Cisco 12000 シリーズインターネットルータのアクセス・リストの実装

目次

概要

この文書では、Cisco 12000 シリーズ インターネット ルータでの Access Control List (ACL; アクセス コントロール リスト) のサポートについて説明しています。

前提条件

要件

Cisco は ACL が Ciscoルータでどのようにの動作するか基本のナレッジがあることを推奨します。

ACL およびアプリケーションの概要に関してはこれらの文書を参照して下さい:

- アクセス・コントロール・リスト: 外観およびガイドライン
- IP サービスの設定: フィルタ IP パケット

使用するコンポーネント

この文書に記載されている情報は基づいた on Cisco 12000 シリーズ インターネット ルータです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Cisco 12000 シリーズ インターネットルータのACL サポートの概要

Cisco 12000 シリーズ インターネット ルータで、ACL はハードウェア（特定用途向け集積回路-ASIC）、ソフトウェア（ラインカードの CPU 処理される）で、またはハイブリッド機能として–処理することができますハードウェア アシストのソフトウェアで。 ACL がハードウェアまたはソフトウェアのどちらで処理されるかは、ACL アプリケーション、ラインカード エンジンのタイプ、および他のラインカードにおける ACL からのインタラクションによって異なります。

Cisco 12000 シリーズのラインカード エンジンには、さまざまな ACL 機能が用意されています。 特定のラインカード エンジンの ACL サポート情報に関しては、この資料の対応した セクションに行って下さい。

注: IP Multicast ACL は Cisco IOS® ソフトウェア リリース 12.0S でサポートされません。 IP マルチキャスト境界機能は、マルチキャスト フィルタリングが必要な場合に使用できます。 詳細についてはファスト パス マルチキャスト転送 12000 シリーズ エンジン 2 および ISE ライン カードを on Cisco 参照して下さい。

ASIC ベースのACLかCPU ベースのACLか

Cisco 12000 では、あらゆる世代の ACL 処理がサポートされています。 これらの処理モードのそれぞれがどのようにの互いをはたらき、相互に作用し、サポートするか動作上の了解は Cisco 12000 の有効な ACL Use に必要です。

ACL処理の初期バージョンは ACL を処理するのにプログラマブル CPU を使用しました。 やがて、パケット/秒（PPS）処理の要件が、新しい CPU の能力を超えるようになりました。 ASIC はルータ フォワーディングおよび機能対応のためのより高い PPS レートを実現させるために構築されました。 Line Card （LC） CPU でロードされた ACL は LC ASIC にそれからロードされました。 ASIC はより高い PPS レートを処理するために即席に作られ続けました。 これらの第 二世代 ASIC は生成の開拓作業での前の構築され、より多くの ASIC 機能を提供します。 Cisco 12000 が分散ルーティング プラットフォームであるので、ACL処理のさまざまな生成間の相互対

話は操作上混合を作成できます。

発生するものが ACL処理と説明を助けるのにこの資料の全体にわたって ASICベースのACL、CPUベースACL、高速経路、遅いパスおよび ASIC パントのような用語が使用されています。 これらの用語の説明はここにあります:

- ASIC ベースの ACL （ 高速経路 ） — ACL は ASIC ハードウェアでロードされ、処理されます。 ASIC のパフォーマンス エンベロープにより、ACL の深さ、パフォーマンス、およびケイパビリティが決まります。 パスで高速経路が ASIC ベースの処理し、LC サポート CPU で実行される処理の違いを説明するのに使用されていました。 より多くの ASIC ベースの一般的な用語はこの資料で使用されます。
- CPU ベース ACL （ 遅いパス ） — ACL はラインカードCPU のソフトウェアで処理されます。 初期バージョン カードに関しては（１）エンジン 0 および場合によってはエンジンは LC CPU で、完全に処理してされます。 ASIC ベースの LC は ASIC からパントされるパケットの ACL処理を行います。 低速パスという用語は、以前は、LC の CPU へのパントが ASIC よりもどれだけ低速であるかを示すために使用されていました。 より多くの CPU ベース 一般的な用語はこの資料で使用されます。
- ASIC はパントします— ASIC に厳密な設計エンベロープがあります。 パケットが設計エンベロープを超えた場合、そのパケットは LC をサポートする CPU で処理されるように ASIC からパントされるか、または Route Processor（RP; ルート プロセッサ）に送信されます。 ASIC ベースの ACL は ASIC の設計の外部で落ちるパケットをパントします。 例はログまたは log-input キーワードの ACE がある ACL です。 パケットをログするために必要な情報は ASIC の外部で処理する必要があるため、このパケットは ASIC から LC の CPU に自動的にパントされ、通常の CPU ベースの ACL と同様に処理されます。

注: ACL を一致するためにマッチ ステートメントで Policy Based Routing（PBR）を設定するとき ACL は送信元ポートを一致するべきではありません。 ギガビット スイッチ ルータ（GSR）は送信元ポートを一致する ACL の PBR のためのハードウェア スイッチングをサポートしません。 それはプロセス スイッチングを引き起こし、GSR パフォーマンスは低下します。

コントロールプレーンおよび管理プレーンのフィルタリング

ルータ プロセッサは、Cisco 12000 シリーズの分散アーキテクチャで制御および管理プレーン サービスを提供します。 レシーブ パス ACL （rACL）は制御に簡単な分散フィルタリング送信される機能および RP にマネジメントトラフィックを提供します。 それは分散アーキテクチャの強さを利用するセキュリティの追加層として論理的に表示することができます。

IP 受信パスACLの設定

rACL は Cisco IOS® ソフトウェア リリース 12.0(21)S2 のメンテナンス スロットルに特別な放棄によって導入されました。 それは Cisco IOS software release 12.0(22)S で公式のサポートを提供されます。 詳細については IP Receive ACL 機能を参照して下さい。

ルータ プロセッサは、Cisco 12000 シリーズの分散アーキテクチャで制御プレーン サービスを提供します。 レシーブ ACL はルーティング更新および簡易ネットワーク管理プロトコル（SNMP）クエリのような RP に、向かうコントロール トラフィックにフィルタリング機能を提供します。

rACL はフェーズ 1 Planeトラフィックの制御および管理に新しい保護を追加するための多相努力の考慮されます。 新しいレートリミット機能拡張はソフトウェア アップデートを通して追加され

ています。

ラインカードタイプによるIPv4 ACL サポート

12000 シリーズのラインカードでは、エンジンのタイプごとに異なる ACL 機能を提供しています。 このセクションでは、各種ラインカード エンジンの ACL 機能について説明します。 特定のラインカード エンジンの ACL サポート情報に関しては、この資料の対応した セクションを参照して下さい。

すべての ACL (ASIC ベースおよび CPU ベース) に関して一般的な特性が、いくつかあります。

- インターフェイスに適用できる ACL は、各方向に対して 1 つだけです。 たとえば、interface pos 0/0 は 1 インプットACL および 1 出力 ACL だけある場合があります。
- ACL に対するパケットのテストは、一致が見つかると停止します。 長さ 300 のエントリである ACL がアクセス リストエントリ (ACE) のパケットと #45 一致する場合、パケットは処理され、ACL処理は停止します。
- すべての ACL の最後には暗黙的な deny all エントリが存在します。 その結果、ACL に一致がなければ、パケットはドロップされます。 Cisco ACL は*明示的な割り当て* ACL アーキテクチャで作成されます。 これは処理され、転送されるそれのためのパケットを一致する ACE がある必要があることを意味します。
- 新たに追加された ACE は ACL の終わりに常に追加 されます。 ACL をアップデートする必要があるたびに、ACL を削除して (no access-list コマンドを使用)、新しい ACL を追加し直すことをお勧めします。
- 非初期 IP フラグメントが IP ヘッダーでレイヤ4 プロトコル情報が含まれていないので、標準一致条件だけが先頭 以外 の フラグメントのためにサポートされます。 Cisco ACL が IP断片フィルタリングにどのようにの従うか詳細はおよび IP フラグメント アクセス コントロール リスト (ACL) 見つけることができます。
- 番号を付けられた ACL は Command Line Interface （ CLI) によって入るとすぐ処理され、適用されます。 大きい ACL を使うと、これは時々 RP または LC CPU の CPUスパイクという結果に終ります。

エンジン 0 - ACL 処理

エンジン 0 は Cisco 12000 のために渡される最初のラインカードです。 それはすべての CPU ベースの処理およびフォワーディングです。 それ故に、エンジンは 0 ラインカード LC CPU の ACL を処理します。

これらのラインカードはエンジン 0 に基づいています:

ラインカード型	インターフェイス タイプ	接続
12 x DS3	同軸	SMB
12 x DS3	同軸	SMB
12 x E3	同軸	SMB
1xCHOC12->DS3		IR
1xCHOC12/STM4 ->OC3/STM1	POS	IR
4xOC3c/STM1c	POS	SR

4xOC3c/STM1c	POS	LR
4xOC3c/STM1c	POS	MM
1xOC12c/STM4c	POS	IR
1xOC12c/STM4c	POS	MM
6xCT3->DS1		SMB
2xCHOC3/STM1->DS1/E1		IR
4xOC3c/STM1c	ATM	IR
4xOC3c/STM1c	ATM	MM
1xOC12c/STM4c	ATM	IR
1xOC12c/STM4c	ATM	MM

サポートされている一致基準

すべての Cisco IOS ソフトウェア リリース 12.0S 規格、拡張 ACL およびターボ ACL はエンジン 0 でサポートされます。

サポートされる ACE の数

ACL サイズは性能要件および利用可能なメモリ メモリ・リソースによってだけ制限されます。

出力 ACL 処理

出力 ACL は、システム内の他のラインカードの入力機能パスで処理されます。 他の LC の入力側への出力 ACL のプッシュは廃棄される筈であるフォワーディング パケットからバックプレーンを保護します。 これは、Cisco 7500 の分散アーキテクチャから継承されている機能です。 詳細な説明、原因および操作上ガイドラインは IPv4 出力 ACL で-ラインカード 相互運用 マトリックス提供されます。

ラインカード仕様コマンド

ありません。

操作に関するガイドラインとラインカード インタラクション

- NetFlow がエンジンで 0 ラインカード設定され、出力 ACL が出力 エンジン 3 か 4+ でラインカード設定されれば NetFlow が ACL、また転送されたパケットによって拒否されるパケットを説明するように、出力 ACL は入力および出力 ラインカード両方によって処理されます。

推奨事項

Cisco は大きい ACL のためのエンジン 0 のターボ ACL の使用を推奨します。 ターボ ACL では追加のメモリが必要となるため、小さな ACL には小さなリニア ACL を使用する方が効率的です。

エンジン 1 - ACL 処理

概要

エンジンは 1 つのラインカード エンジン 0 の CPU ベースの処理とソフトウェアのエンジン 2.エンジン 1 ラインカード プロセス ACL の第一世代 フォワーディング/機能 ASIC 間のデフォルトでブリッジです。 Cisco IOS ソフトウェア リリース 12.0(10)S およびそれ以降によって、サルサのどのバージョンにによって判別するために下記のラインカード コマンドレファレンスを特定のカードが装備されているか) エンジン 1 はサルサ ASIC のバージョン 4 または 5 によって装備されているカードにハードウェア ACL を提供します (参照して下さい。

これらのラインカードはエンジン 1 に基づいています:

ラインカード型	インターフェイス タイプ	接続
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
1xGE	SX,	GBIC :
1xGE	SX,	GBIC :
2xOC12c/STM4c	DPT	IR
2xOC12c/STM4c	DPT	LR
2xOC12c/STM4 c	DPT	XLR
2xOC12c/STM4c	DPT	MM
2xOC12c/STM4c	DPT	IR
2xOC12c/STM4c	DPT	LR
2cOC12c/STM4c	DPT	XLR
2xOC12c/STM4c	DPT	MM

サポートされている一致基準

すべての Cisco IOS ソフトウェア リリース 12.0S は標準を、拡張サポートし、ターボ ACL は LC CPU (遅いパス) でサポートされます。 さらに、エンジン 1 はサルサ ASIC のプロセス入力 ACL できます。 従来のリニア ACL処理および Turbo ACL 処理と比較されたときサルサ ASIC はパフォーマンスの向上に終ってルート ルックアップと共に、処理するインプットACL を処理します。 サルサ ASIC はプロセス 出力 ACL かサブインターフェイス ACL できません。

サポートされる ACE の数

ACL サイズは性能要件および利用可能なメモリ メモリ・ リソースによってだけ制限されます。

出力 ACL 処理

出力 ACL は、システム内の他のラインカードの入力機能パスで処理されます。 参照して下さい IPv4 出力 ACL -詳細についてはラインカード 相互運用 マトリックス セクション。

ラインカード仕様コマンド

- access-list hardware salsa
- show controller l3 | ASIC を含んで下さい

操作に関するガイドラインとラインカード インタラクション

- Salsa ASIC と PSA ASIC を同時に稼動させることはできません。 access-list hardware コマンドは、PSA（Engine 2）または Salsa（Engine 1）のいずれかを受け入れますが、両方は受け入れません。
- NetFlow がエンジンで 1 つのラインカード設定され、出力 ACL が出力 エンジン 3 か 4+ でラインカード設定されれば NetFlow が ACL、また転送されたパケットによって拒否されるパケットを説明するように、出力 ACL は入力および出力 ラインカード両方によって処理されます。

推奨事項

ハードウェア ACL をサポートしないエンジン 1 ラインカードのバージョンに関しては、Cisco は大きい ACL のためのターボ ACL の使用を推奨します。 小さな ACL（20 行未満）は、メモリを節約するために、リニア ACL として実装できます。

エンジン 2 - ACL 処理

概要

Engine 2 は、転送/機能 ASIC が備わった最初のラインカードでした。 Cisco IOS ソフトウェア リリース 12.0(10)S およびそれ以降によって、エンジン 2 ラインカードは高性能 Packet Switching ASIC （PSA）のハードウェア ACL 機能を提供します。 すべてのフォワーディング/機能 ASIC と同様に、厳密なパフォーマンス エンベロープは ASIC の機能に境界を置きます。 Engine 2 ACL のキー パフォーマンス エンベロープは、PSA ASIC のメモリ制限によるものです。

エンジン 2 のパケット転送は PSA ASIC によって行われます。 PSA に 3 つの主外部メモリがあります:

- PLU（パス ルックアップ）— mtrie ノードを保存するのに使用しました
- TLU（テーブル 索引）— FIB リーフおよび可能性のある loadbalance 構造を保存するのに使用しました。 また PSA ACL データ構造の多数を保持するのに使用しました
- SRAM — プライマリ 位置はのための構造を負荷分担します

PSA ACL機能は ACL チェックのマイクロコード ベースの実装です。 特派員一組の手順は PSA 半導体素子にロードされます基本 ACL チェックのために可能にする。 展開する前に注意深く理解するはずであるこの機能へいくつかの制限があります。 PSA ACL への 1 つの主な欠点が必要な多量のハードウェア転送 メモリです。

PSA ACL機能は PLU/TLU メモリの大きいブロックがプレフィックス、先祖などの数に関係なく事前割当てされるように要求します このアロケーションは TLU エリアから主に来るので、PSA ACL が設定されるときこれらのカードで維持することができるルーティングの数の重大な影響があります。

PLU/TLU メモリの最初の経費に加えて、TLU メモリで保存される各プレフィクスはかなり多くのメモリを必要とします。 各プレフィクスのための必要なメモリの量は適用される ACL （入力 vs

出力）およびラインカード型の方向に基づいて、変わります。 一般に、出力 ACL は入力よりそれ以上のメモリを必要とし、より多くの物理ポートが付いているラインカードは少数のポートとそれらそのそれ以上のメモリを必要とします。

エンジン 2 ラインカードが ACL を使用しないケースでは、ACL のためのデータ構造は設定される実際の ACL に関係なく構築されます。 より小さい非 ACL 構造に変更するために、ルータの **no access-list hardware psa を**設定して下さい。 このコマンドはすべての方向のすべての Engine2 ラインカードのすべての ACL処理をディセーブルにします。 それらを注意深く使用する Cisco recommeds。

概要

一致深度の依存しないの ACL処理 パフォーマンスを提供するために、エンジン 2 ACL はハードウェア転送 表に統合されています。 これがプレフィックスのスケーラビリティに与える影響については、次の説明を参照してください。

これらのラインカードはエンジン 2 に基づいています:

ラインカード型	インターフェイスタイプ	接続
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC192c/STM64c	イネーブラー	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/STM16	DPT	SR

c		
1xOC48c/STM16c	DPT	LR

サポートされている一致基準

すべての Cisco IOS ソフトウェア リリース 12.0S はレイヤ4 送信元ポートを除く規格および拡張 ACL マッチ基準、サポートしました。 不連続マスク、IP 優先順位フィールドおよびレイヤ4 送信元ポートは PSA ASIC からパントされ、LC CPU で処理されます。

サポートされる ACE の数

PSA で最大 5 個の 448 行の入力 ACL。 1 ACL はポートごとに設定することができます。 追加 ACL はラインカードCPU によって管理されます。 出力 ACL の制限用に「制限」下記の例を参照して下さい。

出力 ACL 処理

このラインカードで設定された出力 ACL はシステムの他のラインカードの入力 機能 パスで実行された。 参照して下さい IPv4 出力 ACL -詳細についてはラインカード 相互運用 マトリックス。

ラインカード仕様コマンド

- **access-list hardware psa limit 128**
- **no access-list hardware psa**
- **psa bypass**
- **show access-list psa detail**
- **show access-list psa summary**
- **show controller psa feature**

操作に関するガイドラインとラインカード インタラクション

- 高速経路 ACL処理はこれらの条件が満たされるように要求します:適用される ACL は、128 または 448 ACE の制限内である。長さは **access-list ハードウェア psa 制限 128** コマンドが設定される場合 128 ACE より小さい必要があります。448 行の ACL マイクロコード バンドルが必要な場合、長さは 448 ACE 分未満である必要がある。入出力 ACL はカードごとに同時に設定されません。ルータ上で出力 ACL を最大で 5 つ設定できる。
- 8 ポートおよび 16 ポートの OC-3/STM-1 POS ラインカードでサポートされているのは、128 行の ACL だけです。 448 行の ACL は、4 ポートの OC-12/STM-4 POS、1 ポートの OC-48/STM-16 POS、および 3 ポートのギガビット イーサネットの各ラインカードでサポートされています。
- 両方とも同じカードで同時に設定されるとき入力 ACL は出力 ACL 上の高速経路の優先順位を奪取 します（出力 ACL は遅いパスで処理されます）。
- 出力 ACL がエンジン 2 カードで設定され、入力 ラインカードがエンジン 0/1/2/4 なら場合、出力 ACL は入力カードで処理されます。 他のエンジンタイプに関しては、出力 ACL はエンジン 2 出力遅いパスで処理されます。
- 出力 ACL は IP に MPLS トラフィックのためにサポートされません（IPパケットに」押され

る最初 MPLS ラベル「 ）。
- ACL処理 情報はハードウェア FIB に統合されて、プレフィクス スケーラビリティに影響を与えることができます。 プレフィクス メモリ枯渇は伴うログメッセージの「exmem=1」シグニチャを持つメモリアロケーション障害によって報告されます。

推奨事項

- ACL処理 情報はプレフィクス スケーラビリティを減らす CEF フォワーディングテーブルに統合されています。 ACL を使用しないアプリケーションはそれにより CEF 表の ACL サポートをディセーブルにし、**no access-list hardware psa コマンドの**発行によって利用可能 な プレフィクス メモリを増加できます。
- **no access-list hardware psa コマンド**の設定は ACL のための PSA サポートをディセーブルにすることに加えてエンジン 2 カードによってすべての ACL処理をディセーブルにします。それは ACL のソフトウェア実行を強制しません。 出力ラインカードで出力 ACL が設定されている場合にも、この条件があてはまります。
- **access-list ハードウェア psa** コマンドが Turbo ACL に PSA のキャパシティを超過する ACE を変換した後 **access-list compiled コマンド**の設定。 最適な ACL パフォーマンスが得られます。デフォルトの ACL マイクロコードは 128 です（Cisco IOS ソフトウェア リリース 12.0(14)S/ST 以降 ）。 より小さい ACL が使用中であり、448-line 機能が必要とならなかったら、プレフィクス スケーラビリティを改善する ） **access-list ハードウェア psa を**設定する **128** コマンドを節約しますフォワーディング（TLU ）メモリを**制限して下さい**。Turbo ACL 処理は **access-list ハードウェア psa 限界 128** コマンドと共に ACL のための **access-list compiled コマンド**でより 129 ライン長く有効に する必要があります。 この組み合せは PSA ASIC の最初の 128 の行および節約している間パフォーマンスを最適化するターボ ACL が付いている残りの行を処理しま、メモリを転送します。
- 4 ポート OC12 ATMラインカードは入力 ACL をサポートしませんが、遅いパスの出力 ACL のプロセスを可能にするマイクロコードの出力 ACL 検出を提供します。
- 8xOC3 ATMラインカードは VC 単位の Cisco IOS ソフトウェア リリース 12.0(23)S およびそれ以降のサポートします 128 ライン ACL を。 最大 16 個別の入力 ACL は高速経路で設定することができます。 448 入力 ACL は、低速パスだけで VC 単位でサポートされています。出力 ACL はサポートされていません。

ISE (IPサービス エンジン) エンジン3 - ACL 処理

概要

Engine 3 は、最初のデュアル ステージ転送ラインカードです。 Engine 3 では、入力と出力パスに転送/機能 ASIC が備わっています。 これにより、入力パスと出力パスの両方で ASIC に ACL を配置できます。 さらに、エンジン 3 ASIC 構造はハイブリッド パイプライン/並列アレイです。ASIC 構造は出力ごとの ACL処理高速 Ternary Content Addressable Memory （ TCAM ） 入力ごとの 20K ACE までの回線レート処理を提供する、および 20K ACE を並行して設定します。

これらのラインカードはエンジン 3 に基づいています:

ラインカード型	インターフェイス タイプ	接続
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
4xOC3c/STM1c	POS	IR
4xOC3c/STM1c	POS	MM
4xOC3c/STM1c	POS	LR
1xOC48c/STM16 c	POS	SR
1xOC48c/STM16 c	POS	LR
1xCHOC48/STM1 6->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

サポートされている一致基準

ラインカードCPU によって処理されるすべての Cisco IOS ソフトウェア リリース 12.0S 標準および拡張マッチ基準は口グ ACE を除いて高速経路でサポートされます。

サポートされる ACE の数

- ポートごとの入力および出方向両方で、VLAN ごとに、フレーム リレー サブインターフェイスごとに、および ATM サブインターフェイスごとに処理する行比率。 各方向および各カードにつき最大 20,000 の拡張 ACE がサポートされています。
- TCP/UDP 出典/宛先ポートのための一致条件は「範囲」、「Lt」、および「gt L4 オペレータ」リソース」を使用して「ハードウェアで処理されるすべてです。
- 個別の L4 オペランドの数は、ラインカード全体で 32 に制限されています。 送信元ポートのオペレータは、最大 6 に制限されています。

出力 ACL 処理

ASIC を処理する送信するパス パケットで処理する回線レート 出力 ACL のためのネイティブ ファスト パス サポート。 参照して下さい IPv4 出力 ACL -詳細については[ラインカード 相互運用マトリックス]。

ラインカード仕様コマンド

- **hw-module <slot #> tcam は非マージをコンパイルします**!! ---12.0(21)S3
- **show-access-list ハードウェアインターフェイス <interface** *名前* **>**
- **示して下さい cef int pos [***x/y***] | 株式会社 if_number**

操作に関するガイドラインとラインカード インタラクション

- 口ギング ACE に照合するパケットは、低速パスで処理されます。
- 拒否 ACE に照合するパケット（システムが中断しないように制限されています）は、低速パスで処理されます。
- ACL がアドレス範囲が含まれている時、ハードウェア使用特別な 3 まで ACE を必要とする ACE によって呼出される「範囲 ACE」。
- ACLマージはユーザー ACL を渡るよくある ACE の共有によって TCAM リソースを節約できます。 ACL がマージされているかどうかを判別するには、show-access-list hardware interface コマンドを使用します。
- ACL カウンターはマージされた ACL のためにサポートされません。 Cisco IOS ソフトウェア リリース 12.0(21)S3 およびそれ以降を使うと、ACLマージは **hw-module <slot #> tcam** を使うと**コンパイルします非マージ** コマンドをディセーブルにすることができます。 ACL がマージされるかどうか判別するために、**show-access-list hardware interface コマンドを**使用して下さい。
- NetFlow がエンジンで 0/1 のラインカード設定され、出力 ACL が出力 エンジン 3 か 4+ でラインカード設定されれば NetFlow が ACL、また転送されたパケットによって拒否されたパケットを説明するように、出力 ACL は入力および出力 ラインカード両方によって処理されます。

ACL カウンタ サポート

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

定義：

- 毎 ACE —正常な Cisco IOSソフトウェア サポートは、**show access-list <number >** RP/LC のコマンド各 ACE と関連付けられる ACL およびカウンターを表示する。 それは ACL を設定する前に**マージが**無効のときだけ利用可能です。 これはこの設定コマンドの使用によって実行することができます:`Router(config)#hw-module slot <number> tcam compile acl no-merge` イネーブルになったときこのオプションはいくつかの TCAM マージ最適化を消し、スケーラビリティに影響を与えます。 実際の影響は、個々の ACL によって異なります。またポリシー ベース ルーティングがそのインターフェイスで適用される場合カウンターが正しくないことに注目して下さい。 そのケースでは、カウンターを使用されるべきです集約して下さい。
- 毎 ACE （ TCAM ）—各 TCAM エントリと関連付けられるハードウェアカウンタ。 設定は必要ではないし、パフォーマンス/スケーラビリティに影響がありません。 この CLI を使用してラインカードでだけ利用可能。 これらのカウンタは、ソフトウェアではクリアできません。 `LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace` このコマンドのための新しく一般的な CLI は Cisco IOS ソフトウェア リリース 22S で利用できます:`LC-Slot4#show access-list hardware interface p0:1 in` 毎 ACE カウンターと同様に、TCAM カウンターは PBR が ACL のそのインターフェイスで使用されないときだけ有効です。
- 集約—各 ACL はサマリ割り当て/拒否カウンターを示します。 これは、個々の ACE カウンタ

すべての合計です。 設定は必要ではないし、パフォーマンスまたはスケーラビリティに影響がありません。

推奨事項

どれも現時点で。

エンジン 4 (POS) - ACL 処理

概要

エンジン 4 は Cisco IOS ソフトウェア Release 12.0(18)S と それ以降をこの ACL サポートに与えます:

- Engine 4 ラインカードが入力カードである場合、出力 ACL は E0/1/2 ラインカードでサポートされています。 この設定では、出力 ACL は出力 ラインカード CPU によって処理されます。

これらのラインカードはエンジン 4 に基づいています:

ラインカード型	インターフェイス タイプ	エンジンタイプ	接続
4xOC48c/STM16c	POS	E4	
4xOC48c/STM16c	POS	E4	LR
1xOC192c/STM64c	POS	E4	IR
1xOC192c/STM64c	POS	E4	SR
1xOC192c/STM64c	POS	E4	VSR-1
10xGE	SFP	E4	

エンジン 4+ (POS およびDPT) - ACL 処理

概要

エンジン 4+ は 10 Gigabit ポ-トフォリオに ACL機能を Cisco 12000 シリーズ導入します。

入出力それぞれのパスで、ACE が最大 1024 サポートされています。 両方入出力 ACL は 96 まで ACE のための行比率で処理されます。 さらに長い一致でのパフォーマンスは、照合深度によって異なります。

これらの POSラインカードはエンジン 4+ に基づいています:

ラインカード型	インターフェイス タイプ	接続

4xOC48c/STM16c	POS	SR
4xOC48c/STM16c	POS	LR
1xOC192c/STM64c	POS	IR
1xOC192c/STM64c	POS	SR
1xOC192c/STM64c	POS	VSR-1
1xOC192/STM64c	POS	LR
4xOC48c/STM16c	DPT	SFP：
1xOC192c/STM64c	DPT	IR
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1
1xOC192c/STM64c	DPT	LR

サポートされている一致基準

すべての Cisco IOS ソフトウェア リリース 12.0S は規格をサポートし、拡張 ACL 基準は口グを除いて高速経路でサポートされるか、または ACE をフラグメント化します。

サポートされる ACE の数

最大 1024 の ACE (1 方向あたり) が、高速パスでサポートされています。

注: 1021 の ACE が設定可能です。 3 つのエントリは ACE 暗示 **permit ip any any** のために予約済み、**deny ip any any** で、**Cpu コマンドに送信 します**。

サポートされる ACE の数に上限はありません。 1021 制限を越えるどの ACE でもラインカード遅いパスで実行された。

出力 ACL 処理

出力 ACL は、送信側の高速パスで処理されます。 参照して下さい IPv4 出力 ACL -詳細についてはラインカード 相互運用 マトリックス。

ラインカード仕様コマンド

- **show tcam appl [ACL** で / **<label** *ACL*] **tcam >**
- **show tcam appl [ACL** で / *ACL*]**メモリ <port >** *エントリの* **<number >**

操作に関するガイドラインとラインカード インタラクション

- サブインターフェイス ACL はサポートされていません。
- パフォーマンスは、照合深度によって異なります。
- 範囲エントリでは、2 つの ACL ルール (2 個のエントリが境界をまたがる場合は 3 つの ACL ルール) が使用されます。
- 物理インターフェイスごとに ACL が 1 つサポートされています。
- 最大 1024 の ACE (1 方向あたり) が、高速パスでサポートされています。
- 1024 高速経路のうちのどれかが ACE ポートを渡って共有することができます。
- フラグメント キーワードを使用する ACE は遅いパスでフィルタリングされます。
- 遅いパスで処理される拒否されたパケットは ACE のために数えられません。
- NetFlow がエンジンで 0 ラインカード設定され、出力 ACL が出力 エンジン 3 か 4+ でラインカード設定されれば NetFlow が ACL、また転送されたパケットによって拒否されたパケットを説明するように、出力 ACL は入力および出力 ラインカード両方によって処理されます。

推奨事項

どれも現時点で。

エンジン 4+ (イーサネット) - ACL 処理

概要

エンジン 4+ イーサネットラインカードは Cisco 12000 10 ギガビット イーサネット ポ-トフォリオにハードウェアの VLAN ごとのインプットACL 機能性をもたらします。 これらはいくつかの特性です:

- 入出力 ACL はパフォーマンス影響なしでシングル ポートで同時に加えることができます。
- ACL は VLAN またはポートごとに適用します。
- 15K ACE までのインプットACL パフォーマンスは一致深度と低下しません。
- 出力 ACL は、最大 96 の ACE に対してライン レートで処理されます。 さらに長い一致でのパフォーマンスは、照合深度によって異なります。

これらのイーサネットラインカードはエンジン 4+ に基づいています:

ラインカード型	インターフェイス タイプ	エンジンタイプ
10xGE Rev B ("X-B")	SFP：	E4+
モジュラ	SFP：	E4+
1x10GE	10G	E4+
1x10GE	10G	E4+

サポートされている一致基準

すべての Cisco IOS ソフトウェア リリース 12.0S は規格をサポートし、拡張 ACL 基準は口グを除いて高速経路でサポートされるか、または ACE をフラグメント化します。

サポートされる ACE の数

- 15,000 までポートまたは VLAN ごとに設定することができる ACL を入力します。
- 1024 はポートの原則ごとの a で適用することができるカードごとの ACE を出力します。**注**：1021 の ACE が設定可能です。 3 つのエントリは ACE 暗示 **permit ip any any** のために予約済み、**deny ip any any** で、**Cpu コマンドに送信 します**。

出力 ACL 処理

出力 ACL は、送信側の高速パスでネイティブに処理されます。 参照して下さい IPv4 出力 ACL - 詳細についてはラインカード 相互運用 マトリックス。

ラインカード仕様コマンド

- **hw-module slot <number > IP ACL マージ**

操作に関するガイドラインとラインカード インタラクション

- フラグメント キーワードが含まれている ACE は遅いパスで処理されます。
- ACL カウンターはその他の機能と結合される ACL のためにサポートされません。
- ACL カウンターはマージされた ACL のためにサポートされません。 マージされた ACL は **hw-module slot <slot** *数* **> IP ACL マージ** コマンドで設定可能です。
- ラインカードあたり最大 168 の L4 操作がサポートされています。 これが超過すれば、ACL は遅いパスで動作します。
- エンジンに 1 つのラインカード 有効に なる サンプルNetFlow があり、出力 ACL が出力 エンジン 3 か 4+ でラインカード 有効に なれば NetFlow が ACL、また転送されたパケットによって拒否されるパケットを説明するように、出力 ACL は入力および出力 ラインカード両方によって処理されます。

推奨事項

どれも現時点で。

ACL ロギング

Cisco IOS ソフトウェア リリース 12.0(21)S の前に、ACLロギング 情報はメンテナンスバス（ MBUS ）上の RP に専ら送信 されました。 ACLロギング アクティビティのハイ レベルの間に、MBUS のキャパシティを超過することは可能性のあるでした。 Cisco IOS ソフトウェア リリース 12.0(21)S はこのシナリオを防ぐ複数の最適化をもたらします。

MBUS 過負荷 状況はこれらのエラーメッセージが付いている Cisco IOSソフトウェアによって報告されます:

```
LCLOG-3-INVSTATE

MBUS_SYS-3-SEQUENCE
```

Cisco IOS ソフトウェア リリース 12.0(21)S およびそれ以降によって、高い重大度（ 重大度 0-4 ）ロギングメッセージは MBUS による RP により低い深刻度（ 重大度 5-7 ）ログメッセージが

高キャパシティ スイッチング ファブリックを通した RP に提供される間、提供されます。 ACL ログメッセージは高い重大度で、従ってスイッチング ファブリックを通した RP に今渡されます。

この追加された記録 機能性はこれらのコマンドを使用して設定可能です:

- **logging method mbus （ severity ）** —どのメッセージが、重大度によって MBUS を使用して RP に、送られるか判別します。 より高い重大度 メッセージはスイッチ ファブリックを通して送信 されます。
- show logging method - すべてのメッセージ重大度に対して現在の口ギング方式を表示します。
- **logging sequence-nums** —このコマンドはシーケンス番号 ログメッセージにメッセージが RP によってきちんと追加注文することができるように送信 ラインカードを有効に します。 このコマンドなしで、ログメッセージは不連続順序で RP に提供することができます。

IPv4 出力ACL - ラインカード相互運用マトリックス

エンジン 3 およびエンジン 4+ のリリースの出力 ACL処理の概要が入力 ラインカードによって、出力 ACL 処理された前に。 出力 ACL は、高性能な Engine 3 および Engine 4+ の出力 ACL 処理機能を利用できるようにアップデートされています。

この図はの出力 ACL がさまざまなラインカード組み合わせのために処理される要約を提供します:

	出力 ラインカード					
入力 ラインカード (メンバー インターフェイスに適用される出力 ACL)	**E0**	**E1**	**E2**	**E3**	**E4**	**E4+**
E0	入力	入力	入力	出力	該当なし	出力
E1	入力	入力	入力	出力	該当なし	出力
E2	入力	入力	入力	出力	該当なし	出力
E3	出力	出力	出力	出力	該当なし	出力
E4	出力	出力	出力	出力	該当なし	出力
E4+	出力	出力	出力	出力	該当なし	出力

IPv6 ACL サポート

IPv6 延長 ACL は Cisco IOS ソフトウェア リリース 12.0(23)S の E0、E1、E2、E3 および E4+

の遅いパスで（入力および出力）サポートされます。

エンジン 3 では、IPv6 ACL機能は Cisco IOS ソフトウェア リリース 12.0(25)S のハードウェアでサポートされます。 ACL は各アクセス リストの端に暗黙の deny 文を用いる特定のインターフェイスに、適用されます。 IPv6 ACL は否定で **ipv6 access-list コマンド**を使用して設定され、グローバル コンフィギュレーション モードのキーワードを可能にします。 エンジン トラフィック ベース IPv6 オプション ヘッダの 3 ベースのカード サポート フィルタリング、フロー ラベル、およびオプションで、上位層プロトコル型情報。

Cisco 12000 ACL コマンドレファレンス

エンジン 1 コマンド

- **access-list hardware salsa**
- **show controller l3 | ASIC を含んで下さい**

エンジン 2 コマンド

- **access-list hardware psa limit 128**
- **no access-list hardware psa**
- **psa bypass**
- **show access-list psa detail**
- **show access-list psa summary**
- **show controller psa feature**

エンジン 3 コマンド

- **hw-module <slot *#*> tcam は非マージをコンパイルします*!! ------ Cisco IOS ソフトウェア リリース 12.0(21)S3 現在***
- **show-access-list ハードウェアインターフェイス <interface *名前* >**
- **contr [*tofab* を示して下さい*|frfab*]アルファ ACL <int > vmr2ace**

エンジン 4+ コマンド

- **show access-list gen7 label**
- **show tcam appl [ACL *で* | <label *ACL*] tcam >**
- **show tcam appl [ACL *で* | *エントリの ACL*]メモリ <port ><number >**

エンジン 4+ イーサネット コマンド

- **hw-module slot <number > IP ACL マージ**

用語集

このセクションでは、関連用語の標準的な定義を示します。

- 処理プレーン - 論理的に 3 つの処理プレーンに分割できるネットワーク デバイス。データ平面—ネットワークデバイスをフローするパケットの処理。コントロール プレーン—ネットワークデバイスを繋ぐのに使用されるパケットの処理。 これには、回線プロトコル（Point-to-Point Protocol - PPP、High-Level Data Link Control - HDLC など）、ルーティング プロトコル（Border Gateway Protocol - BGP、Routing Information Protocol version 2 - RIPv2、Open Shortest Path First - OSPF など）、およびタイミング プロトコル（Network Time Protocol -

NTP）が含まれます。管理プレーン—ネットワークデバイスを管理するのに使用するパケットの処理。 これには telnet、セキュア シェル（SSH）、File Transfer Protocol （FTP）、Trivial File Transfer Protocol （TFTP）、SNMP および他の管理プロトコルが含まれています。

- **標準 ACL** —標準 ACL はレイヤ3 で専らフィルタリングします。
- **拡張 ACL** —拡張IPアクセス リストは一致するオペレーションのために送信元 および 宛先アドレス、また制御のより細かい粒状度のためにオプションのプロトコル タイプ 情報を使用します。
- **リニアは処理しました ACL** —ソフトウェアで直線に処理される。 パフォーマンスは、照合深度（一致が決定される前にチェックする必要があるエントリの数）によって異なります。
- ターボ ACL（コンパイル済み） - ターボ ACL は、ソフトウェア処理を加速する、高度に最適化された一連のルックアップ テーブルに ACL をコンパイルすることにより、ソフトウェア ACL 処理を最適化します。 ターボ ACL のパフォーマンスは、照合深度には左右されません。
- **入力 ACL** — ACL は適用するポートを入力するトラフィックに適用しました。
- 出力 ACL - 適用先のポートから出るトラフィックに適用される ACL。 出力 ACL は入力ラインカードで処理されます（ただし、例外はあります）。
- 受信パス ACL - 受信パス ACL は、ルータ自身が宛先になっている制御トラフィック（ルーティング アップデート、SNMP クエリーなど）に対して、フィルタリングを提供します。
- **ラインカード二倍になりますステージ フォワーディング**—入力および出力 パス両方のフォワーディング/機能 ASIC があるラインカード。 これはラインカードが LC CPU へのパンティングパケットのない入力 パケットフローおよび出力 パケットフロー両方の機能を行うようにします。 それはまた二重ステージ転送アルゴリズムの新しい波を Cisco 12000 の内で使用されるために可能にします。 Engine 3 ラインカードがあります。
- **単段 フォワーディング ラインカード**—ちょうど入力パスのフォワーディング/機能 ASIC があるラインカード。 これらのラインカードは入力パスで流れるパケットの ASIC ベースの処理だけを行います。 出トラフィックは（ちょうど転送される）処理されませんか、他の LC の入力 ASIC によって処理されるか、または LC CPU によって管理されます。 エンジン 2、エンジン 4、およびエンジン 4+ は単段 フォワーディング ライン カードの例です。

関連情報

- Cisco 12000 シリーズ インターネット ルータ
- テクニカルサポートとドキュメント - Cisco Systems