Implementazione degli elenchi degli accessi sui router Internet serie 12000

Sommario

Introduzione

In questo documento viene descritto il supporto degli Access Control List (ACL) sui router Internet Cisco serie 12000.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza delle nozioni di base sul funzionamento di un ACL su un router Cisco.

Per informazioni generali sugli ACL e le relative applicazioni, consultare i seguenti documenti:

- Access Control Lists: Panoramica e linee guida
- Configurazione dei servizi IP: Filtra pacchetti IP

Componenti usati

Per la stesura del documento, sono stati usati router Internet Cisco serie 12000.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica del supporto ACL su Cisco serie 12000 Internet Router

Sui router Internet Cisco serie 12000, gli ACL possono essere elaborati in hardware (ASIC - Application-Specific Integrated Circuit), software (CPU di una scheda di linea) o come funzionalità ibrida - elaborati in software con assistenza hardware. L'elaborazione di un ACL nell'hardware o nel software dipende dall'applicazione ACL, dal tipo di motore della scheda di linea e dall'interazione degli ACL nelle altre schede di linea.

I motori delle schede di linea Cisco serie 12000 offrono diverse funzionalità ACL. Per informazioni sul supporto degli ACL per un particolare motore di scheda di linea, consultare la sezione corrispondente in questo documento.

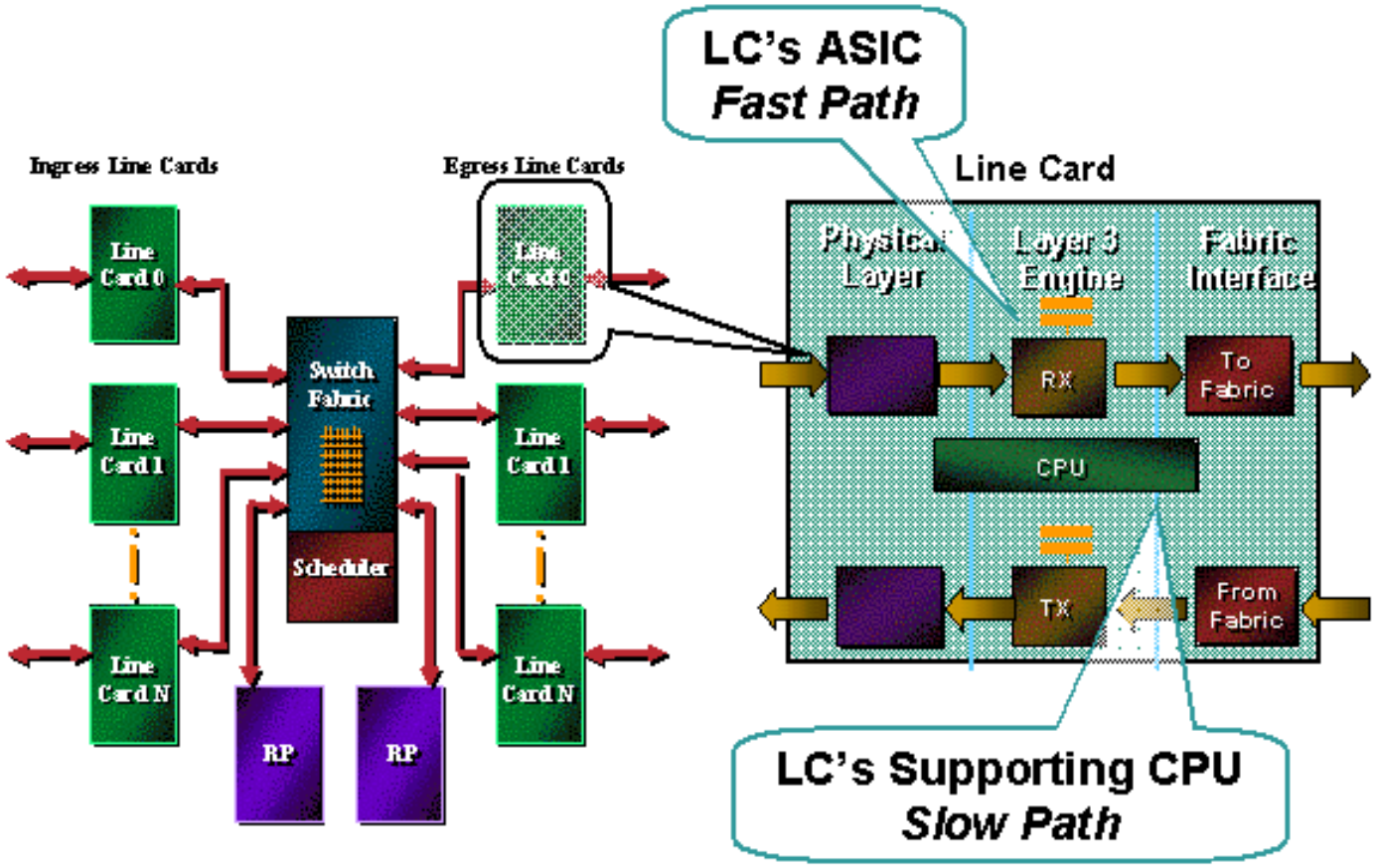
Nota: gli ACL IP multicast non sono supportati nel software Cisco IOS® versione 12.0S. La funzione IP Multicast Boundary può essere utilizzata dove è richiesto il filtro multicast. Per ulteriori informazioni, fare riferimento a Fast-Path Multicast Forwarding su Cisco serie 12000 Engine 2 e sulle schede di linea ISE.

ACL basati su ASIC e ACL basati su CPU

Cisco 12000 supporta tutte le generazioni di elaborazione degli ACL. Per un uso efficace degli ACL su Cisco 12000, è essenziale avere una comprensione operativa del funzionamento, dell'interazione e del supporto reciproci di ciascuna modalità di elaborazione.

Nelle prime generazioni di elaborazione degli ACL, veniva usata una CPU programmabile per elaborare gli ACL. Nel tempo, i requisiti di elaborazione del pacchetto al secondo (PPS) superavano la capacità delle nuove CPU di tenere il passo. Gli ASIC sono stati creati per ottenere velocità PPS più elevate per l'inoltro dei router e le funzionalità. Gli ACL caricati sulla CPU della scheda di linea (LC) sono stati quindi caricati sull'ASIC LC. Gli ASIC continuarono a essere improvvisati per gestire velocità PPS più elevate. Questi ASIC di seconda generazione sono stati creati sulla base del lavoro pionieristico della generazione precedente e offrono maggiori

funzionalità ASIC. Poiché Cisco 12000 è una piattaforma di routing distribuito, l'interazione tra le diverse generazioni di elaborazione degli ACL può creare una certa confusione operativa.



In questo documento vengono usati termini come ACL basato su ASIC, ACL basato su CPU, Fast Path, Slow Path e ASIC Punts per spiegare cosa succede all'elaborazione degli ACL. Ecco le spiegazioni di questi termini:

- ACL basati su ASIC (Fast Path): gli ACL vengono caricati ed elaborati nell'hardware ASIC. Il livello di prestazioni dell'ASIC determina la profondità, le prestazioni e le funzionalità dell'ACL. Fast Path è stato utilizzato nel percorso per illustrare la differenza tra l'elaborazione basata su ASIC e l'elaborazione eseguita nella CPU con supporto LC. Nel presente documento viene utilizzato il termine più generico, basato su ASIC.
- ACL basati sulla CPU (Slow Path): gli ACL vengono elaborati nel software sulla CPU della scheda di linea. Per le schede di prima generazione (motore 0 e in alcuni casi motore 1), tutta l'elaborazione viene eseguita sulla CPU LC. I controller di dominio basati sull'ASIC eseguono l'elaborazione degli ACL sui pacchetti provenienti dall'ASIC. Slow Path è stato usato in passato per illustrare come i punt alla CPU LC erano più lenti dell'ASIC. Nel presente documento viene utilizzato il termine più generico, basato sulla CPU.
- Punte ASIC (ASIC Punts) - Gli ASIC hanno buste di progettazione molto rigide. Quando un pacchetto supera l'inviluppo progettato, viene puntato dall'ASIC per essere elaborato sul LC che supporta la CPU o inviato al Route Processor (RP). Gli ACL basati sull'ASIC restringono i pacchetti che non rientrano nella progettazione dell'ASIC. Un esempio è un ACL con una ACE con una parola chiave log o log-input. Le informazioni richieste per registrare il pacchetto devono essere elaborate all'esterno dell'ASIC, in modo che il pacchetto venga automaticamente reindirizzato dall'ASIC alla CPU della CPU della CPU e elaborato come un normale ACL basato sulla CPU.

Nota: quando si configura il routing basato su criteri (PBR) con istruzioni match per far

corrispondere gli ACL, gli ACL non devono corrispondere alla porta di origine. Il router dello switch Gigabit (GSR) non supporta la commutazione hardware per il PBR con ACL corrispondenti alla porta di origine. Innesca la commutazione di processo e il peggioramento delle prestazioni GSR.

Filtraggio del piano di controllo e gestione

Il processore router offre servizi di controllo e gestione del piano nell'architettura distribuita della serie Cisco 12000. Gli ACL di ricezione del percorso (ACL) offrono una semplice funzionalità di filtro distribuito per il controllo e la gestione del traffico destinato all'RP. Può essere visto logicamente come un ulteriore livello di sicurezza che sfrutta i punti di forza di un'architettura distribuita.

Configurazione degli ACL del percorso di ricezione IP

L'ACL è stato introdotto tramite una funzionalità speciale nel software Cisco IOS® versione 12.0(21)S2. È ufficialmente supportato nel software Cisco IOS versione 12.0(22)S. Per ulteriori informazioni, fare riferimento a IP Receive ACL.

Il processore router offre servizi di control plane nell'architettura distribuita della serie Cisco 12000. Gli ACL di ricezione offrono funzionalità di filtro per il controllo del traffico destinato all'RP, ad esempio aggiornamenti di routing e query SNMP (Simple Network Management Protocol).

L'rACL è considerato la fase 1 di uno sforzo multifase per aggiungere nuove protezioni al controllo e alla gestione del traffico aereo. Gli aggiornamenti software apportano nuovi miglioramenti alle limitazioni di velocità.

Supporto ACL IPv4 per tipo di scheda di linea

Le schede di linea della serie 12000 offrono funzionalità ACL diverse per ciascun tipo di motore. In questa sezione vengono descritte le funzionalità degli ACL dei diversi motori delle schede di linea. Per informazioni sul supporto degli ACL per un particolare motore di scheda di linea, vedere la sezione corrispondente di questo documento.

Esistono alcune caratteristiche generali per tutti gli ACL (basati su ASIC e CPU):

- Èpossibile applicare un solo ACL a un'interfaccia per ciascuna direzione. Ad esempio, l'interfaccia POS 0/0 può avere solo un ACL di input e un ACL di output.
- Il test del pacchetto con un ACL si interrompe dopo che viene trovata una corrispondenza. Se un ACL con 300 voci corrisponde al pacchetto con Access-list Entry (ACE) #45, il pacchetto viene elaborato e l'elaborazione dell'ACL interrotta.
- Alla fine di ciascun ACL, è presente un'istruzione implicita di **negazione** di **tutte** le voci. Di conseguenza, se non c'è corrispondenza nell'ACL, il pacchetto viene scartato. Gli ACL Cisco vengono creati con un'architettura ACL *con permesso esplicito*. Ciò significa che per essere elaborato e inoltrato, il pacchetto deve essere associato a un ACE.
- Le voci di controllo di accesso appena aggiunte vengono sempre aggiunte alla fine dell'ACL. Quando l'ACL deve essere aggiornato, è buona norma rimuovere l'ACL (usare il comando **no access-list**) e aggiungere nuovamente il nuovo ACL.
- Poiché i frammenti IP non iniziali non contengono informazioni sul protocollo di layer 4 nell'intestazione IP, per i frammenti non iniziali sono supportati solo i criteri di corrispondenza

standard. Per informazioni dettagliate sulla conformità degli ACL Cisco al filtro dei frammenti IP, consultare le liste di controllo dell'accesso e i frammenti IP.

- Gli ACL numerati vengono elaborati e applicati appena immessi tramite l'interfaccia della riga di comando (CLI). Con ACL di grandi dimensioni, a volte si verifica un picco della CPU sull'RP o sulla CPU LC.

Motore 0 - Elaborazione ACL

Il motore 0 è la prima scheda di linea fornita per Cisco 12000. È tutto basato sulla CPU per l'elaborazione e l'inoltro. Pertanto, le schede di linea del motore 0 elaborano gli ACL nella CPU LC.

Queste schede di linea sono basate sul motore 0:

Tipo di scheda di linea	Tipo di interfaccia	Connettività
12 DS3	Coassiale	PMI
12 DS3	Coassiale	PMI
12 E3	Coassiale	PMI
1xCHOC12->DS3		IR
1xCHOC12/STM4 ->OC3/STM1	POS	IR
4 OC3c/STM1c	POS	SR
4 OC3c/STM1c	POS	LR
4 OC3c/STM1c	POS	MM
1xOC12c/STM4c	POS	IR
1xOC12c/STM4c	POS	MM
6xCT3->DS1		PMI
2xCHOC3/STM1->DS1/E1		IR
4 OC3c/STM1c	ATM	IR
4 OC3c/STM1c	ATM	MM
1xOC12c/STM4c	ATM	IR
1xOC12c/STM4c	ATM	MM

Criteri di corrispondenza supportati

Tutti gli ACL Cisco IOS versione 12.0S Standard, Extended ACL e Turbo ACL sono supportati sul motore 0.

Numero di ACE supportati

Le dimensioni degli ACL sono limitate solo dai requisiti di prestazioni e dalle risorse di memoria disponibili.

Elaborazione ACL di output

Gli ACL di uscita vengono elaborati nel percorso della funzionalità in entrata nelle altre schede di linea del sistema. Il push dell'ACL di uscita sul lato in entrata degli altri LC protegge il backplane dall'inoltro dei pacchetti che verranno scartati. Si tratta di una funzione ereditata dall'architettura distribuita del Cisco 7500. Una spiegazione dettagliata, le ragioni e le linee guida operative sono fornite nella matrice IPv4 Output ACL - Line Card Interoperation.

Comandi specifici della scheda di linea

Nessuna.

Linee guida operative e interazioni con le schede di linea

- Se NetFlow è configurato su una scheda di linea Engine 0 e un ACL di output è configurato su una scheda di linea Engine 3 o 4+, l'ACL di output viene elaborato sia dalle schede di linea in entrata che da quelle in uscita in modo da consentire a NetFlow di registrare i pacchetti rifiutati dagli ACL e i pacchetti inoltrati.

Raccomandazioni

Cisco consiglia di utilizzare gli ACL turbo sul motore 0 per gli ACL di grandi dimensioni. Gli ACL lineari di piccole dimensioni sono più efficienti per gli ACL di piccole dimensioni in quanto gli ACL turbo richiedono una quantità di memoria aggiuntiva.

Motore 1 - Elaborazione ACL

Panoramica

La scheda di linea Engine 1 è un ponte tra l'elaborazione basata sulla CPU sul Engine 0 e l'ASIC di inoltro/funzionalità di prima generazione sul Engine 2. Le schede di linea Engine 1 elaborano gli ACL nel software per impostazione predefinita. Con il software Cisco IOS versione 12.0(10)S e successive, il motore 1 fornisce ACL hardware per le schede dotate della versione 4 o 5 dell'ASIC Salsa (per informazioni sulla versione di Salsa fornita su una scheda specifica, vedere la guida di riferimento dei comandi della scheda di linea riportata di seguito).

Queste schede di linea sono basate sul motore 1:

Tipo di scheda di linea	Tipo di interfaccia	Connettività
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
1xGE	SX	GBIC:
1xGE	SX	GBIC:
2 OC12c/STM4c	DPT	IR
2 OC12c/STM4c	DPT	LR
2 OC12c/STM4 c	DPT	XLR

2 OC12c/STM4c	DPT	MM
2 OC12c/STM4c	DPT	IR
2 OC12c/STM4c	DPT	LR
2cOC12c/STM4c	DPT	XLR
2 OC12c/STM4c	DPT	MM

Criteri di corrispondenza supportati

Tutti gli ACL standard, estesi e turbo supportati dal software Cisco IOS versione 12.0S sono supportati nella CPU LC (Slow Path). Inoltre, il motore 1 può elaborare gli ACL di input nell'ASIC Salsa. Salsa ASIC gestisce l'elaborazione degli ACL di input insieme alla ricerca dei percorsi, migliorando le prestazioni rispetto all'elaborazione degli ACL lineari tradizionali e degli ACL turbo. Salsa ASIC non può elaborare ACL di output o ACL di sottointerfaccia.

Numero di ACE supportati

Le dimensioni degli ACL sono limitate solo dai requisiti di prestazioni e dalle risorse di memoria disponibili.

Elaborazione ACL di output

Gli ACL di uscita vengono elaborati nel percorso della funzionalità in entrata nelle altre schede di linea del sistema. Per ulteriori informazioni, vedere la sezione ACL di output IPv4 - matrice di interoperabilità della scheda di linea.

Comandi specifici della scheda di linea

- **access-list salsa hardware**
- **show controller l3 | includere ASIC**

Linee guida operative e interazioni con le schede di linea

- L'ASIC Salsa e l'ASIC PSA non possono essere gestiti contemporaneamente. Il comando **access-list hardware** accetta solo PSA (Engine 2) o Salsa (Engine 1) ma non entrambi.
- Se NetFlow è configurato su una scheda di linea Engine 1 e un ACL di output è configurato su una scheda di linea Engine 3 o 4+, l'ACL di output viene elaborato sia dalle schede di linea in entrata che da quelle in uscita in modo da consentire a NetFlow di registrare i pacchetti rifiutati dagli ACL e i pacchetti inoltrati.

Raccomandazioni

Per le versioni delle schede di linea del motore 1 che non supportano ACL hardware, Cisco consiglia di utilizzare ACL turbo per ACL di grandi dimensioni. È possibile implementare piccoli ACL (con meno di 20 linee) come ACL lineari per preservare la memoria.

Motore 2 - Elaborazione ACL

Panoramica

Il Engine 2 è stato la prima scheda di linea con un ASIC di inoltro/funzionalità. Con il software Cisco IOS versione 12.0(10)S e successive, le schede di linea del motore 2 offrono funzionalità ACL hardware nell'ASIC (Packet Switching) a elevate prestazioni. Come per tutti gli ASIC di inoltro/funzionalità, gli inviluppi rigidi delle prestazioni pongono limiti alle funzionalità dell'ASIC. L'inviluppo di prestazioni delle chiavi negli ACL Engine 2 è dovuto a limitazioni della memoria nell'ASIC PSA.

L'inoltro dei pacchetti nel motore 2 viene eseguito dall'ASIC PSA. PSA ha tre memorie esterne principali:

- PLU (Path-lookup) - Utilizzato per memorizzare i nodi della matrice
- TLU (Table Lookup) - Utilizzato per memorizzare le foglie FIB e possibilmente le strutture di bilanciamento del carico. Utilizzato anche per contenere molte strutture di dati degli ACL PSA
- SRAM - Posizione principale per le strutture di condivisione del carico

La funzionalità ACL di PSA è un'implementazione basata su microcodice del controllo ACL. Nel chip PSA viene caricato uno speciale set di istruzioni che consente il controllo di base degli ACL. Per questa funzionalità sono previste alcune limitazioni che è necessario valutare attentamente prima di procedere alla distribuzione. Uno dei principali inconvenienti degli ACL PSA è la grande quantità di memoria di inoltro hardware richiesta.

La funzionalità ACL di PSA richiede la preallocazione di un ampio blocco di memoria PLU/TLU, a prescindere dal numero di prefissi, ecc. Poiché questa assegnazione proviene principalmente dall'area TLU, ha un impatto significativo sul numero di route che possono essere gestite su queste schede quando vengono configurati gli ACL PSA.

Oltre alla memoria iniziale di PLU/TLU, ciascun prefisso memorizzato nella memoria TLU richiede una quantità di memoria significativamente maggiore. La quantità di memoria richiesta per ciascun prefisso varia in base alla direzione dell'ACL applicato (in entrata o in uscita) e al tipo di scheda di linea. In generale, gli ACL in uscita richiedono una quantità di memoria maggiore rispetto agli ACL in entrata e le schede di linea con un numero di porte fisiche maggiore richiedono una quantità di memoria maggiore rispetto a quelle con un numero di porte inferiore.

Nel caso in cui la scheda di linea del Engine 2 non utilizzi gli ACL, le strutture di dati per gli ACL vengono costruite indipendentemente dagli ACL configurati. Per modificare le strutture non ACL di dimensioni inferiori, è necessario configurare **sul** router **nessun** access-**list** hardware **psa**. Questo comando disabilita tutta l'elaborazione ACL su tutte le schede di linea Engine2 in tutte le direzioni. Cisco consiglia di utilizzarli con estrema cautela.

Panoramica

Per fornire prestazioni di elaborazione degli ACL indipendenti dalla profondità della corrispondenza, gli ACL del motore 2 sono integrati nella tabella di inoltro hardware. Di seguito sono riportate le spiegazioni su come ciò possa influire sulla scalabilità dei prefissi.

Queste schede di linea sono basate sul motore 2:

Tipo di scheda di linea	Tipo di interfaccia	Connettività
1xOC48c/STM16	POS	SR

c		
1xOC48c/STM16c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC192c/STM64c	Enabler	SR
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	ATM	IR
4xOC12c/STM4c	ATM	MM
8xOC3cSTM1c	ATM/TS	IR
8xOC3c/STM1c	ATM/TS	MM
3xGE	SX	GBIC:
3xGE	CWDM	GBIC:
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR

Criteri di corrispondenza supportati

Tutti i software Cisco IOS versione 12.0S supportano i criteri di corrispondenza degli ACL standard ed estesi, ad eccezione delle porte di origine di layer 4. Le maschere discontinue, i campi di precedenza IP e le porte di origine di layer 4 vengono punzonate dall'ASIC PSA ed elaborate sulla CPU LC.

Numero di ACE supportati

Fino a cinque ACL di input a 448 linee nel PSA. È possibile configurare un ACL per porta. Gli ACL aggiuntivi vengono amministrati dalla CPU della scheda di linea. Per le restrizioni sugli ACL di output, vedere la sezione "Restrizioni" più avanti.

Elaborazione ACL di output

Un ACL di uscita configurato su questa scheda di linea verrà eseguito nel percorso della

funzionalità in entrata delle altre schede di linea del sistema. Per ulteriori informazioni, vedere la matrice di interoperabilità tra schede di linea e ACL di output IPv4.

Comandi specifici della scheda di linea

- **access-list limite psa hardware 128**
- **psa hardware access-list non disponibile**
- **bypass psa**
- **mostra dettagli psa access-list**
- **mostra riepilogo psa access-list**
- **funzione show controller psa**

Linee guida operative e interazioni con le schede di linea

- L'elaborazione degli ACL con percorso rapido richiede il rispetto delle seguenti condizioni:L'ACL applicato rientra nel limite di 128 o 448 ACE.Se il comando **access-list hardware psa limit 128** è configurato, la lunghezza deve essere inferiore a 128 ACE.La lunghezza deve essere inferiore a 448 ACE quando è richiesto il bundle del microcodice ACL a 448 linee.Gli ACL di input e output non sono configurati insieme per scheda.Èpossibile configurare fino a cinque ACL di uscita sul *router*.
- Solo gli ACL a 128 linee sono supportati sulle schede di linea OC-3/STM-1 POS a 8 e 16 porte. 448 ACL di linea sono supportati sui POS OC-12/STM-4 a 4 porte, sui POS OC-48/STM-16 a 1 porta e sulle schede di linea Gigabit Ethernet a 3 porte.
- Quando entrambi gli ACL sono configurati contemporaneamente sulla stessa scheda (l'ACL di output viene elaborato sul percorso lento), gli ACL di input hanno priorità sul percorso rapido sugli ACL di output.
- Se un ACL di uscita è configurato su una scheda Engine 2 e la scheda di linea in entrata è Engine 0/1/2/4, nella scheda in entrata verrà elaborato un ACL di uscita. Per altri tipi di motori, l'ACL di output verrà elaborato nel percorso lento in uscita del motore 2.
- Gli ACL di output non sono supportati per il traffico IP-MPLS (la prima etichetta MPLS viene "spinta" su un pacchetto IP).
- Le informazioni sull'elaborazione degli ACL sono integrate nel FIB dell'hardware e possono influire sulla scalabilità dei prefissi. L'esaurimento della memoria del prefisso viene segnalato da errori di allocazione della memoria con la firma "exmem=1" nel messaggio di log associato.

Raccomandazioni

- Le informazioni sull'elaborazione degli ACL sono integrate nella tabella di inoltro CEF, che riduce la scalabilità dei prefissi. Le applicazioni che non usano ACL possono disabilitare il supporto degli ACL nella tabella CEF e aumentare la memoria del prefisso disponibile usando il comando **no access-list hardware psa**.
- La configurazione del comando **no access-list hardware psa** disabilita tutte le elaborazioni ACL da parte delle schede del motore 2, oltre a disabilitare il supporto PSA per gli ACL. Non forza l'esecuzione software degli ACL. Questa condizione si applica anche se per la scheda di linea in uscita è configurato un ACL di output.
- La configurazione del comando **access-list compiled** dopo che il comando **access-list hardware psa** ha convertito le voci ACE che superano la capacità del PSA in un ACL turbo.

Ciò garantisce prestazioni ottimali per gli ACL di lunghezza superiore a 448 ACE.Il microcodice ACL predefinito è 128 (a partire dal software Cisco IOS versione 12.0(14)S/ST). Se si usano ACL di dimensioni inferiori e non è richiesta la funzionalità su 448 righe, la configurazione del comando **access-list hardware psa limit 128** consente di preservare la memoria di inoltro (TLU) e di migliorare la scalabilità del prefisso.L'elaborazione degli ACL turbo deve essere abilitata con il comando **access-list compiled** per gli ACL di lunghezza superiore a 129 righe insieme al comando **access-list hardware psa limit 128**. Questa combinazione elabora le prime 128 righe nell'ASIC PSA e le restanti righe con ACL turbo, ottimizzando le prestazioni e conservando la memoria di inoltro.

- La scheda di linea OC12 ATM a 4 porte non supporta ACL di input, ma fornisce il rilevamento degli ACL di output nel microcodice, che consente il processo degli ACL di output nel percorso lento.
- La scheda di linea OC3 ATM 8x supporta ACL di linea per-vc 128 con software Cisco IOS versione 12.0(23)S e successive. In un percorso rapido è possibile configurare un massimo di 16 ACL di input distinti. Gli ACL con 448 ingressi sono supportati per ogni VC solo su percorsi lenti. Gli ACL di output non sono supportati.

ISE (IP Services Engine) Engine 3 - Elaborazione ACL

Panoramica

Engine 3 è la prima scheda di linea di inoltro dual stage. Il motore 3 dispone di ASIC di inoltro/funzionalità sul percorso in entrata e in uscita. Ciò consente di inserire gli ACL nell'ASIC sui percorsi in entrata e in uscita. Inoltre, la struttura ASIC Engine 3 è una pipeline ibrida/array parallelo. La struttura ASIC implementa l'elaborazione ACL in TCAM (High-Speed Ternary Content Indirissable Memory) parallelo, che fornisce elaborazione della velocità di linea fino a 20.000 ACE per ingresso e 20.000 ACE per uscita.

Queste schede di linea sono basate sul motore 3:

Tipo di scheda di linea	Tipo di interfaccia	Connettività
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xCHOC12/STM4 ->OC3/STM1- >DS3/E3	POS	IR
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
8xOC3/STM1c	POS	IR
8xOC3c/STM1c	POS	MM
4 OC3c/STM1c	POS	IR
4 OC3c/STM1c	POS	MM
4 OC3c/STM1c	POS	LR
1xOC48c/STM16 c	POS	SR
1xOC48c/STM16	POS	LR

c		
1xCHOC48/STM16->STM4->OC3/STM1->DS3/E3	POS	SR
4xOC12c/STM4c	ATM/IP	IR
4xOC12c/STM4c	ATM/IP	MM
4xGE	GE	
4xOC12c/STM4c	DPT	IR
4xOC12c/STM4c	DPT	XLR

Criteri di corrispondenza supportati

Nel percorso rapido sono supportati tutti i criteri di corrispondenza standard ed estesa del software Cisco IOS versione 12.0S, ad eccezione degli ACE dei log elaborati dalla CPU della scheda di linea.

Numero di ACE supportati

- Elaborazione della velocità della linea in entrata e in uscita per porta, per VLAN, per sottointerfaccia Frame Relay e per sottointerfaccia ATM. Sono supportati fino a 20.000 ACE estesi per direzione e per scheda.
- I criteri di corrispondenza per le porte di origine/destinazione TCP/UDP "range", "lt" e "gt" vengono tutti gestiti nell'hardware utilizzando le risorse "L4 operator".
- Il numero di operandi L4 distinti è limitato a 32 per l'intera scheda di linea. Gli operatori delle porte di origine sono limitati a un massimo di sei.

Elaborazione ACL di output

Supporto del percorso rapido nativo per l'elaborazione degli ACL di output con velocità di linea nell'ASIC di elaborazione dei pacchetti sul percorso di trasmissione. Per ulteriori informazioni, vedere la matrice di interoperabilità tra schede di linea e ACL di output IPv4.

Comandi specifici della scheda di linea

- **hw-module <*slot #*> tcam compilazione senza unione*!—12.0(21)S3***
- **show-access-list hardware interface <*nome interfaccia*>**
- **show cef int pos[*x/y*] | inc if_number**

Linee guida operative e interazioni con le schede di linea

- Le voci di controllo di accesso corrispondenti ai pacchetti vengono elaborate nel percorso lento.
- I pacchetti corrispondenti agli ACE di negazione (limitati per evitare l'interruzione del sistema) vengono elaborati nel percorso lento.
- Quando un ACL include un intervallo di indirizzi, l'hardware utilizza le ACE speciali denominate "ACE dell'intervallo" che richiedono fino a tre ACE.

- L'unione degli ACL consente di risparmiare le risorse TCAM condividendo gli ACE comuni tra i singoli ACL. Per determinare se un ACL è stato unito, usare il comando **show-access-list hardware interface**.
- I contatori ACL non sono supportati per gli ACL uniti. Con il software Cisco IOS versione 12.0(21)S3 e successive, l'unione degli ACL può essere disabilitata con il comando **no-merge tcam-module <slot #>**. Per determinare se un ACL è stato unito, usare il comando **show-access-list dell'interfaccia hardware**.
- Se NetFlow è configurato su una scheda di linea Engine 0/1 e un ACL di output è configurato su una scheda di linea Engine 3 o 4+, l'ACL di output verrà elaborato sia dalle schede di linea in entrata che da quelle in uscita in modo da consentire a NetFlow di registrare i pacchetti rifiutati dagli ACL e i pacchetti inoltrati.

Supporto contatore ACL

	Per-ACE	Per-ACE (hardware counters)	Aggregate
21S3/ST3		X	
22S		X	X
23S	X	X	X

Definizioni:

- Per-ACE: per il normale supporto del software Cisco IOS, il comando **show access-list<*number*>** sull'RP/LC visualizza l'ACL e il contatore associati a ciascuna ACE. È disponibile solo quando l'**unione** è disabilitata prima di configurare gli ACL. A tale scopo, è possibile utilizzare il seguente comando di configurazione:
  `Router(config)#hw-module slot <number> tcam compile acl no-merge`

  Questa opzione, se attivata, disattiva alcune ottimizzazioni di unione TCAM e influisce sulla scalabilità. L'effetto esatto dipende dai singoli ACL.Si noti inoltre che i contatori non saranno corretti se all'interfaccia viene applicato il routing basato su criteri. In tal caso, utilizzare un contatore aggregato.
- Per-ACE (TCAM): contatori hardware associati a ciascuna voce TCAM. Non è necessaria alcuna configurazione e non vi è alcun impatto sulle prestazioni e sulla scalabilità. Disponibile solo sulla scheda di linea che utilizza questa CLI. Questi contatori non possono essere cancellati dal software.
  `LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace`

  Una nuova CLI generica per questo comando sarà disponibile nel software Cisco IOS versione 22S:
  `LC-Slot4#show access-list hardware interface p0:1 in`

  Come con il contatore per-ACE, i contatori TCAM sono validi solo quando PBR non è usato su quell'interfaccia con ACL.
- Aggrega: ogni ACL mostra un contatore di riepilogo di autorizzazioni/rifiuti. Somma di tutti i singoli contatori ACE. Non è necessaria alcuna configurazione e non vi è alcun impatto sulle prestazioni o sulla scalabilità.

Raccomandazioni

Nessuno in questo momento.

Engine 4 (POS) - Elaborazione ACL

Panoramica

Il motore 4 supporta questo ACL con il software Cisco IOS versione 12.0(18)S e successive:

- Gli ACL di uscita sono supportati sulle schede di linea E0/1/2 se una scheda di linea Engine 4 è la scheda in entrata. In questa configurazione, l'ACL di output viene elaborato dalla CPU della scheda di linea in uscita.

Queste schede di linea sono basate sul motore 4:

Tipo di scheda di linea	Tipo di interfaccia	Tipo di motore	Connettività
4x OC48c/STM 16c	POS	E4	
4x OC48c/STM 16c	POS	E4	LR
1xOC192c/STM64c	POS	E4	IR
1xOC192c/STM64c	POS	E4	SR
1xOC192c/STM64c	POS	E4	VSR-1
10xGE	SFP	E4	

Engine 4+ (POS e DPT) - Elaborazione ACL

Panoramica

Engine 4+ introduce la funzionalità ACL nella linea di prodotti Cisco serie 12000 da 10 Gigabit.

In ciascuno dei percorsi in entrata e in uscita sono supportate fino a 1024 ACE. Gli ACL di input e output vengono elaborati alla velocità di linea per un massimo di 96 ACE. Le prestazioni per le corrispondenze più lunghe variano in base alla profondità della corrispondenza.

Queste schede di linea POS sono basate su Engine 4+:

Tipo di scheda di linea	Tipo di interfaccia	Connettività
4x OC48c/STM16c	POS	SR
4x OC48c/STM16c	POS	LR

1xOC192c/STM64c	POS	IR
1xOC192c/STM64c	POS	SR
1xOC192c/STM64c	POS	VSR-1
1xOC192/STM64c	POS	LR
4x OC48c/STM16c	DPT	SFP:
1xOC192c/STM64c	DPT	IR
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1
1xOC192c/STM64c	DPT	LR

Criteri di corrispondenza supportati

Tutti i criteri ACL standard ed estesi supportati dal software Cisco IOS versione 12.0S sono supportati nel percorso rapido, ad eccezione delle voci di controllo di accesso di log o frammenti.

Numero di ACE supportati

Nel percorso rapido sono supportate fino a 1024 ACE per direzione.

Nota: è possibile configurare 1021 ACE. Tre voci sono riservate per i comandi ACE: **allow ip any any** implicito, **deny ip any any** e **send to CPU**.

Non esiste un limite massimo per il numero di ACE supportate. Qualsiasi ACE oltre il limite di 1021 viene eseguito nel percorso lento della scheda di linea.

Elaborazione ACL di output

Gli ACL di output vengono elaborati nel percorso rapido del lato trasmissione. Per ulteriori informazioni, vedere la matrice di interoperabilità tra schede di linea e ACL di output IPv4.

Comandi specifici della scheda di linea

- **show tcam appl [*acl-in | acl-out*] tcam <*label-no*>**
- **show tcam appl [*acl-in | acl-out*] memoria <*porta*> <*numero di voci*>**

Linee guida operative e interazioni con le schede di linea

- ACL di sottointerfaccia non supportati.

- Le prestazioni variano a seconda della profondità della corrispondenza.
- Le voci di intervallo utilizzano due regole ACL (tre se le due voci attraversano un limite).
- Èsupportato un ACL per interfaccia fisica.
- Nel percorso rapido sono supportate fino a 1024 ACE (per direzione).
- Èpossibile condividere tra le porte qualsiasi ACE con percorso rapido 1024.
- Le voci ACE che utilizzano la parola chiave fragment vengono filtrate nel percorso lento.
- I pacchetti negati non vengono conteggiati per le voci ACE in fase di elaborazione nel percorso lento.
- Se NetFlow è configurato su una scheda di linea Engine 0 e un ACL di output è configurato su una scheda di linea Engine 3 o 4+, l'ACL di output verrà elaborato sia dalle schede di linea in entrata che da quelle in uscita per consentire a NetFlow di registrare i pacchetti rifiutati dagli ACL e i pacchetti inoltrati.

Raccomandazioni

Nessuno in questo momento.

Engine 4+ (Ethernet) - Elaborazione ACL

Panoramica

Le schede di linea Engine 4+ Ethernet introducono la funzionalità ACL di input per vlan nell'hardware alla linea di prodotti Cisco 12000 10-Gigabit Ethernet. Queste sono alcune delle caratteristiche:

- Gli ACL di input e output possono essere applicati contemporaneamente su una singola porta senza alcun impatto sulle prestazioni.
- Èpossibile applicare gli ACL a ciascuna VLAN o a ciascuna porta.
- Le prestazioni degli ACL di input fino a 15.000 ACE non diminuiscono con la profondità della corrispondenza.
- Gli ACL di output vengono elaborati alla velocità di linea per un massimo di 96 ACE. Le prestazioni per le corrispondenze più lunghe variano in base alla profondità della corrispondenza.

Le schede di linea Ethernet si basano sul motore 4+:

Tipo di scheda di linea	Tipo di interfaccia	Tipo di motore
10xGE Rev B ("X-B")	SFP:	E4+
Modulare	SFP:	E4+
1x10GE	10 G	E4+
1x10GE	10 G	E4+

Criteri di corrispondenza supportati

Tutti i criteri ACL standard ed estesi supportati dal software Cisco IOS versione 12.0S sono supportati nel percorso rapido, ad eccezione delle voci di controllo di accesso di log o frammenti.

Numero di ACE supportati

- Fino a 15.000 ACL di input che possono essere configurati per porta o per VLAN.
- 1024 ACE di uscita per scheda, che possono essere applicati su base per porta.**Nota:** è possibile configurare 1021 ACE. Tre voci sono riservate per i comandi ACE: **allow ip any any** implicito, **deny ip any any** e **send to CPU**.

Elaborazione ACL di output

Gli ACL di output vengono elaborati in modo nativo nel percorso rapido del lato trasmissione. Per ulteriori informazioni, vedere la matrice di interoperabilità tra schede di linea e ACL di output IPv4.

Comandi specifici della scheda di linea

- **unione acl ip <*number*> dello slot hw-module**

Linee guida operative e interazioni con le schede di linea

- Le voci ACE contenenti la parola chiave fragment vengono elaborate nel percorso lento.
- I contatori ACL non sono supportati per gli ACL combinati con altre funzionalità.
- I contatori ACL non sono supportati per gli ACL uniti. Gli ACL uniti sono configurabili con il comando **hw-module slot <*slot number*> ip acl merge**.
- Sono supportate fino a 168 operazioni L4 per scheda di linea. Una volta superato questo valore, l'ACL viene eseguito nel percorso lento.
- Se una scheda di linea del motore 1 ha abilitato il campionamento di NetFlow e un ACL di output è abilitato su una scheda di linea del motore 3 o 4+, l'ACL di output viene elaborato sia dalle schede di linea in entrata che da quelle in uscita in modo da consentire a NetFlow di registrare i pacchetti rifiutati dagli ACL e i pacchetti inoltrati.

Raccomandazioni

Nessuno in questo momento.

Registrazione ACL

Prima della versione 12.0(21)S del software Cisco IOS, le informazioni di registrazione degli ACL venivano inviate al punto di ripristino esclusivamente tramite il bus di manutenzione (MBUS). Durante gli alti livelli di attività di registrazione degli ACL, era possibile superare la capacità dell'MBUS. Il software Cisco IOS versione 12.0(21)S introduce diverse ottimizzazioni che impediscono questo scenario.

Le situazioni di sovraccarico MBUS vengono segnalate dal software Cisco IOS con questi messaggi di errore:

```
LCLOG-3-INVSTATE

MBUS_SYS-3-SEQUENCE
```

Con il software Cisco IOS versione 12.0(21)S e successive, i messaggi di log con livelli di gravità elevati (gravità da 0 a 4) vengono recapitati all'RP tramite l'MBUS, mentre i messaggi di log con livelli di gravità inferiori (gravità da 5 a 7) vengono recapitati all'RP tramite il fabric di switching con capacità superiore. Poiché i messaggi di log ACL hanno un livello di gravità elevato, vengono ora recapitati all'RP tramite il fabric di switching.

Questa funzionalità di registrazione aggiunta è configurabile utilizzando i seguenti comandi:

- **logging method mbus [*severity*]**: determina quali messaggi, per gravità, verranno inviati all'RP utilizzando l'MBUS. I messaggi con livelli di gravità più elevati verranno inviati tramite la struttura dello switch.
- **show logging method**: visualizza il metodo di log corrente per tutti i livelli di gravità dei messaggi.
- **logging sequence-number** - Questo comando consente alla scheda della linea di invio di sequenziare i messaggi di log in modo che possano essere riordinati correttamente dall'RP. Senza questo comando, i messaggi di log possono essere recapitati all'RP in ordine non sequenziale.

ACL IPv4 Output - Matrice di interoperabilità scheda di linea

Prima dell'introduzione dell'elaborazione degli ACL in uscita con la versione del motore 3 e 4+, gli ACL in uscita venivano elaborati dalla scheda di linea in entrata. Gli ACL di output sono stati aggiornati per sfruttare le funzionalità di elaborazione degli ACL di output Engine 3 e Engine 4+ ad alte prestazioni.

Questo grafico mostra la posizione in cui gli ACL di output vengono elaborati per diverse combinazioni di schede di linea:

	Scheda linea in uscita					
Scheda di linea in ingresso (ACL di uscita applicato all'interfaccia del membro)	**E0**	**E1**	**E2**	**E3**	**E4**	**E4+**
E0	In ingresso	In ingresso	In ingresso	In uscita	n/d	In uscita
E1	In ingresso	In ingresso	In ingresso	In uscita	n/d	In uscita
E2	In ingresso	In ingresso	In ingresso	In uscita	n/d	In uscita
E3	In uscita	In uscita	In uscita	In uscita	n/d	In uscita

E4	In uscita	In uscita	In uscita	In uscita	n/d	In uscita
E4+	In uscita	In uscita	In uscita	In uscita	n/d	In uscita

Supporto ACL IPv6

Gli ACL estesi IPv6 sono supportati nel percorso lento (in entrata e in uscita) sui protocolli E0, E1, E2, E3 e E4+ nel software Cisco IOS versione 12.0(23)S.

Nel motore 3, la funzionalità ACL IPv6 è supportata sull'hardware nel software Cisco IOS versione 12.0(25)S. Gli ACL vengono applicati a un'interfaccia specifica, con un'istruzione di rifiuto implicita alla fine di ciascun elenco degli accessi. Gli ACL IPv6 vengono configurati utilizzando il comando **ipv6 access-list** con le parole chiave deny e allow nella modalità di configurazione globale. Le schede basate sul motore 3 supportano il filtro delle intestazioni delle opzioni IPv6 basate sul traffico, le etichette di flusso e, facoltativamente, informazioni sul tipo di protocollo di livello superiore.

Guida di riferimento ai comandi di Cisco 12000 ACL

Comandi Engine 1

- **access-list salsa hardware**
- **show controller l3 | includere ASIC**

Comandi Engine 2

- **access-list limite psa hardware 128**
- **psa hardware access-list non disponibile**
- **bypass psa**
- **mostra dettagli psa access-list**
- **mostra riepilogo psa access-list**
- **funzione show controller psa**

Comandi Engine 3

- **hw-module <*slot #*> tcam compilazione senza unione***!— a partire dal software Cisco IOS versione 12.0(21)S3***
- **show-access-list hardware interface <*nome interfaccia*>**
- **show contr [*tofab|frfab*] alfa acl <*int*> vmr2ace**

Comandi Engine 4+

- **etichetta show access-list gen7**
- **show tcam appl [*acl-in | acl-out*] tcam <*label-no*>**
- **show tcam appl [*acl-in | acl-out*] memoria <*porta*><*numero di voci*>**

Comandi Ethernet Engine 4+

- **unione acl ip <*number*> dello slot hw-module**

Glossario

In questa sezione vengono fornite definizioni standard dei termini rilevanti:

- **Piani di elaborazione (Planes of Processing**) - Un dispositivo di rete può essere diviso logicamente in tre piani di elaborazione:Piano dati (Data Plane) - Elaborazione dei pacchetti che passano attraverso il dispositivo di rete.Piano di controllo (Control Plane) - Elaborazione sui pacchetti utilizzati per associare i dispositivi di rete. Sono inclusi i protocolli di linea (ad esempio Point-to-Point Protocol - PPP e High-Level Data Link Control - HDLC), i protocolli di routing (Border Gateway Protocol - BGP, Routing Information Protocol versione 2 - RIPv2, Open Shortest Path First - OSPF e così via) e i protocolli di temporizzazione (ad esempio Network Time Protocol - NTP).Piano di gestione: elaborazione su pacchetti utilizzati per gestire i dispositivi di rete. tra cui telnet, Secure Shell (SSH), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), SNMP e altri protocolli di gestione.
- **ACL standard**: gli ACL standard filtrano solo sul layer 3.
- **ACL estesi**: gli elenchi degli accessi IP estesi utilizzano gli indirizzi di origine e di destinazione per le operazioni di corrispondenza, nonché informazioni facoltative sul tipo di protocollo per una maggiore granularità del controllo.
- **ACL lineari elaborati** - Elaborati linearmente nel software. Le prestazioni variano in base alla profondità della corrispondenza (il numero di voci da controllare prima di determinare una corrispondenza).
- **ACL turbo (compilati)**: gli ACL turbo ottimizzano l'elaborazione degli ACL software compilando un ACL in una serie di tabelle di ricerca altamente ottimizzate in grado di velocizzare l'elaborazione del software. Le prestazioni degli ACL turbo non variano a seconda della profondità della corrispondenza.
- **ACL di input**: ACL applicato al traffico in entrata sulla porta a cui è applicato.
- **ACL di output**: un ACL applicato al traffico in uscita dalla porta a cui è applicato. Con alcune eccezioni, gli ACL di output vengono elaborati dalla scheda della linea di input.
- **Receive Path ACL**: gli ACL di ricezione del percorso forniscono il filtro per il traffico di controllo destinato al router stesso, ad esempio gli aggiornamenti di routing e le query SNMP.
- **Scheda di linea di inoltro dual stage**: schede di linea con ASIC di inoltro/funzionalità sia sul percorso in entrata che in uscita. Ciò consente alla scheda di linea di eseguire le funzioni sia sul flusso del pacchetto in entrata che su quello in uscita senza puntare i pacchetti alla CPU LC. Consente inoltre di utilizzare nuove ondate di algoritmi di inoltro a doppio stadio in Cisco 12000. La scheda di linea Engine 3 è un esempio di scheda di linea di inoltro a doppio stadio.
- **Scheda di linea di inoltro a stadio singolo**: schede di linea che dispongono di ASIC di inoltro/funzionalità solo sul percorso in entrata. Queste schede di linea eseguono solo l'elaborazione basata su ASIC sui pacchetti in entrata nel percorso. Il traffico in uscita non viene elaborato (solo inoltrato), gestito dagli ASIC in entrata di altri LC o gestito dalla CPU LC. Engine 2, Engine 4 e Engine 4+ sono esempi di schede di linea di inoltro a stadio singolo.

Informazioni correlate

- Cisco serie 12000 Internet Router
- Documentazione e supporto tecnico – Cisco Systems