Access Control Lists e IP Fragments

Sommario

Introduzione

In questo white paper vengono illustrati i diversi tipi di voci dell'elenco di controllo di accesso (ACL, Access Control List) e viene spiegato cosa succede quando diversi tipi di pacchetto incontrano queste varie voci. Gli ACL vengono usati per impedire che i pacchetti IP vengano inoltrati da un router.

RFC 1858 copre le considerazioni sulla sicurezza per il filtro dei frammenti IP e sottolinea due attacchi sugli host che coinvolgono frammenti IP di pacchetti TCP, il Tiny Fragment Attack e il Fragment Attack sovrapposto. Bloccare questi attacchi è desiderabile perché possono compromettere un host o bloccare tutte le risorse interne.

RFC 1858 descrive anche due metodi per difendersi da questi attacchi, diretti e indiretti. Nel metodo diretto, i frammenti iniziali di lunghezza inferiore a quella minima vengono eliminati. Il metodo indiretto prevede l'eliminazione del secondo frammento di un set di frammenti, a condizione che inizi al byte 8 del datagramma IP originale. Per ulteriori informazioni, vedere la RFC 1858 .

In genere, i filtri di pacchetto come gli ACL vengono applicati ai non frammenti e al frammento iniziale di un pacchetto IP perché contengono sia le informazioni di livello 3 che quelle di livello 4 con cui gli ACL possono confrontare la decisione di autorizzazione o di rifiuto. In genere, i frammenti non iniziali sono autorizzati tramite l'ACL perché possono essere bloccati in base alle informazioni di layer 3 contenute nei pacchetti; tuttavia, poiché questi pacchetti non contengono informazioni sul layer 4, non corrispondono alle informazioni sul layer 4 nella voce ACL, se esistente. Permettere il passaggio di frammenti non iniziali di un datagramma IP è accettabile in quanto l'host che riceve i frammenti non può ricomporre il datagramma IP originale senza il frammento iniziale.

I firewall possono essere utilizzati anche per bloccare i pacchetti mantenendo una tabella di frammenti indicizzati per indirizzo IP di origine e di destinazione, protocollo e ID IP. Sia il Cisco

PIX Firewall che il Cisco IOS® Firewall possono filtrare tutti i frammenti di un particolare flusso mantenendo questa tabella di informazioni, ma è troppo costoso farlo su un router per le funzionalità base degli ACL. Il compito principale di un firewall è bloccare i pacchetti, mentre il suo ruolo secondario è instradare i pacchetti; il compito principale di un router è indirizzare i pacchetti e il suo ruolo secondario è bloccarli.

Il software Cisco IOS versione 12.1(2) e 12.0(11) è stato modificato in due versioni per risolvere alcuni problemi di sicurezza relativi ai frammenti TCP. Il metodo indiretto, descritto nella RFC 1858 , è stato implementato nell'ambito del controllo di integrità dei pacchetti TCP/IP standard. Sono state apportate modifiche anche alla funzionalità degli ACL rispetto ai frammenti non iniziali.

Tipi di voci ACL

Sono disponibili sei tipi di righe ACL, ognuna delle quali ha una conseguenza se il pacchetto corrisponde o meno. Nell'elenco seguente, FO = 0 indica un frammento non iniziale o un frammento iniziale in una connessione TCP, FO > 0 indica che il pacchetto è un frammento non iniziale, L3 indica il livello 3 e L4 indica il livello 4.

Nota: se la riga ACL contiene informazioni sia sul layer 3 che sul layer 4 e la parola chiave **fragments** è presente, l'azione ACL è conservativa sia per le azioni di autorizzazione che per quelle di negazione. Le azioni sono conservative in quanto non si desidera negare accidentalmente una parte frammentata di un flusso in quanto i frammenti non contengono informazioni sufficienti per soddisfare tutti gli attributi del filtro. In questo caso, invece di negare un frammento non iniziale, viene elaborata la voce ACL successiva. Nel caso di autorizzazioni, si presume che le informazioni di layer 4 nel pacchetto, se disponibili, corrispondano alle informazioni di layer 4 nella riga ACL.

Consenti riga ACL con solo informazioni L3

1. Se le informazioni L3 di un pacchetto corrispondono alle informazioni L3 nella riga ACL, sono consentite.
2. Se le informazioni L3 di un pacchetto non corrispondono alle informazioni L3 nella riga ACL, viene elaborata la voce ACL successiva.

Riga ACL di rifiuto con solo informazioni L3

1. Se le informazioni L3 di un pacchetto corrispondono alle informazioni L3 nella riga ACL, il pacchetto viene rifiutato.
2. Se le informazioni L3 di un pacchetto non corrispondono alle informazioni L3 nella riga ACL, viene elaborata la voce ACL successiva.

Permit ACL line with L3 information only (Consenti riga ACL solo con informazioni L3) e la parola chiave fragments è presente

Se le informazioni L3 di un pacchetto corrispondono alle informazioni L3 nella linea ACL, viene controllato l'offset del frammento del pacchetto.

1. Se il valore FO è > 0, il pacchetto è autorizzato.
2. Se il valore FO di un pacchetto è = 0, viene elaborata la voce ACL successiva.

Riga Deny ACL con solo informazioni L3. È presente la parola chiave fragments

Se le informazioni L3 di un pacchetto non corrispondono alle informazioni L3 nella linea ACL, viene controllato il valore di offset del frammento del pacchetto.

1. Se il valore FO è > 0, il pacchetto viene rifiutato.
2. Se il valore FO di un pacchetto è = 0, viene elaborata la riga ACL successiva.

Linea ACL consentita con informazioni L3 e L4

1. Se le informazioni L3 e L4 di un pacchetto corrispondono alla riga ACL e FO = 0, il pacchetto è autorizzato.
2. Se le informazioni L3 di un pacchetto corrispondono alla riga ACL e FO > 0, il pacchetto è autorizzato.

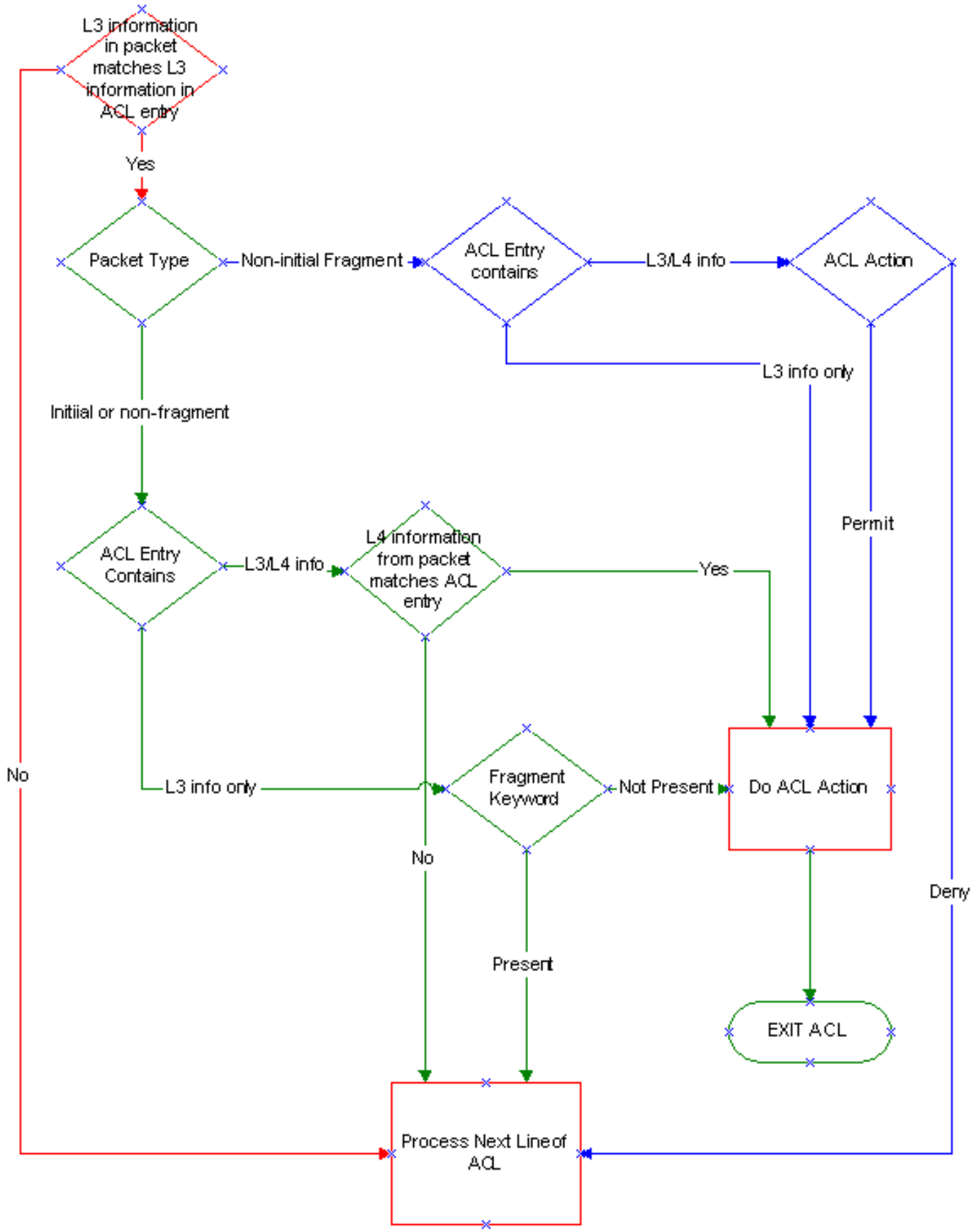
Riga ACL di rifiuto con informazioni L3 e L4

1. Se le informazioni L3 e L4 di un pacchetto corrispondono alla voce ACL e FO = 0, il pacchetto viene rifiutato.
2. Se le informazioni L3 di un pacchetto corrispondono alla riga ACL e FO > 0, viene elaborata la voce ACL successiva.

Diagramma di flusso delle regole ACL

Il diagramma di flusso seguente mostra le regole ACL quando i frammenti non frammentati, i frammenti iniziali e i frammenti non iniziali vengono confrontati con l'ACL.

Nota: i frammenti non iniziali contengono solo informazioni sul layer 3 e non sul layer 4, anche se l'ACL può contenere informazioni sul layer 3 e sul layer 4.



Corrispondenza dei pacchetti con un ACL

Esempio 1

I cinque scenari possibili riportati di seguito riguardano diversi tipi di pacchetti che incontrano ACL

100. Fare riferimento alla tabella e al diagramma di flusso per informazioni su quanto accade in ciascuna situazione. L'indirizzo IP del server Web è 171.16.23.1.

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

access-list 100 deny ip any any
```

Il pacchetto è un frammento iniziale o un non frammento destinato al server sulla porta 80:

La prima riga dell'ACL contiene informazioni sul layer 3 e sul layer 4, che corrispondono alle informazioni sul layer 3 e sul layer 4 nel pacchetto, quindi il pacchetto è autorizzato.

Il pacchetto è un frammento iniziale o un non frammento destinato al server sulla porta 21:

1. La prima riga dell'ACL contiene informazioni sul layer 3 e sul layer 4, ma le informazioni sul layer 4 nell'ACL non corrispondono al pacchetto, quindi viene elaborata la riga dell'ACL successiva.
2. La seconda riga dell'ACL rifiuta tutti i pacchetti, quindi il pacchetto viene rifiutato.

Il pacchetto è un frammento non iniziale inviato al server con un flusso di porta 80:

La prima riga dell'ACL contiene informazioni sul layer 3 e sul layer 4, le informazioni sul layer 3 nell'ACL corrispondono al pacchetto e l'azione ACL è autorizzare, quindi il pacchetto è autorizzato.

Il pacchetto è un frammento non iniziale inviato al server in un flusso della porta 21:

La prima riga dell'ACL contiene informazioni sia sul layer 3 che sul layer 4. Le informazioni di layer 3 nell'ACL corrispondono al pacchetto, il pacchetto non contiene informazioni di layer 4 e l'azione ACL è autorizzare, quindi il pacchetto è autorizzato.

Il pacchetto è un frammento iniziale, non frammentato o non iniziale inviato a un altro host nella subnet del server:

1. La prima riga dell'ACL contiene informazioni sul layer 3 che non corrispondono alle informazioni sul layer 3 nel pacchetto (l'indirizzo di destinazione), quindi viene elaborata la riga dell'ACL successiva.
2. La seconda riga dell'ACL rifiuta tutti i pacchetti, quindi il pacchetto viene rifiutato.

Esempio 2

Gli stessi cinque scenari possibili riguardano diversi tipi di pacchetti che incontrano l'ACL 101. Di nuovo, fare riferimento alla tabella e al diagramma di flusso come si segue cosa succede in ciascuna situazione. L'indirizzo IP del server Web è 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
```

Il pacchetto è un frammento iniziale o non frammentato destinato al server sulla porta 80:

1. La prima riga dell'ACL contiene informazioni sul layer 3 che corrispondono alle informazioni sul layer 3 nel pacchetto. L'azione ACL consiste nel negare, ma poiché è presente la parola chiave **fragments**, viene elaborata la voce ACL successiva.
2. La seconda riga dell'ACL contiene informazioni sul layer 3 e sul layer 4, che corrispondono al pacchetto, quindi il pacchetto è autorizzato.

Il pacchetto è un frammento iniziale o non frammentato destinato al server sulla porta 21:

1. La prima riga dell'ACL contiene informazioni sul layer 3, che corrispondono al pacchetto, ma la voce ACL contiene anche la parola chiave **fragments**, che non corrisponde al pacchetto perché FO = 0, quindi viene elaborata la voce ACL successiva.
2. La seconda riga dell'ACL contiene informazioni sul layer 3 e sul layer 4. In questo caso, le informazioni sul layer 4 non corrispondono, quindi viene elaborata la voce ACL successiva.
3. La terza riga dell'ACL rifiuta tutti i pacchetti, quindi il pacchetto viene rifiutato

Il pacchetto è un frammento non iniziale inviato al server con un flusso di porta 80:

La prima riga dell'ACL contiene informazioni sul layer 3 che corrispondono alle informazioni sul layer 3 nel pacchetto. Tenere presente che anche se questo fa parte di un flusso della porta 80, non ci sono informazioni sul layer 4 nel frammento non iniziale. Il pacchetto è stato rifiutato perché le informazioni sul layer 3 corrispondono.

Il pacchetto è un frammento non iniziale inviato al server in un flusso della porta 21:

La prima riga dell'ACL contiene solo informazioni sul layer 3 e corrisponde al pacchetto, quindi il pacchetto viene rifiutato.

Il pacchetto è un frammento iniziale, non frammentato o non iniziale inviato a un altro host nella subnet del server:

1. La prima riga dell'ACL contiene solo informazioni sul layer 3 e non corrisponde al pacchetto, quindi viene elaborata la riga dell'ACL successiva.
2. La seconda riga dell'ACL contiene informazioni sul layer 3 e sul layer 4. Le informazioni di layer 4 e layer 3 nel pacchetto non corrispondono a quelle dell'ACL, quindi viene elaborata la riga dell'ACL successiva.
3. La terza riga dell'ACL rifiuta questo pacchetto

Scenari con parole chiave fragments

Scenario 1

Il router B si connette a un server Web e l'amministratore di rete non desidera consentire ai frammenti di raggiungere il server. In questo scenario viene mostrato cosa succede se l'amministratore di rete implementa gli ACL 100 rispetto agli ACL 101. L'ACL viene applicato in entrata sull'interfaccia Serial0 (s0) dei router e deve consentire solo ai pacchetti non frammentati di raggiungere il server Web. Vedere il diagramma di flusso delle regole ACL e le sezioni Come i pacchetti possono corrispondere a un ACL mentre si segue lo scenario.

Conseguenze dell'uso della parola chiave fragments

Di seguito viene riportato l'ACL 100:

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

access-list 100 deny ip any any
```

La prima riga dell'ACL 100 permette solo il protocollo HTTP al server, ma permette anche ai frammenti non iniziali di raggiungere qualsiasi porta TCP sul server. Questi pacchetti sono autorizzati perché i frammenti non iniziali non contengono informazioni sul layer 4 e la logica dell'ACL presume che se le informazioni sul layer 3 corrispondono, anche le informazioni sul layer 4, se disponibili, corrisponderebbero. La seconda linea è implicita e nega tutto il resto del traffico.

Èimportante notare che, a partire dal software Cisco IOS versione 12.1(2) e 12.0(11), il nuovo codice ACL elimina i frammenti che non corrispondono a nessuna altra riga dell'ACL. Nelle versioni precedenti, i frammenti non iniziali possono passare attraverso se non corrispondono a nessuna altra riga dell'ACL.

Di seguito viene riportato l'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 non consente il passaggio di frammenti non iniziali al server a causa della prima riga. Quando rileva la prima riga dell'ACL, un frammento non iniziale inviato al server viene rifiutato in quanto le informazioni di layer 3 nel pacchetto corrispondono alle informazioni di layer 3 nella riga dell'ACL.

Anche i frammenti iniziali o non iniziali della porta 80 sul server corrispondono alla prima riga

dell'ACL per le informazioni sul layer 3, ma, poiché la parola chiave fragments è presente, viene elaborata la voce dell'ACL successiva (la seconda riga). La seconda riga dell'ACL permette i frammenti iniziali o non, in quanto corrispondono alla riga ACL per le informazioni di layer 3 e layer 4.

I frammenti non iniziali destinati alle porte TCP di altri host sulla rete 171.16.23.0 vengono bloccati da questo ACL. Le informazioni di layer 3 in questi pacchetti non corrispondono alle informazioni di layer 3 nella prima riga dell'ACL, quindi viene elaborata la riga dell'ACL successiva. Le informazioni di layer 3 in questi pacchetti non corrispondono neanche alle informazioni di layer 3 nella seconda riga ACL, quindi viene elaborata la terza riga ACL. La terza linea è implicita e nega tutto il traffico.

In questo scenario, l'amministratore di rete decide di implementare l'ACL 101 perché consente solo flussi HTTP non frammentati verso il server.

Scenario 2

Un cliente dispone di una connessione a Internet in due siti diversi e tra i due siti è disponibile anche una connessione tramite backdoor. Il criterio dell'amministratore di rete prevede di consentire al Gruppo A nel Sito 1 di accedere al server HTTP nel Sito 2. I router di entrambi i siti utilizzano indirizzi privati (RFC 1918) e NAT (Network Address Translation) per tradurre i pacchetti instradati tramite Internet.

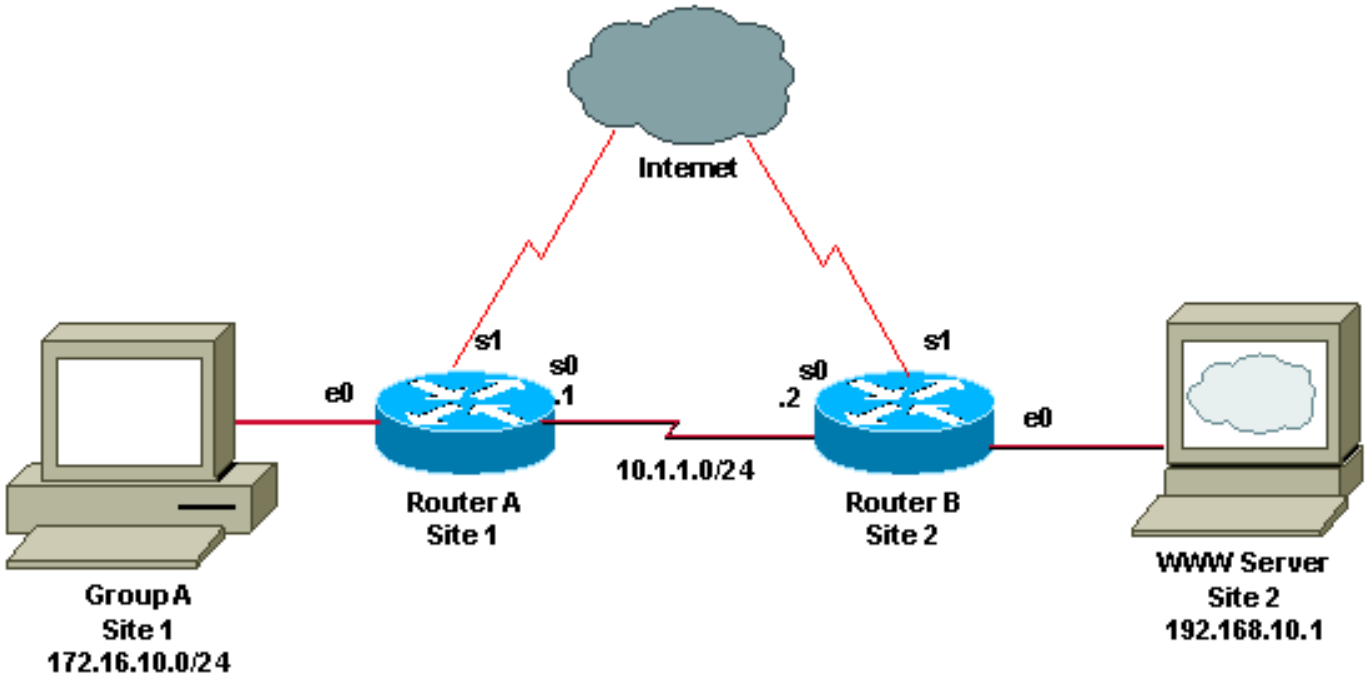
L'amministratore di rete del Sito 1 sta indirizzando tramite policy gli indirizzi privati assegnati al Gruppo A, in modo che utilizzino la backdoor attraverso il router A Serial0 (s0) quando accedono al server HTTP del Sito 2. Il router del Sito 2 ha una route statica a 172.16.10.0, in modo che anche il traffico di ritorno al Gruppo A venga instradato attraverso la backdoor. Tutto il resto del traffico viene elaborato da NAT e instradato tramite Internet. In questo scenario, l'amministratore di rete deve decidere quale applicazione o flusso funzionerà se i pacchetti vengono frammentati. Non è possibile far funzionare contemporaneamente i flussi HTTP e FTP (File Transfer Protocol) perché uno dei due si interrompe.

Vedere il diagramma di flusso delle regole ACL e le sezioni Come i pacchetti possono corrispondere a un ACL mentre si segue lo scenario.

Spiegazione delle opzioni dell'amministratore di rete

Nell'esempio seguente, la mappa dei percorsi chiamata FOO sul router A invia i pacchetti che corrispondono all'ACL 100 dal router B al router S0. Tutti i pacchetti che non corrispondono vengono elaborati da NAT e accettano il percorso predefinito attraverso Internet.

Nota: se un pacchetto cade dalla parte inferiore dell'ACL o viene rifiutato, non viene indirizzato in base a criteri.



Di seguito viene riportata una configurazione parziale del router A, che mostra come all'interfaccia e0 venga applicata una mappa dei percorsi basata su criteri chiamata FOO, in cui il traffico proveniente dal gruppo A entra nel router:

```
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 consente il routing delle policy sui frammenti iniziali, non iniziali e non iniziali dei flussi HTTP verso il server. I flussi HTTP iniziali e non frammentati verso il server sono autorizzati dall'ACL e i criteri sono instradati perché corrispondono alle informazioni di layer 3 e layer 4 nella prima riga dell'ACL. I frammenti non iniziali sono autorizzati dall'ACL e la policy viene indirizzata perché le informazioni di layer 3 nel pacchetto corrispondono anche alla prima riga dell'ACL; la logica dell'ACL presume che le informazioni di layer 4 nel pacchetto corrispondano anche se fossero disponibili.

Nota: ACL 100 interrompe altri tipi di flussi TCP frammentati tra il gruppo A e il server perché i frammenti iniziali e non iniziali raggiungono il server attraverso percorsi diversi; i frammenti iniziali vengono elaborati da NAT e instradati tramite Internet, ma i frammenti non iniziali dello stesso flusso vengono instradati tramite policy.

Un flusso FTP frammentato aiuta a illustrare il problema in questo scenario. I frammenti iniziali di un flusso FTP corrispondono alle informazioni del layer 3, ma non alle informazioni del layer 4, della prima linea ACL, e vengono quindi negati dalla seconda linea. Questi pacchetti vengono elaborati da NAT e instradati attraverso Internet.

I frammenti non iniziali di un flusso FTP corrispondono alle informazioni del layer 3 nella prima riga

dell'ACL, quindi la logica dell'ACL presuppone una corrispondenza positiva con le informazioni del layer 4. Questi pacchetti sono indirizzati ai criteri e l'host che ricompone i pacchetti non riconosce i frammenti iniziali come parte dello stesso flusso dei frammenti non iniziali indirizzati ai criteri perché NAT ha modificato l'indirizzo di origine dei frammenti iniziali.

ACL 100 nella configurazione seguente risolve il problema FTP. La prima riga dell'ACL 100 rifiuta i frammenti FTP iniziali e non iniziali dal gruppo A al 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
```

I frammenti iniziali corrispondono alle informazioni del layer 3 nella prima riga dell'ACL, ma la presenza della parola chiave **fragments** causa l'elaborazione della riga dell'ACL successiva. Il frammento iniziale non corrisponde alla seconda riga dell'ACL per le informazioni di layer 4, quindi viene elaborata la riga implicita successiva dell'ACL, che rifiuta il pacchetto. I frammenti non iniziali corrispondono alle informazioni del layer 3 nella prima riga dell'ACL, quindi vengono rifiutati. I frammenti iniziali e non iniziali vengono elaborati da NAT e instradati tramite Internet, quindi il server non ha problemi di riassemblaggio.

La correzione dei flussi FTP interrompe i flussi HTTP frammentati, in quanto i frammenti HTTP iniziali vengono ora instradati secondo le policy, mentre i frammenti non iniziali vengono elaborati da NAT e instradati tramite Internet.

Quando un frammento iniziale di un flusso HTTP dal gruppo A al server incontra la prima riga dell'ACL, trova una corrispondenza nelle informazioni di layer 3 nell'ACL, ma, a causa della parola chiave **fragments**, viene elaborata la riga successiva dell'ACL. La seconda riga dell'ACL autorizza e regola il routing del pacchetto al server.

Quando i frammenti HTTP non iniziali destinati dal gruppo A al server incontrano la prima riga dell'ACL, le informazioni di layer 3 nel pacchetto corrispondono alla riga dell'ACL e il pacchetto viene rifiutato. Questi pacchetti vengono elaborati da NAT e attraversano Internet per raggiungere il server.

Il primo ACL di questo scenario consente flussi HTTP frammentati e interrompe flussi FTP frammentati. Il secondo ACL consente flussi FTP frammentati e interrompe i flussi HTTP frammentati. I flussi TCP si interrompono in ciascun caso perché i frammenti iniziali e non iniziali utilizzano percorsi diversi per raggiungere il server. Impossibile riassemblare. NAT ha modificato l'indirizzo di origine dei frammenti non iniziali.

Poiché non è possibile costruire un ACL che consenta entrambi i tipi di flussi frammentati verso il server, l'amministratore di rete deve scegliere il flusso da utilizzare.

Informazioni correlate

- Pagina di supporto per il routing IP
- Documentazione e supporto tecnico – Cisco Systems