an Port 21 bestimmt ist:

1. Die erste Zeile der ACL enthält Layer-3- und Layer-4-Informationen, die Layer-4-Informationen in der ACL stimmen jedoch nicht mit dem Paket überein, sodass die nächste ACL-Zeile verarbeitet wird.
2. Die zweite Zeile der Zugriffskontrollliste verwehrt alle Pakete, sodass das Paket abgelehnt wird.

Das Paket ist ein nicht initiales Fragment zum Server in einem Port 80-Fluss:

Die erste Zeile der ACL enthält Layer-3- und Layer-4-Informationen, die Layer-3-Informationen in der ACL stimmen mit dem Paket überein, und die ACL-Aktion ist "Zulassen", damit das Paket zulässig ist.

Das Paket ist ein nicht initiales Fragment zum Server in einem Port-21-Fluss:

Die erste Zeile der ACL enthält Informationen zu Layer 3 und Layer 4. Die Layer-3-Informationen in der ACL stimmen mit dem Paket überein, es gibt keine Layer-4-Informationen im Paket, und die ACL-Aktion ist zulässig, sodass das Paket zugelassen wird.

Das Paket ist ein initiales Fragment, kein Fragment oder nicht initiales Fragment zu einem anderen Host im Server-Subnetz:

1. Die erste Zeile der ACL enthält Layer-3-Informationen, die nicht mit den Layer-3-Informationen im Paket (der Zieladresse) übereinstimmen. Daher wird die nächste ACL-Zeile verarbeitet.
2. Die zweite Zeile der Zugriffskontrollliste verwehrt alle Pakete, sodass das Paket abgelehnt wird.

Beispiel 2

Die folgenden fünf möglichen Szenarien beziehen sich auf verschiedene Pakettypen mit ACL 101. Beachten Sie auch hier die Tabellen- und Flussdiagramme, wenn Sie verfolgen, was in jeder

Situation geschieht. Die IP-Adresse des Webservers lautet 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
```

Das Paket ist ein initiales Fragment oder ein Non-Fragment, das für den Server an Port 80 bestimmt ist:

1. Die erste Zeile der ACL enthält Layer-3-Informationen, die mit den Layer-3-Informationen im Paket übereinstimmen. Die ACL-Aktion lautet "deny". Da das **fragments-**Schlüsselwort vorhanden ist, wird der nächste ACL-Eintrag verarbeitet.
2. Die zweite Zeile der ACL enthält Layer-3- und Layer-4-Informationen, die mit dem Paket übereinstimmen, sodass das Paket zulässig ist.

Das Paket ist ein initiales Fragment oder ein Non-Fragment, das für den Server an Port 21 bestimmt ist:

1. Die erste Zeile der ACL enthält Layer-3-Informationen, die mit dem Paket übereinstimmen. Der ACL-Eintrag enthält jedoch auch das **fragments**-Schlüsselwort, das nicht mit dem Paket übereinstimmt, da FO = 0 ist. Der nächste ACL-Eintrag wird also verarbeitet.
2. Die zweite Zeile der ACL enthält Informationen zu Layer 3 und Layer 4. In diesem Fall stimmen die Layer-4-Informationen nicht überein, sodass der nächste ACL-Eintrag verarbeitet wird.
3. Die dritte Zeile der Zugriffskontrollliste blockiert alle Pakete, sodass das Paket abgelehnt wird.

Das Paket ist ein nicht initiales Fragment zum Server in einem Port 80-Fluss:

Die erste Zeile der ACL enthält Layer-3-Informationen, die mit den Layer-3-Informationen im Paket übereinstimmen. Beachten Sie, dass, obwohl dies Teil eines Port 80-Datenflusses ist, das nicht initiale Fragment keine Layer-4-Informationen enthält. Das Paket wird abgelehnt, da die Layer-3-Informationen übereinstimmen.

Das Paket ist ein nicht initiales Fragment zum Server in einem Port-21-Fluss:

Die erste Zeile der ACL enthält nur Layer-3-Informationen, die mit dem Paket übereinstimmen, sodass das Paket abgelehnt wird.

Das Paket ist ein initiales Fragment, kein Fragment oder nicht initiales Fragment zu einem anderen Host im Server-Subnetz:

1. Die erste Zeile der ACL enthält nur Layer-3-Informationen, die nicht mit dem Paket übereinstimmen. Daher wird die nächste ACL-Zeile verarbeitet.
2. Die zweite Zeile der ACL enthält Informationen zu Layer 3 und Layer 4. Die Layer-4- und

Layer-3-Informationen im Paket stimmen nicht mit denen der ACL überein, sodass die nächste ACL-Zeile verarbeitet wird.
3. Die dritte Zeile der ACL verweigert dieses Paket.

Fragmente Schlüsselwortszenarien

Szenario 1

Router B stellt eine Verbindung zu einem Webserver her, und der Netzwerkadministrator möchte nicht zulassen, dass Fragmente den Server erreichen. Dieses Szenario zeigt, was passiert, wenn der Netzwerkadministrator ACL 100 und ACL 101 implementiert. Die ACL wird eingehend auf die serielle0-Schnittstelle (s0) des Routers angewendet und sollte es nur nicht fragmentierten Paketen ermöglichen, den Webserver zu erreichen. Weitere Informationen finden Sie im Flussdiagramm zu Zugriffskontrolllisten und in den Abschnitten Wie Pakete einer Zugriffskontrollliste zugeordnet werden können.

Folgen der Verwendung des Schlüsselworts "Fragmente"

ACL 100 ist wie folgt:

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

access-list 100 deny ip any any
```

Die erste Zeile der ACL 100 erlaubt nur HTTP zum Server, aber sie erlaubt auch nicht initiale Fragmente zu jedem TCP-Port auf dem Server. Diese Pakete werden zugelassen, da nicht initiale Fragmente keine Layer-4-Informationen enthalten. Die ACL-Logik geht davon aus, dass bei Übereinstimmung der Layer-3-Informationen auch die Layer-4-Informationen übereinstimmen, wenn diese verfügbar sind. Die zweite Leitung ist implizit und verweigert den gesamten anderen Datenverkehr.

Beachten Sie, dass der neue ACL-Code mit Version 12.1(2) und 12.0(11) der Cisco IOS-Software Fragmente verwirft, die keiner anderen Zeile in der ACL entsprechen. Frühere Versionen ermöglichen die Übertragung nicht initialer Fragmente, wenn sie keiner anderen ACL-Zeile entsprechen.

ACL 101 ist wie folgt:

```
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
```

Die ACL 101 ermöglicht aufgrund der ersten Zeile keine nicht initialen Fragmente bis zum Server. Ein nicht initiales Fragment zum Server wird abgelehnt, wenn es auf die erste ACL-Zeile trifft, da die Layer-3-Informationen im Paket mit den Layer-3-Informationen in der ACL-Zeile übereinstimmen.

Ursprüngliche oder nicht fragmentierte Elemente für Port 80 auf dem Server stimmen auch mit der ersten Zeile der ACL für Layer-3-Informationen überein. Da jedoch das Schlüsselwort fragments vorhanden ist, wird der nächste ACL-Eintrag (die zweite Zeile) verarbeitet. Die zweite Zeile der ACL erlaubt die anfängliche oder nicht fragmentierte Konfiguration, da sie mit der ACL-Zeile für Layer-3- und Layer-4-Informationen übereinstimmen.

Nicht initiale Fragmente, die an die TCP-Ports anderer Hosts im Netzwerk 171.16.23.0 gerichtet sind, werden durch diese ACL blockiert. Die Layer-3-Informationen in diesen Paketen stimmen nicht mit den Layer-3-Informationen in der ersten ACL-Zeile überein, sodass die nächste ACL-Zeile verarbeitet wird. Die Layer-3-Informationen in diesen Paketen stimmen auch nicht mit den Layer-3-Informationen in der zweiten ACL-Zeile überein, sodass die dritte ACL-Zeile verarbeitet wird. Die dritte Leitung ist implizit und verweigert den gesamten Datenverkehr.

In diesem Szenario beschließt der Netzwerkadministrator, die ACL 101 zu implementieren, da er nur nicht fragmentierte HTTP-Datenflüsse zum Server zulässt.

Szenario 2

Ein Kunde hat an zwei verschiedenen Standorten eine Internetverbindung, und es besteht auch eine Backdoor-Verbindung zwischen den beiden Standorten. Die Richtlinie des Netzwerkadministrators besteht darin, der Gruppe A an Standort 1 den Zugriff auf den HTTP-Server an Standort 2 zu gestatten. Die Router an beiden Standorten verwenden private Adressen (RFC 1918) und Network Address Translation (NAT), um Pakete zu übersetzen, die über das Internet geroutet werden.

Der Netzwerkadministrator an Standort 1 leitet die privaten Adressen, die Gruppe A zugewiesen sind, so weiter, dass er die Backdoor über die Serial0 (s0) von Router A beim Zugriff auf den HTTP-Server an Standort 2 verwendet. Der Router an Standort 2 weist eine statische Route zu 172.16.10.0 auf, sodass der Rückverkehr an Gruppe A auch über die Hintertür weitergeleitet wird. Der gesamte andere Datenverkehr wird über NAT verarbeitet und über das Internet weitergeleitet. Der Netzwerkadministrator muss in diesem Szenario entscheiden, welche Anwendung oder welcher Datenfluss funktioniert, wenn die Pakete fragmentiert sind. Es ist nicht möglich, sowohl HTTP- als auch FTP-Datenflüsse gleichzeitig zu verwenden, da der eine oder der andere Fehler verursacht.

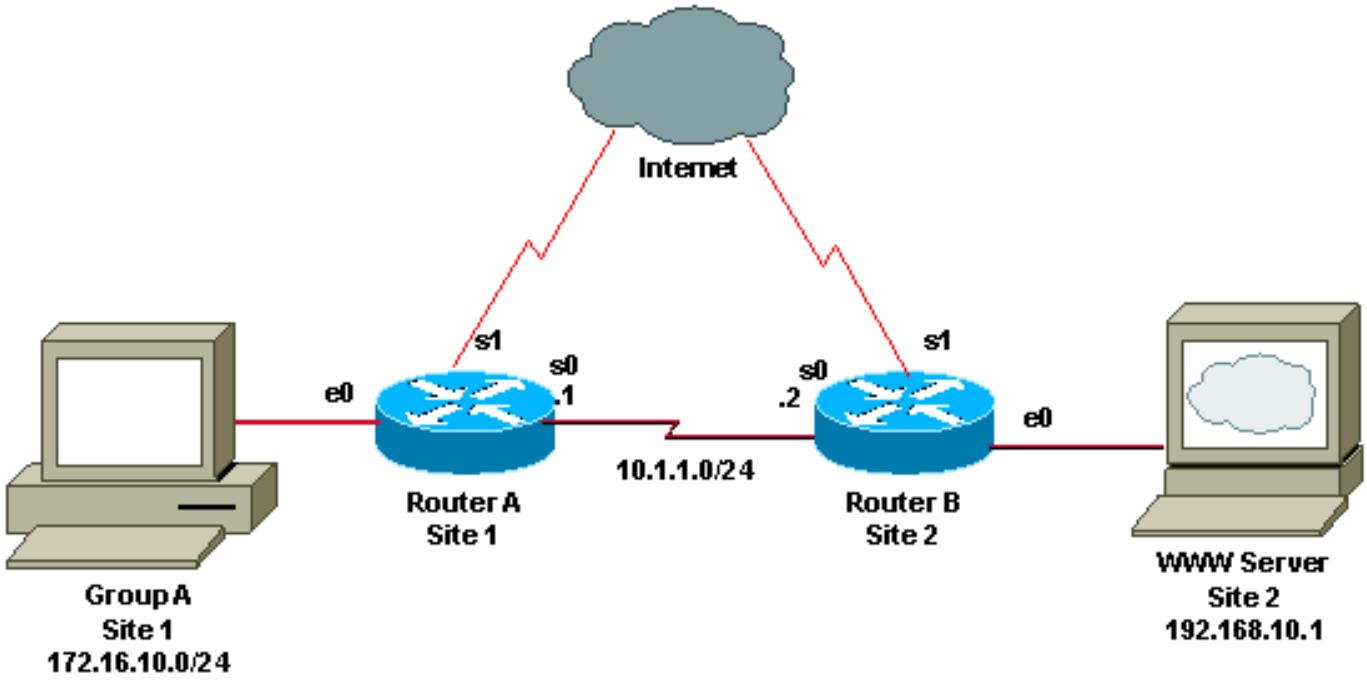
Weitere Informationen finden Sie im Flussdiagramm zu Zugriffskontrolllisten und in den Abschnitten Wie Pakete einer Zugriffskontrollliste zugeordnet werden können.

Erläuterung der Optionen des Netzwerkadministrators

Im folgenden Beispiel sendet die Routenübersicht FOO auf Router A Pakete, die mit ACL 100

übereinstimmen, über Router B bis s0. Alle Pakete, die nicht übereinstimmen, werden von NAT verarbeitet und nehmen die Standardroute über das Internet ein.

Hinweis: Wenn ein Paket unter die ACL fällt oder von dieser abgelehnt wird, wird es nicht von der Richtlinie weitergeleitet.



Im Folgenden sehen Sie eine Teilkonfiguration von Router A, die anzeigt, dass eine Richtlinienroute-Map mit dem Namen FOO auf die Schnittstelle e0 angewendet wird, auf der der Datenverkehr von Gruppe A in den Router eingeht:

```
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
```

Die ACL 100 ermöglicht das richtlinienbasierte Routing sowohl auf anfänglichen, nicht fragmentierten als auch nicht initialen Fragmenten von HTTP-Datenströmen zum Server. Initiale und nicht fragmentierte HTTP-Datenflüsse an den Server werden von der ACL zugelassen und die Richtlinie wird weitergeleitet, da sie mit den Layer-3- und Layer-4-Informationen in der ersten ACL-Zeile übereinstimmen. Nicht initiale Fragmente werden von der ACL zugelassen und werden weitergeleitet, da die Layer-3-Informationen im Paket auch mit der ersten ACL-Leitung übereinstimmen. Die ACL-Logik geht davon aus, dass die Layer-4-Informationen im Paket auch übereinstimmen, wenn sie verfügbar sind.

Hinweis: ACL 100 unterbricht andere Typen fragmentierter TCP-Datenflüsse zwischen Gruppe A und dem Server, da die anfänglichen und nicht initialen Fragmente über verschiedene Pfade zum Server gelangen. Die anfänglichen Fragmente werden von NAT verarbeitet und über das Internet weitergeleitet, die nicht initialen Fragmente desselben Datenflusses werden jedoch von Richtlinien

geroutet.

Ein fragmentierter FTP-Fluss veranschaulicht das Problem in diesem Szenario. Die ursprünglichen Fragmente eines FTP-Datenflusses stimmen mit den Layer-3-Informationen, nicht jedoch mit den Layer-4-Informationen der ersten ACL-Leitung überein. Diese werden anschließend von der zweiten Zeile abgelehnt. Diese Pakete werden von NAT verarbeitet und über das Internet weitergeleitet.

Die nicht initialen Fragmente eines FTP-Datenflusses stimmen mit den Layer-3-Informationen in der ersten ACL-Zeile überein, und die ACL-Logik geht von einer positiven Übereinstimmung mit den Layer-4-Informationen aus. Diese Pakete werden von der Richtlinie geroutet, und der Host, der diese Pakete neu zusammenfügt, erkennt die anfänglichen Fragmente nicht als Teil desselben Flusses wie die von der Richtlinie weitergeleiteten, nicht initialen Fragmente, da NAT die Quelladresse der ursprünglichen Fragmente geändert hat.

Mit der ACL 100 in der unten stehenden Konfiguration wird das FTP-Problem behoben. Die erste Zeile von ACL 100 verweigert sowohl die anfänglichen als auch die nicht initialen FTP-Fragmente von Gruppe A an den 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
```

Die anfänglichen Fragmente stimmen mit den Layer-3-Informationen in der ersten ACL-Zeile überein. Das Vorhandensein des **fragments-**Schlüsselworts bewirkt jedoch, dass die nächste ACL-Zeile verarbeitet wird. Das ursprüngliche Fragment stimmt nicht mit der zweiten ACL-Zeile für Layer-4-Informationen überein. Daher wird die nächste implizite Zeile der ACL verarbeitet, die das Paket ablehnt. Nicht initiale Fragmente stimmen mit den Layer-3-Informationen in der ersten Zeile der ACL überein, sodass sie abgelehnt werden. Sowohl die anfänglichen als auch die nicht initialen Fragmente werden von NAT verarbeitet und über das Internet weitergeleitet, sodass der Server kein Problem mit der Reassemblierung hat.

Durch das Fixieren von FTP-Datenflüssen werden fragmentierte HTTP-Datenflüsse unterbrochen, da die ursprünglichen HTTP-Fragmente jetzt per Richtlinie weitergeleitet werden, die nicht initialen Fragmente jedoch von NAT verarbeitet und über das Internet weitergeleitet werden.

Wenn ein anfängliches Fragment eines HTTP-Datenflusses von Gruppe A zum Server auf die erste Zeile der ACL trifft, wird es mit den Layer-3-Informationen in der ACL übereinstimmen. Aufgrund des **fragments-**Schlüsselworts wird die nächste Zeile der ACL verarbeitet. Die zweite Zeile der ACL erlaubt und leitet das Paket an den Server weiter.

Wenn nicht initiale HTTP-Fragmente, die für die Gruppe A an den Server bestimmt sind, auf die erste Zeile der ACL stoßen, stimmen die Layer-3-Informationen im Paket mit der ACL-Leitung überein, und das Paket wird abgelehnt. Diese Pakete werden von NAT verarbeitet und über das Internet zum Server geleitet.

Die erste ACL in diesem Szenario ermöglicht fragmentierte HTTP-Datenflüsse und die Unterbrechung fragmentierter FTP-Flüsse. Die zweite ACL ermöglicht fragmentierte FTP-Flüsse und unterbricht fragmentierte HTTP-Flüsse. Die TCP-Datenflüsse brechen in jedem Fall ab, da die anfänglichen und nicht initialen Fragmente unterschiedliche Pfade zum Server haben. Eine Reassemblierung ist nicht möglich, da NAT die Quelladresse der nicht initialen Fragmente geändert hat.

Es ist nicht möglich, eine ACL zu erstellen, die beide Arten von fragmentierten Datenflüssen zum Server zulässt. Daher muss der Netzwerkadministrator den gewünschten Datenfluss auswählen.

Zugehörige Informationen

- Support-Seite für IP-Routing
- Technischer Support und Dokumentation - Cisco Systems