IP ACL の設定

この章では、Cisco NX-OS デバイスの IP アクセス コントロール リスト（ACL）を設定する方法について説明します。

特に指定がなければ、IP ACL は IPv4 および IPv6 の ACL を意味します。

この章は、次の項で構成されています。

ACL について

ACL とは、トラフィックのフィルタリングに使用する順序付きのルール セットのことです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。デバイスは、ある ACL がパケットに適用されると判断すると、そのすべてのルールの条件にパケットを照合し、テストします。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するものがなければ、デバイスは適用可能な暗黙のルールを適用します。デバイスは、許可されたパケットの処理を続行し、拒否されたパケットはドロップします。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACL を使用して、厳重にセキュリティ保護された

ネットワークからインターネットにHTTPトラフィックが流入するのを禁止できます。また、特定のサイトへのHTTPトラフィックだけを許可することもできます。その場合は、サイトのIP アドレスが、IP ACL に指定されているかどうかによって判定します。

ACL のタイプと適用

セキュリティ トラフィック フィルタリングには次のタイプの ACL を使用できます。

IPv4 ACL
IPv4 トラフィックだけに適用されます。
IPv6 ACL
IPv6 トラフィックだけに適用されます。
MAC ACL
デバイスにより MAC ACL のみが非 IP トラフィックに適用されます。

IP および MAC ACL には以下の種類のアプリケーションがあります。

ポート ACL
レイヤ 2 トラフィックのフィルタリング
ルータ ACL
レイヤ 3 トラフィックのフィルタリング
VLAN ACL
VLAN トラフィックのフィルタリング
VTY ACL
仮想テレタイプ（VTY）トラフィックのフィルタリング

次の表に、セキュリティ ACL の適用例の概要を示します。

Table 1: セキュリティ ***ACL*** の適用

適用	サポートするインターフェイス	サポートする ACL のタイプ
ポート ACL	• レイヤ 2 インターフェイス • レイヤ 2 イーサネット ポート チャネル インターフェイス ポート ACL をトランク ポートに適用すると、その ACL は、当該トランク ポート上のすべての VLAN 上のトラフィックをフィルタリングします。	• IPv4 ACL • IPv6 ACL • MAC ACL

適用	サポートするインターフェイス	サポートする ACL のタイプ
ルータ ACL	• VLAN インターフェイス • 物理層 3 インターフェイス • レイヤ3イーサネットサブインターフェイス • レイヤ 3 イーサネット ポート チャネル インターフェイス • 管理インターフェイス **Note** VLAN インターフェイスを設定するには、先に VLAN インターフェイスをグローバルにイネーブルにする必要があります。	• IPv4 ACL • IPv6 ACL **Note** MAC ACL は、MAC パケット分類をイネーブルにする場合だけ、レイヤ 3 インターフェイスでサポートされます。 **Note** 出力ルータ ACL は Cisco Nexus 9300 シリーズ スイッチ アップリンク ポートではサポートされません。
VLAN ACL	• VLAN	• IPv4 ACL • IPv6 ACL • MAC ACL
VTY ACL	• VTY	• IPv4 ACL • IPv6 ACL

Related Topics

VLAN ACL について
MAC ACL について

ACL の適用順序

デバイスは、パケットを処理する際に、そのパケットの転送パスを決定します。デバイスがトラフィックに適用する ACL はパスによって決まります。デバイスは、次の順序で ACL を適用します。

1. ポート ACL
2. 入力 VACL
3. 入力ルータ ACL
4. 入力 VTY ACL
5. 出力 VTY ACL
6. 出力ルータ ACL

7. 出力 VACL

パケットが入力 VLAN 内でブリッジされる場合、ルータ ACL は適用されません。

***Figure 1: ACL* の適用順序**

次の図に、デバイスが ACL を適用する順序を示します。

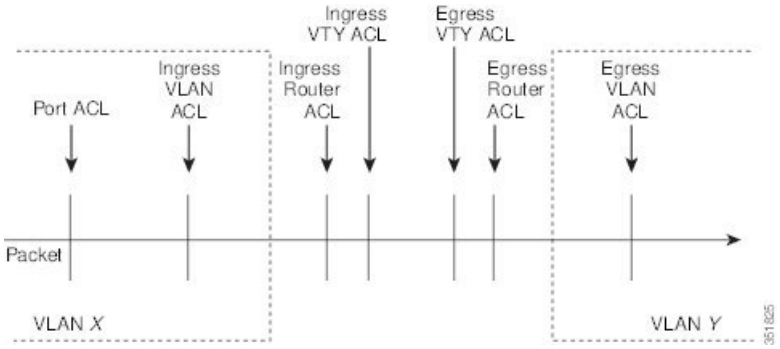
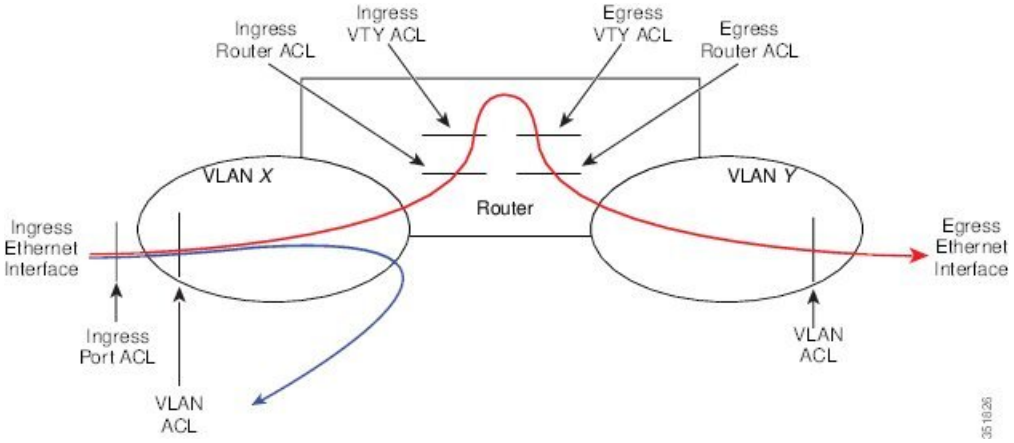


***Figure 2: ACL* とパケット フロー**

次の図に、ACL のタイプに応じた ACL の適用場所を示します。赤いパスは送信元とは異なるインターフェイス上の宛先に送信されるパケットを表しています。青いパスは同じ VLAN 内でブリッジされるパケットを表しています。

デバイスは適用可能な ACL だけを適用します。たとえば、入力ポートがレイヤ 2 ポートの場合、VLAN インターフェイスである VLAN 上のトラフィックには、ポート ACL とルータ ACL が両方とも適用される可能性があります。さらに、その VLAN に VACL が適用される場合、デバイスはその VACL も適用します。



ルールについて

ACL によるネットワーク トラフィックのフィルタリング方法を設定する際に、何を作成、変更、削除するかを決めるのがルールです。ルールは実行コンフィギュレーション内に表示されます。ACL をインターフェイスに適用するか、またはインターフェイスにすでに適用されている ACL 内のルールを変更すると、スーパーバイザ モジュールは実行コンフィギュレーション

内のルールから ACL のエントリを作成し、それらの ACL エントリを適用可能な I/O モジュールに送信します。ACL の設定によっては、ルールよりも ACL エントリの方が数が多くなることがあります。特に、ルールを設定するときにオブジェクトグループを使用してポリシーベース ACL を実装する場合などです。

アクセスリストコンフィギュレーションモードでルールを作成するには、**permit** または **deny** コマンドを使用します。デバイスは、許可ルール内の基準と一致するトラフィックを許可し、拒否ルール内の基準と一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

ここでは、ルールを設定する際に使用できるオプションをいくつか紹介します。

IP ACL および MAC ACL のプロトコル

IPv4、IPv6、および MAC の ACL では、トラフィックをプロトコルで識別できます。指定の際の手間を省くために、一部のプロトコルは名前で指定できます。たとえば、IPv4 または IPv6 の ACL では、ICMP を名前で指定できます。

プロトコルはすべて番号で指定できます。MAC ACL では、プロトコルをそのプロトコルの EtherType 番号（16 進数）で指定できます。たとえば、MAC ACL ルールの IP トラフィックの指定に 0x0800 を使用できます。

IPv4 および IPv6 ACL では、インターネットプロトコル番号を表す整数でプロトコルを指定できます。

送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。送信元と宛先の指定方法は、IPv4 ACL、IPv6 ACL、MAC ACL のどの ACL を設定するのかによって異なります。

IP ACL および MAC ACL の暗黙ルール

IP ACL および MAC ACL には暗黙ルールがあります。暗黙ルールは、実行コンフィギュレーションには設定されていませんが、ACL 内の他のルールと一致しない場合にデバイスがトラフィックに適用するルールです。ACL のルール単位の統計情報を維持するようにデバイスを設定した場合、暗黙ルールの統計情報はデバイスに維持されません。

すべての IPv4 ACL には、次の暗黙のルールがあります。

```
deny ip any any
```

この暗黙ルールによって、デバイスは不一致 IP トラフィックを確実に拒否します。

すべての IPv6 ACL には、次の暗黙のルールがあります。

```
deny ipv6 any any
```

この暗黙ルールによって、デバイスは不一致 IPv6 トラフィックを確実に拒否します。

Note

- IPv6 近隣探索パケット (ルータ要請、およびルータ アドバタイズメント) は、IPv6 ACL の暗黙の **deny ipv6 any any** ルールにより許可されません。
- Cisco Nexus 93180YC-EX、Nexus 93180YC-FX、Nexus 93240YC-FX2、Nexus 93360YC-FX2、Nexus 9336C-FX2、Nexus 9336C-FX2-E、Nexus 93180YC-FX3、N9K-C9316D-GX、N9K-C93600CD-GX、Nexus 9364C-GX、N9K-C9332D-GX2B、Nexus 9364C、および Nexus 9332C プラットフォーム スイッチ で IPv6 ネイバー探索パケットを許可するには、次のルールを明示的に追加する必要があります。
  - **permit icmp any any router-advertisement**
  - **permit icmp any any router-solicitation**
- ネイバー要請（NS）メッセージとネイバーアドバタイズメント（NA）メッセージは、暗黙のルールでは一致しません。NS または NA IPv6 トラフィックを照合するには、次のコマンドが必要です。
  - **permit/deny icmp any any nd-na**
  - **permit/deny icmp any any nd-ns**

すべての MAC ACL には、次の暗黙のルールがあります。

```
deny any any protocol
```

この暗黙ルールによって、デバイスは、トラフィックのレイヤ2ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックを確実に拒否します。

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。これらのオプションは、ACLのタイプによって異なります。次のリストには、ほとんどの追加フィルタリング オプションが含まれていますが、すべてを網羅しているわけではありません。

- IPv4 ACL には、次の追加フィルタリング オプションが用意されています。
  - レイヤ 4 プロトコル
  - TCP/UDP ポート
  - ICMP タイプおよびコード
  - IGMP タイプ
  - 優先レベル
  - DiffServ コード ポイント（DSCP）値
  - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
  - 確立済み TCP 接続

- パケット長

- IPv6 ACL では、次のフィルタリング オプションが追加されています。
  - レイヤ 4 プロトコル
  - カプセル化セキュリティ ペイロード
  - ペイロード圧縮プロトコル
  - Stream Control Transmission Protocol（SCTP）
  - SCTP、TCP、および UDP の各ポート
  - ICMP タイプおよびコード
  - DSCP の値
  - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
  - 確立済み TCP 接続
  - パケット長

- MAC ACL は、次の追加フィルタリング オプションをサポートしています。
  - レイヤ 3 プロトコル (Ethertype)
  - VLAN ID
  - サービス クラス（CoS）

シーケンス番号

デバイスはルールのシーケンス番号をサポートしています。入力するすべてのルールにシーケンス番号が割り当てられます（ユーザによる割り当てまたはデバイスによる自動割り当て）。シーケンス番号によって、次の ACL 設定作業が容易になります。

既存のルールの間に新しいルールを追加

シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。

ルールの削除

シーケンス番号を使用しない場合は、ルールを削除するために、次のようにルール全体を入力する必要があります。

```
switch(config-acl)# no permit tcp 10.0.0.0/8 any
```

このルールに 101 番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

```
switch(config-acl)# no 101
```

ルールの移動

シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号を使用せずにルールを入力すると、デバイスはそのルールを ACL の最後に追加し、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号を割り当てます。たとえば、ACL 内の最後のルールのシーケンス番号が 225 で、シーケンス番号を指定せずにルールを追加した場合、デバイスはその新しいルールにシーケンス番号 235 を割り当てます。

また、Cisco NX-OS では、ACL 内ルールのシーケンス番号を再割り当てできます。シーケンス番号の再割り当ては、ACL 内に、100、101 のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

論理演算子と論理演算ユニット

TCP および UDP トラフィックの IP ACL ルールでは、論理演算子を使用して、ポート番号に基づきトラフィックをフィルタリングできます。Cisco NX-OS では、入力方向でのみ論理演算子をサポートします。

このデバイスは、論理演算ユニット（LOU）というレジスタに、演算子とオペランドの組み合わせを格納します。各タイプの演算子は、次のように LOU を使用します。

eq
LOU には格納されません。

gt
1 LOU を使用します。

lt
1 LOU を使用します。

neq
1 LOU を使用します。

range
1 LOU を使用します。

ACL ロギング

ACL ロギング機能は、 ACL のフローをモニタし、統計情報をログに記録します。

フローは、送信元インターフェイス、プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート値によって定義されます。フローの統計情報には、転送されたパケット（ACL エントリの許可条件に一致する各フロー）およびドロップされたパケット（ACL エントリの拒否条件に一致する各フロー）の数が含まれます。

時間範囲

時間範囲を使用して、ACL ルールが有効になる時期を制御できます。たとえば、インターフェイスに着信するトラフィックに特定の ACL を適用するとデバイスが判断し、その ACL のある

ルールの時間範囲が有効になっていない場合、デバイスは、トラフィックをそのルールと照合しません。デバイスは、そのデバイスのクロックに基づいて時間範囲を評価します。

時間範囲を使用する ACL を適用すると、デバイスはその ACL で参照される時間範囲の開始時または終了時に影響する I/O モジュールをアップデートします。時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。

IPv4、IPv6、および MAC の各 ACL は時間範囲をサポートしています。デバイスがトラフィックに ACL を適用する場合、有効なルールは次のとおりです。

- 時間範囲が指定されていないすべてのルール
- デバイスがその ACL をトラフィックに適用した時点（秒）が時間範囲に含まれているルール

名前が付けられた時間範囲は再利用できます。多くの ACL ルールを設定する場合は、時間範囲を名前で一度設定すれば済みます。時間範囲の名前は最大 64 の英文字で指定します。

時間範囲には、1 つまたは複数のルールで構成されます。これらのルールは次の 2 種類に分類できます。

絶対

特定の開始日時、終了日時、その両方を持つルール、またはそのどちらも持たないルール。絶対時間範囲のルールがアクティブかどうかは、開始日時または終了日時の有無によって、次のように決まります。

- 開始日時と終了日時が両方指定されている：この時間範囲ルールは、現在の時刻が開始日時よりも後で終了日時よりも前の場合にアクティブになります。
- 開始日時が指定され、終了日時は指定されていない：この時間範囲ルールは、現在の時刻が開始日時よりも後である場合にアクティブになります。
- 開始日時は指定されず、終了日時が指定されている：この時間範囲ルールは、現在の時刻が終了日時よりも前である場合にアクティブになります。
- 開始日時も終了日時も指定されていない：この時間範囲ルールは常にアクティブです。

たとえば、新しいサブネットへのアクセスを許可するようにネットワークを設定する場合、そのサブネットをオンラインにする予定日の真夜中からアクセスを許可するような時間範囲を指定し、この時間範囲をそのサブネットに適用する ACL ルールに使用します。デバイスはこのルールを含む ACL を適用する場合、開始日時が過ぎると、この時間範囲を使用するルールの適用を自動的に開始します。

定期

毎週 1 回以上アクティブになるルール。たとえば、定期時間範囲を使用すると、平日の営業時間中だけ、研究室のサブネットにアクセスできるようにすることができます。デバイ

スは、そのルールを含む ACL が適用されていて、時間範囲がアクティブな場合にだけ、この時間範囲を使用する ACL ルールを自動的に適用します。

Note デバイスは、時間範囲内のルールの順序に関係なく、時間範囲がアクティブかどうかを判断します。Cisco NX-OS は、時間範囲を編集できるように時間範囲内にシーケンス番号を入れます。

時間範囲には備考を含めることもできます。備考を使用すると、時間範囲にコメントを挿入できます。備考は、最大 100 文字の英数字で指定します。

デバイスは次の方法で時間範囲がアクティブかどうかを判断します。

- 時間範囲に絶対ルールが 1 つまたは複数含まれている：現在の時刻が 1 つまたは複数の絶対ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に定期ルールが 1 つまたは複数含まれている：現在の時刻が 1 つまたは複数の定期ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に絶対ルールと定期ルールが両方含まれている：現在の時刻が 1 つまたは複数の絶対ルールと 1 つ以上の定期ルールの範囲内にある場合に、その時間範囲はアクティブです。

時間範囲に絶対ルールと定期ルールが両方含まれている場合、定期ルールがアクティブになるのは、最低 1 つの絶対ルールがアクティブな場合だけです。

ポリシーベース ACL

デバイスはポリシーベース ACL（PBACL）をサポートしています。PBACL を使用すると、オブジェクト グループ全体にアクセス コントロール ポリシーを適用できます。オブジェクト グループは、IP アドレスのグループまたは TCP ポートもしくは UDP ポートのグループです。ルール作成時に、IP アドレスやポートを指定するのではなく、オブジェクト グループを指定できます。

IPv4 または IPv6 の ACL の設定にオブジェクト グループを使用すると、ルールの送信元または宛先に対してアドレスまたはポートの追加や削除を行う場合に、ACL を簡単にアップデートできます。たとえば、3 つのルールが同じ IP アドレス グループ オブジェクトを参照している場合は、3 つのすべてのルールを変更しなくても、オブジェクトに IP アドレスを追加すれば済みます。

PBACL を使用しても、インターフェイスに ACL を適用する際にその ACL が必要とするリソースは減りません。PBACL の適用時、またはすでに適用されている PBACL のアップデート時には、デバイスはオブジェクト グループを参照する各ルールを展開し、グループ内の各オブジェクトと ACL エントリが 1 対 1 になるようにします。あるルールに、送信元と宛先が両方ともオブジェクト グループとして指定されている場合、この PBACL を適用する際に I/O モジュールに作成される ACL エントリの数は、送信元グループ内のオブジェクト数に宛先グループ内のオブジェクト数をかけた値になります。

ポート、ルータ、Policy-Based Routing（PBR）、 VLAN ACL には、次のオブジェクト グループ タイプが適用されます。

IPv4 アドレス オブジェクト グループ

IPv4 ACL ルールで送信元または宛先アドレスの指定に使用できます。**permit** コマンドまたは **deny** コマンドを使用してルールを設定する際に、**addrgroup** キーワードを使用すると、送信元または宛先のオブジェクト グループを指定できます。

IPv6 アドレス オブジェクト グループ

IPv6 ACL ルールで送信元または宛先アドレスの指定に使用できます。**permit** コマンドまたは **deny** コマンドを使用してルールを設定する際に、**addrgroup** キーワードを使用すると、送信元または宛先のオブジェクト グループを指定できます。

プロトコル ポート オブジェクト グループ

IPv4 および IPv6 の TCP および UDP ルールで送信元または宛先のポートの指定に使用できます。**permit** または **deny** コマンドを使用してルールを設定する際に、**portgroup** キーワードを使用すると、送信元または宛先のオブジェクト グループを指定できます。

Note ポリシーベースルーティング（PBR）ACLは、ルールを設定するためのdenyアクセスコントロールエントリ（ACE）またはdenyコマンドをサポートしていません。

統計情報と ACL

このデバイスは IPv4、IPv6、および MAC の ACL に設定した各ルールのグローバル統計を保持できます。1 つの ACL が複数のインターフェイスに適用される場合、ルール統計には、その ACL が適用されるすべてのインターフェイスと一致する（ヒットする）パケットの合計数が維持されます。

Note インターフェイスレベルの ACL 統計はサポートされていません。

設定する ACL ごとに、その ACL の統計情報をデバイスが維持するかどうかを指定できます。これにより、ACL によるトラフィック フィルタリングが必要かどうかに応じて ACL 統計のオン、オフを指定できます。また、ACL 設定のトラブルシューティングにも役立ちます。

デバイスには ACL の暗黙ルールの統計情報は維持されません。たとえば、すべての IPv4 ACL の末尾にある暗黙の **deny ip any any** ルールと一致するパケットのカウントはデバイスに維持されません。暗黙ルールの統計情報を維持する場合は、暗黙ルールと同じルールを指定した ACL を明示的に設定する必要があります。

Related Topics

IP ACL の統計情報のモニタリングとクリア （54 ページ）
IP ACL および MAC ACL の暗黙ルール （5 ページ）

Atomic ACL のアップデート

デフォルトでは、Cisco Nexus 9000 シリーズのデバイスのスーパーバイザ モジュールで、ACL の変更を I/O モジュールにアップデートする際には、Atomic ACL のアップデートを実行します。Atomic アップデートでは、アップデートされる ACL が適用されるトラフィックを中断させることがありません。しかし、Atomic アップデートでは、ACL のアップデートを受け取る I/O モジュールに、関係する ACL の既存のすべてのエントリに加えて、アップデートされた ACL エントリを保存するのに十分なリソースがあることが必要です。アップデートが行われた後、アップデートに使用されたリソースは開放されます。I/O モジュールに十分なリソースがない場合は、デバイスからエラー メッセージが出力され、この I/O モジュールに対する ACL のアップデートは失敗します。

I/O モジュールに Atomic アップデートに必要なリソースがない場合は、**no hardware access-list update atomic** コマンドを使用して Atomic アップデートをディセーブルにすることができますが、デバイスで既存の ACL を削除して、アップデートされた ACL を適用するには、多少の時間がかかります。ACL が適用されるトラフィックは、デフォルトでドロップされます。

ACL が適用されるすべてのトラフィックを許可し、同時に非 Atomic アップデートを受信するようにするには、**hardware access-list update default-result permit** コマンドを使用してください。

次の例では、ACL に対する Atomic アップデートをディセーブルにする方法を示します。

```
switch# config t
switch(config)# no hardware access-list update atomic
```

次の例では、非 Atomic ACL アップデートの際に、関連するトラフィックを許可する方法を示します。

```
switch# config t
switch(config)# hardware access-list update default-result permit
```

次の例では、Atomic アップデート方式に戻る方法を示します。

```
switch# config t
switch(config)# no hardware access-list update default-result permit
switch(config)# hardware access-list update atomic
```

IP ACL に対する Session Manager のサポート

Session Manager は IP ACL および MAC ACL の設定をサポートしています。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。

ACL TCAM リージョン

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。

Cisco Nexus 9300 および 9500 シリーズ スイッチと Cisco Nexus 3164Q、31128PQ、3232C、および 3264Q スイッチでは、出力 TCAM サイズは 1K で、4 つの 256 エントリに分割されます。他の Cisco Nexus 9300 および 9500 シリーズ スイッチ、3164Q および 31128PQ スイッチでは、入力 TCAM サイズは 4K で、8 つの 256 スライスと 4 つの 512 スライスに分割されます。スライスは割り当ての単位です。1 つのスライスを割り当てることができるのは 1 つのリージョンだけです。たとえば、サイズが 512 のスライスを使用して、サイズがそれぞれ 256 の 2 つの機能を設定することはできません。同様に、256 サイズのスライスを使用して、サイズがそれぞれ 128 の 2 つの機能を設定することはできません。IPv4 TCAM リージョンはシングル幅です。IPv6、QoS、MAC、CoPP、およびシステム TCAM リージョンはダブル幅で、物理 TCAM エントリを 2 倍消費します。たとえば、サイズ 256 の論理リージョン エントリが実際に消費する物理 TCAM エントリは 512 です。

IPv6、ポート ACL、VLAN ACL、およびルータ ACLを作成でき、QoS の IPv6 と MAC アドレスを照合できます。ただし、Cisco NX-OS ではすべてを同時にサポートすることはできません。Ipv6、MAC、およびその他希望の TCAM リージョンを有効にするには、既存の TCAM リージョン（TCAM カービング）のサイズを削除または削減する必要があります。すべての TCAM リージョンの設定コマンドでは、新たな変更を TCAM に組み込むことができるかを評価します。できない場合は、エラーを報告し、コマンドは拒否されます。既存の TCAM リージョンのサイズを削除または削減して、新しい要件のためのスペースを確保する必要があります。

N9K-X9636C-RX では、PACL が外部 TCAM リージョンを使用する場合、内部 TCAM は ifacl に 2K を使用する必要があり、入力 RACL-IPv4 は最大 2044 を使用できます。出力 PACL 外部 TCAM リージョンを使用する場合は、追加の 4 つのエントリが必要です。

ACL TCAM リージョン サイズには、次の注意事項と制約事項があります。

- 既存の TCAM リージョンで RACL または PACL をイネーブル化するには、12,288 を超える TCAM リージョンを分割する必要があります。
- Cisco Nexus 9300 シリーズ スイッチでは、X9536PQ、X9564PX、および X9564TX ライン カードを使用して、40G ポートに適用される QoS 分類ポリシーを適用します。ここでは、256 エントリの粒度でのカービングに使用できる 768 の TCAM エントリが利用可能です。これらのリージョン名にはプレフィックス「ns-」が付けられます。
- X9536PQ、X9564PX、および X9564TX ライン カードの場合、IPv6 TCAM リージョンのみが倍幅のエントリを消費します。他の TCAM リージョンは、シングル幅のエントリを消費します。
- VACL リージョンを設定する場合は、入力および出力方向の両方で同じサイズが設定されます。リージョン サイズがいずれかの方向に対応できない設定は拒否されます。
- RACL v6、CoPP、およびマルチキャストの TCAM サイズはデフォルト値です。以下の Cisco Nexus 9504 および Cisco Nexus 9508 ラインカードでは、リロード中にライン カード障害が発生しないように、これらの TCAM サイズをゼロ以外にする必要があります。
  - N9K-X96136YC-R
  - N9K-X9636C-RX
  - N9K-X9636Q-R

- N9K-X9636C-R

- N9K-X96136YC-R および N9K-X9636C-R ライン カードは、2K の出力 RACL をサポートします。

次の表に、特定の機能を動作させるために設定する必要があるリージョンをまとめます。リージョン サイズは、特定の機能のスケール要件に基づいて選択する必要があります。

表 *2: ACL TCAM* リージョンごとの機能

機能名	リージョン名
ポート ACL	ifacl：IPv4ポートACL用 ipv6-ifacl：IPv6 ポート ACL 用 mac-ifacl：MAC ポート ACL 用
ポート QoS（レイヤ 2 ポートまたはポート チャネルに適用される QoS 分類ポリシー）	qos、qos-lite、、ns-qos、e-qos、または e-qos-lite：IPv4 パケット分類用 ipv6-qos、ns-ipv6-qos、または e-ipv6-qos：IPv6 パケット分類用 mac-qos、ns-mac-qos、または e-mac-qos：非 IP パケット分類用 （注） Cisco Nexus 9300 シリーズ スイッチの 40G ポートで分類する必要があるトラフィックの場合は、qos リージョンと対応する ns- * qos 領域を分割する必要があります。
VACL	vacl：IPv4 パケット用 ipv6-vacl：IPv6 パケット用 Mac-vacl：非 IP パケット用

機能名	リージョン名
VLAN QoS（VLAN に適用される QoS 分類ポリシー）	vqos または ns-vqos：IPv4 パケットの分類用 ipv6-vqos または ns-ipv6-vqos：IPv6 パケットの分類用 mac-vqos or ns-mac-vqos：非 IP パケットの分類用 （注） Cisco Nexus 9300 シリーズ スイッチの 40G ポートで分類する必要があるトラフィックの場合は、qos 領域と対応する ns- * qos 領域を分割する必要があります。
RACL	e-racl：出力 IPv4 RACL 用 e-ipv6-racl：出力 IPv6 RACL 用 racl：IPv4 RACL の場合 ipv6-racl：IPv6 RACL の場合
レイヤ 3 QoS（レイヤ 3 ポートまたはポート チャネルに適用される QoS 分類ポリシー）	L3qos、l3qos-lite、または ns-l3qos：IPv4 パケットの分類用 Ipv6-l3qos または ns-ipv6-l3qos：IPv6 パケットの分類用 （注） Cisco Nexus 9300 シリーズ スイッチの 40G ポートで分類する必要があるトラフィックの場合は、qos 領域と対応する ns- * qos 領域を分割する必要があります。
VLAN 送信元または VLAN フィルタ SPAN（Cisco Nexus 9500 または 9300 シリーズ スイッチ用） 40G ポートの Rx SPAN（Cisco Nexus 9300 シリーズ スイッチのみ）	span

機能名	リージョン名
SPAN フィルタ	Ifacl：レイヤ 2（スイッチ ポート）送信元インターフェイスでの IPv4 トラフィックのフィルタリング用。 Ipv6-ifacl：レイヤ 2（スイッチ ポート）送信元インターフェイスでの IPv6 トラフィックのフィルタリング用。 Mac-ifacl：レイヤ 2（スイッチ ポート）送信元インターフェイスでのレイヤ 2 トラフィックのフィルタリング用。 vacl：VLAN 送信元の IPv4 トラフィックをフィルタリングします。 ipv6-vacl：VLAN 送信元の IPv6 トラフィックをフィルタリングします。 mac-vacl：VLAN 送信元のレイヤ 2 トラフィックをフィルタリングします。 Racl：レイヤ 3 インターフェイスでの IPv4 トラフィックのフィルタリング用。 Ipv6-racl：レイヤ 3 インターフェイスでの IPv6 トラフィックのフィルタリング用。
SVI カウンタ （注） この領域は、レイヤ 3 SVI インターフェイスのパケット カウンタを有効にします。	svi
BFD、DHCP リレー、または DHCPv6 リレー	redirect
CoPP	copp （注） リージョン サイズを 0 にすることはできません。
システム管理ACL	system （注） 領域サイズは変更できません。

機能名	リージョン名
vPC コンバージェンス （注） この領域は、vPC リンクがダウンし、トラフィックをピアリンクにリダイレクトする必要がある場合にコンバージェンス時間を増加させます。	vPC コンバージェンス （注） この領域サイズを 0 に設定すると、vPC リンク障害のコンバージェンス時間が影響を受ける可能性があります。
ファブリック エクステンダ（FEX）	fex-ifacl、fex-ipv6-ifacl、fex-ipv6-qos、fex-mac-ifacl、fex-mac-qos、fex-qos、fex-qos-lite

関連トピック

ACL TCAM リージョン サイズの設定 （30 ページ）
TCAM カービングの設定 （37 ページ）

ACL タイプでサポートされる最大ラベル サイズ

Cisco NX-OS スイッチは、対応する ACL タイプに対して次のラベル サイズをサポートします。

表 *3 : ACL* タイプと最大ラベル サイズ

ACL タイプ	方向（Direction）	ラベル（Label）	ラベルタイプ
RACL/PBR/VACL/ L3-VLAN QoS/L3-VLAN SPAN ACL	受信側	62	BD
RACL/VACL/L3-VLAN QoS	送信側	254	BD
L2 QoS	送信側	31	IF

IP ACL の前提条件

IP ACL の前提条件は次のとおりです。

- IP ACL を設定するためには、IP アドレッシングおよびプロトコルに関する知識が必要です。
- ACL を設定するインターフェイス タイプについての知識が必要です。

IP ACL の注意事項と制約事項

IP ACL の設定に関する注意事項と制約事項は次のとおりです。

- ACL の設定には Session Manager を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、1,000 以上のルールが含まれている ACL に対して特に推奨されます。Session Manager の詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* システム管理設定ガイド』を参照してください。
- 12K ー 64K の範囲の IPv4 PACL の設定は、-RX ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされます。
- 異なるシーケンス番号を持つ重複した ACL エントリは、設定で許可されます。ただし、これらの重複エントリはハードウェア アクセス リストにプログラムされません。
- 最大 62 の一意の ACL を設定できます。各 ACL は、1 つのラベルを持ちます。同じ ACL が複数のインターフェイスで設定される場合、同じラベルが共有されます。ただし、各 ACL が一意のエントリを持つ場合、ACL のラベルは共有されず、そのラベルの上限は 62 です。これは、Cisco Nexus 9500 シリーズ スイッチおよび Cisco Nexus 3636C-R スイッチには適用されません。
- 通常、IP パケットに対する ACL 処理は I/O モジュール上で実行されます。これには、ACL 処理を加速化するハードウェアを使用します。場合によっては、スーパーバイザ モジュールで処理が実行されることもあります。この場合、特に多数のルールが設定されている ACL を処理する際には、処理速度が遅くなることがあります。管理インターフェイス トラフィックは、常にスーパーバイザ モジュールで処理されます。次のカテゴリのいずれかに属する IP パケットがレイヤ 3 インターフェイスから出る場合、これらのパケットはスーパーバイザ モジュールに送られて処理されます。
  - レイヤ 3 最大伝送単位チェックに失敗し、そのためにフラグメント化を要求しているパケット
  - IP オプションがある IPv4 パケット（他の IP パケット ヘッダーのフィールドは、宛先アドレス フィールドの後）
  - 拡張 IPv6 ヘッダー フィールドがある IPv6 パケット

  レート制限を行うことで、リダイレクト パケットによってスーパーバイザ モジュールに過剰な負荷がかかるのを回避します。
- 時間範囲を使用する ACL を適用すると、デバイスは、その ACL エントリで参照される時間範囲の開始時または終了時に ACL エントリを更新します。時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。
- IP ACL を VLAN インターフェイスに適用するためには、VLAN インターフェイスをグローバルにイネーブル化する必要があります。VLAN インターフェイスの詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* インターフェイス設定ガイド』を参照してください。
- VTY ACL 機能はすべての VTY 回線のすべてのトラフィックを制限します。異なる VTY 回線に異なるトラフィックの制限を指定できません。どのルータの ACL も VTY ACL として設定できます。

- 出力 VTY ACL（アウトバウンド方向の VTY 回線に適用される IP ACL）は、ファイル転送プロトコル（TFTP、FTP、SCP、SFTPなど）が出力 VTY ACL 内で明示的に許可されていない限り、スイッチがファイル転送プロトコルによってファイルをコピーするのを禁止します。
- 未定義の ACL をインターフェイスに適用すると、システムは空の ACL と見なし、すべてのトラフィックを許可します。
- IP トンネルは、ACLまたはQoSポリシーをサポートしません。
- VXLAN 向け ACL には次の注意事項が適用されます。
  - アクセスからネットワーク方向（レイヤ 2 からレイヤ 3 のカプセル化パス）のトラフィックに対してレイヤ 2 ポートに適用される入力ポート ACL は、内部ペイロードでサポートされます。
  - アクセス側でポート ACL を使用して、オーバーレイ ネットワークに入るトラフィックをフィルタリングすることを推奨します。
  - ネットワークからアクセス方向（レイヤ 3 からレイヤ 2 へのカプセル化解除パス）の内部または外部ペイロードで照合されるアップリンク レイヤ3インターフェイスに適用される入力ルータ ACL はサポートされません。
  - アクセスからネットワーク方向（カプセル化パス）の内部または外部ペイロードで照合されるアップリンク レイヤ 3 インターフェイスに適用される出力ルータ ACL はサポートされません。
- Cisco Nexus 9300 および 9500 シリーズ スイッチ、および Cisco Nexus 9200 および 9300-EX シリーズスイッチには、VXLAN トラフィックで使用できる ACL オプションに関する次の制限があります。
  - ネットワークからアクセス方向（カプセル化解除パス）のトラフィックに対する、レイヤ 2 ポートに適用される出力ポート ACL はサポートされません。
  - アクセスからネットワーク方向（カプセル化パス）のトラフィックに対する、VLAN に適用される入力 VACL はサポートします。
  - ネットワークからアクセス方向（カプセル化解除パス）のトラフィックに対する、VLAN に適用される出力 VACL はサポートします。
  - アクセスからネットワーク方向（カプセル化パス）のトラフィックに対する、SVI に面するテナントまたはサーバに適用される入力 RACL はサポートします。
  - ネットワークのアクセス方向（カプセル化解除パス）へのトラフィック用に、テナントまたはサーバに適用される出力 RACL はサポートします。
- 出力方向の IPv4 ACL ロギングはサポートされていません。
- VACL の ACL ロギングはサポートされていません。
- ACL ロギングは、**ip port access-group** コマンドで設定されたポート ACL と、**ip access-group** コマンドで設定されたルータ ACL にのみ適用されます。

- DoS 攻撃を防ぐため、IPv4 ACL フローの総数はユーザ定義の最大値に制限されます。この制限に到達すると、新しいログは既存のフローが終了するまで作成されません。
- IPv4 ACL ロギングによって生成される syslog エントリ数は、ACL ロギング プロセスで設定されたログ レベルによって制限されています。Syslogエントリの数がこの制限を超えると、ロギング機能が一部のロギング メッセージをドロップする場合があります。したがって、IPv4 ACL ロギングは課金ツールやACLとの一致数を正確に把握するための情報源として使用しないでください。
- 出力ルータ ACL は Cisco Nexus 9300 シリーズ スイッチ アップリンク ポートではサポートされません。
- Cisco NX-OS リリース 9.2(1) では、出力 ACL は、X9636C-R、X9636C-RX、および X9636Q-R ライン カードを搭載したCisco Nexus 9508スイッチではサポートされていません。
- レイヤ 3 の物理または論理インターフェイスに適用されるルータ ACL がマルチキャスト トラフィックとマッチしません。マルチキャスト トラフィックをブロックする必要がある場合は、代わりに PACL を使用します。この動作は、Cisco Nexus 9000、9300、9300-EX と 9500 シリーズ スイッチ、および Cisco Nexus 3164Q、31128PQ、3232C、および 3264Q スイッチに適用されます。
- ネットワーク フォワーディング エンジン（NFE）対応スイッチの場合、トンネル インターフェイスの外部ヘッダーで照合される入力 RACL はサポートされません。
- 複数のインターフェイスに同じ QoS ポリシーと ACL が適用された場合、ラベルが共有されるのは、QoS ポリシーが no-stats オプションで適用されたときだけです。
- スイッチ ハードウェアは、出力 TCAM の範囲チェック（レイヤ 4 動作）をサポートしません。したがって、レイヤ 4 オペレーション ベースの分類をする ACL および QoS ポリシーは、出力 TCAM での複数エントリに拡張する必要があります。
- TCAM リソースは次のシナリオでは共有されま。
  - ルーテッドACLを複数のスイッチ仮想インターフェイス（SVI）に入力方向で適用する場合。
- TCAM リソースは次のシナリオでは共有されません。
  - VACL（VLAN ACL）が複数のVLANに適用される場合。
  - ルーテッド ACL を出力方向の複数の SVI に適用する場合。
- HTTP 方式に基づくアクセス リストは、Cisco Nexus 9200、9300-EX、9300-FX、9300-FX2、9300-FXP プラットフォーム スイッチと、X9700- EX および X9700-FX ライン カードを搭載した 9500 スイッチではサポートされません。これらすべてのスイッチでは、UDF ベースの ACL を使用する必要があります。
- HTTP メソッドは FEX ポートではサポートされません。
- 次の注意事項と制約事項は、Cisco Nexus 9200 および 9200-EX シリーズ スイッチに適用されます。

- 出力 MAC ACL はサポートされていません。
- トンネルがトラフィックの発信元となっているデバイスでのトンネルインターフェイスの外部ヘッダーでパケットが照合される場合、出力RACLはインターフェイスでサポートされません。
- トンネル インターフェイスの外部ヘッダーで照合される入力 RACL はサポートされません。
- IP の長さをベースに一致基準はサポートされていません。
- すべての ACL ベースの機能を同時に有効にすることはできません。
- 16 の レイヤ 4 操作がサポートされます。
- レイヤ 4 動作は、出力 TCAM リージョンではサポートされません。
- MAC 圧縮表サイズは 4096 + 512 オーバーフロー TCAM です。
- MAC アドレスと MAC マスクのオーバーラップは拒否されます。
- ACL ログ レート リミッタには、送信またはドロップされたパケット用のハードウェア カウンタはありません。
- ACL ログ レート リミッタは、集約レート制限を使用する代わりに、TCAM 単位のエントリ レベルで実装され、デフォルトは 1 pps です。
- ネットワーク アドレス変換（NAT）の例外カウンタはゼロです。
- TAP アグリゲーションでは PACL リダイレクトだけがサポートされます。VACLリダイレクトはサポートされていません。
- DHCPv4 スヌーピングまたはリレー、DHCPv6 リレー、ARP スヌーピング、VXLAN の 4 つの機能のうち、同時にサポートできるのは 3 つだけです。適用されるのは最初に設定された 3 つの機能であり、3 つのブリッジ ドメイン ラベル ビットがすべて使用中になるため、4 番目は失敗します。
- RACLは、マルチキャスト MAC 宛先アドレスを持つパケットでは照合できません。

- -R ライン カードを備えた Cisco Nexus 9504 および Cisco Nexus 9508 スイッチでは、次の TCAM はサポートされません。
  - すべての FEX 関連 TCAM
  - すべての xxx-lite 関連の TCAM リージョン
  - レンジャー関連の TCAM
  - すべての FCoE 関連の TCAM

- ing-netflow リージョンの TCAM カービング設定は、-FX ライン カードでは実行できます。-EX ライン カードでは、デフォルトの ing-netflow リージョン TCAM カービングが 1024 で

あり、それ以外の場合は設定できません。-EXおよび-FXラインカードのポートの場合、ing-netflow リージョンの推奨最大値は 1024 です。

- Cisco Nexus 9200 および 9300-EX プラットフォーム スイッチでは、sup-redirect ACL の方が SUP 宛てのトラフィックに対してより高いプライオリティを持っているため、ACL ログオプションを使用したルータ ACL は有効になりません。
- Cisco Nexus 9300-GX プラットフォーム スイッチでは、ACL リダイレクトを使用する dot1q VLAN は、1 ー 511 の VLAN ID のみをサポートします。

  PACL リダイレクトまたは TapAgg が設定されている場合、**switchport access vlan** *vlan-id* コマンドは 1 ー 511 の VLAN ID のみをサポートします。
- FHRP VIP 宛てのトラフィックで、トラフィックを許可するように設計された ACL ログが有効な ACE と一致する FHRP スタンバイで入力されるトラフィックの場合、Cisco Nexus 9000 シリーズ スイッチはこのパケットをドロップします。
- Cisco Nexus 3048、3172PQ、3172TQ、3132Q-X、3172PQ-XL、3172TQ-XL、31108PC-V、31108TC-V、3132Q-V、3132C-Z、3232C、3264Q、3264C-E、36180YC -R および 3636C-R スイッチでは、同じ VLAN タグに一致する SVI およびサブインターフェイスがある場合、その SVI でアクセスリストが設定されていると、サブインターフェイスを介してルーティングされるトラフィックはドロップされます。これは ASIC の制限によるもので、L3 サブインターフェイスの出力ルータ ACL はこの制限によりサポートされません。
- 出力 ACL は、VLAN 間ルーティングフローの 2 番目の VLAN の IP アドレスを宛先とするトラフィックをサポートしません。
- Cisco Nexus 9300-EX/FX/FX2/FX3/GX プラットフォーム スイッチおよび 93180YC-FX スイッチでは、レイヤ 3 インターフェイスのマルチキャスト MAC 宛先アドレスを持つパケットで RACL を照合できません。ルーティング可能な修飾子を削除するようにACLを設定する場合は、**ignore routable** コマンドを使用します。ただし、ignore-routable を RACL に追加して SVI に適用すると、RACL はブリッジされたパケットともマッチします。
- ワイルドカード ビットが A.B.C.D 形式の場合、Get 操作は不完全なデータを提供したり、シーケンス番号を提供しなかったりします。これは既知の動作です。Open Config モデルには、srcPrefixMask/dstPrefixMask がありません。また、連続していないマスクのプレフィックス長にマスクを変換できないため、プレフィックス長に対して意味のある値を返すことはできません。
- ing-sup リージョンの最小サイズは 512 エントリで、egr-sup リージョンの最小サイズは 256 エントリです。これらのリージョンを小さい値に設定することはできません。任意のリージョンサイズを、256の倍数のエントリの値だけで切り分けることができます（ただし、spanリージョンは512の倍数のエントリで切り分けることができます）。
- リダイレクト オプションを使用した MAC ACL または PACL（ポート ACL）の拒否 ACE は、Cisco Nexus 9000 シリーズ スイッチではサポートされていません。

IP ACL のデフォルト設定

次の表に、IP ACL パラメータのデフォルト設定を示します。

Table 4: IP ACL パラメータのデフォルト値

パラメータ	デフォルト
IP ACL	デフォルトでは IP ACL は存在しません。
IP ACL エントリ	1024
ACL ルール	すべての ACL に暗黙のルールが適用されます。
オブジェクト グループ	デフォルトではオブジェクト グループは存在しません。
時間範囲	デフォルトでは時間範囲は存在しません。

Related Topics

IP ACL および MAC ACL の暗黙ルール （5 ページ）

IP ACL の設定

IP ACL の作成

デバイスに IPv4 ACL または IPv6 ACL を作成し、これにルールを追加できます。

Before you begin

ACL の設定には Session Manager を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

	Command or Action	Purpose

ステップ 2	次のいずれかのコマンドを入力します。
	• **ip access-list** *name*
	• **ipv6 access-list** *name*
	Example:
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。*name* 引数は 64 文字以内で指定します。

ステップ 3	(Optional) **fragments** {**permit-all** | **deny-all**} **Example:** `switch(config-acl)# fragments permit-all`	初期状態でないフラグメントのフラグメント処理を最適化します。**fragments** コマンドが含まれている ACL がデバイスによってトラフィックに適用される場合、 **fragments** コマンドは初期状態でないフラグメント（このフラグメントは、ACL 内のどの明示的な **permit** コマンドまたは **deny** コマンドとも一致しません）のみと一致します。
ステップ 4	[*sequence-number*] {**permit** | **deny**} *protocol* {*source-ip-prefix* | *source-ip-mask*} {*destination-ip-prefix* | *destination-ip-mask*}	IP ACL 内にルールを作成します。多数のルールを作成できます。 *sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。 IPv4 および IPv6 アクセス リストの場合、送信元と宛先の IPv4 または IPv6 プレフィックスを指定できます。これは、最初の連続するビットでのみ一致します。または、アドレスのいずれかのビットに一致する送信元と宛先の IPv4 ワイルド カードマスクを指定できます。
ステップ 5	(Optional) **statistics per-entry** **Example:** `switch(config-acl)# statistics per-entry`	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。
ステップ 6	(Optional) 次のいずれかのコマンドを入力します。 • **show ip access-lists** *name* • **show ipv6 access-lists** *name* **Example:**	IP ACL の設定を表示します。

	Command or Action	Purpose
	`switch(config-acl)# show ip access-lists acl-01`	
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL の変更

既存の IPv4 ACL または IPv6 ACL のルールの追加と削除は実行できますが、既存のルールを変更することはできません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

Before you begin

ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **ip access-list** *name*
	• **ipv6 access-list** *name*
	Example:
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		名前で指定した ACL の IP ACL コンフィギュレーション モードを開始します。

ステップ 3	(Optional) [*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:**	IP ACL 内にルールを作成します。シーケンス番号を指定すると、ACL内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の

	Command or Action	Purpose
	`switch(config-acl)# 100 permit ip 192.168.2.0/24 any`	末尾に追加されます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	(Optional) [**no**] **fragments** {**permit-all** | **deny-all**} **Example:** `switch(config-acl)# fragments permit-all`	初期状態でないフラグメントのフラグメント処理を最適化します。**fragments** コマンドが含まれている ACL がデバイスによってトラフィックに適用される場合、**fragments** コマンドは初期状態でないフラグメント（このフラグメントは、ACL 内のどの明示的な **permit** コマンドまたは **deny** コマンドとも一致しません）のみと一致します。 **no** オプションを使用すると、フラグメント処理の最適化が削除されます。
ステップ 5	(Optional) **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **Example:** `switch(config-acl)# no 80`	指定したルールを IP ACL から削除します。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 6	(Optional) [**no**] **statistics per-entry** **Example:** `switch(config-acl)# statistics per-entry`	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 **no** オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 7	(Optional) 次のいずれかのコマンドを入力します。 • **show ip access-lists** *name* • **show ipv6 access-lists** *name* **Example:** `switch(config-acl)# show ip access-lists acl-01`	IP ACL の設定を表示します。

	Command or Action	Purpose
ステップ 8	(Optional) **copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

IP ACL 内のシーケンス番号の変更 （28 ページ）

VTY ACL の作成

入力方向または出力方向の全 VTY 回線で、すべての IPv4 または IPv6 トラフィックへのアクセスを制御することにより、VTY ACL を設定できます。

Before you begin

すべての仮想端末回線にユーザが接続できるため、すべての仮想端末回線に同じ制約を設定する必要があります。

ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認でき、特に約 1000 以上のルールを含む ACL に役立ちます。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	{**ip** | **ipv6**} **access-list** *name* **Example:** `switch(config)# ip access-list vtyacl`	ACL を作成し、その ACL の IP アクセス リスト コンフィギュレーション モードを開始します。*name* 引数の最大長は 64 文字です。
ステップ 3	{**permit** | **deny**} プロトコル 送信元 接続先 [**log**] [**time-range** 時間] **Example:** `switch(config-ip-acl)# permit tcp any any`	ACL ルールを作成し、指定した送信元とのすべての TCP トラフィックを許可します。

	Command or Action	Purpose

ステップ 4	**exit**
	Example:
	`switch(config-ip-acl)# exit`
	`switch(config)#`
		IP アクセス リスト コンフィギュレーション モードを終了します。

ステップ 5	**line vty**
	Example:
	`switch(config)# line vty`
	`switch(config-line)#`
		仮想端末を指定し、ラインコンフィギュレーション モードを開始します。

ステップ 6	{**ip** | **ipv6**} **access-class** *name* {**in** | **out**} **Example:** `switch(config-line)# ip access-class vtyacl out`	指定された ACL を使用してすべての VTY 回線に対する着信および発信接続を制限します。*name* 引数の最大長は 64 文字です。
ステップ 7	(Optional) **show** {**ip** | **ipv6**} **access-lists** **Example:** `switch# show ip access-lists`	任意の VTY ACL を含め、設定された ACL を表示します。
ステップ 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

Before you begin

ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

	Command or Action	Purpose
ステップ 2	**resequence** {**ip** | **ipv6**} **access-list** *name starting-sequence-number increment* **Example:** `switch(config)# resequence access-list ip acl-01 100 10`	ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。*starting-sequence-number* 引数と *increment* 引数は、1 ～ 4294967295 の整数で指定します。
ステップ 3	(Optional) **show ip access-lists** *name* **Example:** `switch(config)# show ip access-lists acl-01`	IP ACL の設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL の削除

IP ACL をデバイスから削除できます。

Before you begin

その ACL がインターフェイスに適用されているかどうかを確認します。削除できるのは、現在適用されている ACL です。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。デバイスは削除された ACL を空であると見なします。IP ACL が設定されているインターフェイスを探すには、**show ip access-lists** コマンドまたは **show ipv6 access-lists** コマンドと一緒に summary キーワードを使用します。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • **no ip access-list** *name* • **no ipv6 access-list** *name*	名前で指定した IP ACL を実行コンフィギュレーションから削除します。

	Command or Action	Purpose
	Example: `switch(config)# no ip access-list acl-01`	
ステップ 3	(Optional) 次のいずれかのコマンドを入力します。 • **show ip access-lists** *name* **summary** • **show ipv6 access-lists** *name* **summary** **Example:** `switch(config)# show ip access-lists acl-01 summary`	IP ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ACL TCAM リージョン サイズの設定

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **hardware access-list tcam region** *region tcam-size* 例： `switch(config)# hardware access-list tcam region mpls 256`	ACL TCAM リージョン サイズを変更します。使用可能なリージョンは次のとおりです。 • **copp**：CoPP TCAM リージョン サイズを設定します。 • **E-racl**：**出力フロー**：出力フローカウンタ TCAM リージョン サイズを設定します。 • **e-ipv6-qos**：IPv6 出力 QoS TCAM リージョン サイズを設定します。

	コマンドまたはアクション	目的
		• **e-ipv6-racl**：IPv6 出力ルータ ACL（ERACL）TCAM リージョン サイズを設定します。 • **e-mac-qos**：MAC QoS TCAM リージョン サイズを設定します。 • **e-qos**：IPv4 出力 QoS TCAM リージョン サイズを設定します。 • **e-qos-lite**：IPv4 出力 QoS Lite TCAM リージョン サイズを設定します。 • **e-racl**：IPv4 出力ルータ ACL（ERACL）TCAM リージョン サイズを設定します。 • **fex-ifacl**：FEX IPv4 ポート ACL TCAM リージョン サイズを設定します。 • **fex-ipv6-ifacl**：FEX IPv6 ポート ACL TCAM リージョン サイズを設定します。 • **fex-ipv6-qos**：FEX IPv6 ポート QoS TCAM リージョン サイズを設定します。 • **fex-mac-ifacl**：FEX MAC ポート ACL TCAM リージョン サイズを設定します。 • **fex-mac-qos**：FEX MAC ポート QoS TCAM リージョン サイズを設定します。 • **fex-qos**：FEX IPv4 ポート QoS TCAM リージョン サイズを設定します。 • **fex-qos-lite**：FEX IPv4 ポート QoS TCAM リージョン サイズを設定します。 • **flow**：入力フロー カウンタ TCAM リージョン サイズを設定します。

	コマンドまたはアクション	目的
		• **ifacl**：IPv4 ポート ACL TCAM リージョン サイズを設定します。 • **ipv6-ifacl**：IPv6 ポート ACL TCAM リージョン サイズを設定します。 • **ipv6-l3qos**：IPv6 レイヤ 3 QoS TCAM リージョン サイズを設定します。 • **ipv6-qos**：IPv6 ポート QoS TCAM リージョン サイズを設定します。 • **ipv6-racl**：IPv6 RACL TCAM リージョン サイズを設定します。 • **ipv6-vacl**：IPv6 VACL TCAM リージョン サイズを設定します。 • **ipv6-vqos**：IPv6 VLAN QoS TCAM リージョン サイズを設定します。 • **l3qos**：IPv4 レイヤ 3 QoS TCAM リージョン サイズを設定します。 • **l3qos-lite**：IPv4 レイヤ 3 QoS TCAM リージョン サイズを設定します。 • **mac-ifacl**：MAC ポート ACL TCAM リージョン サイズを設定します。 • **mac-l3qos**：MAC レイヤ 3 QoS TCAM リージョン サイズを設定します。 • **mac-qos**：MAC ポート QoS TCAM リージョン サイズを設定します。 • **mac-vacl**：MAC VACL TCAM リージョン サイズを設定します。 • **mac-vqos**—Configures the size of the MAC VLAN QoS TCAM region. • ns-ipv6-l3qos：X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール（GEM）のIPv6レイヤ3 QoS TCAMリージョンのサイズを設定します。

	コマンドまたはアクション	目的
		• ns-ipv6-qos：X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール（GEM）のIPv6ポートQoS TCAMリージョンのサイズを設定します。 • ns-ipv6-vqos：X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール（GEM）のIPv6 VLAN QoS TCAMリージョンのサイズを設定します。 • ns-l3qos：X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール（GEM）のIPv4レイヤ3 QoS TCAMリージョンのサイズを設定します。 • ns-mac-l3qos：X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール（GEM）のMACレイヤ3 QoS TCAMリージョンのサイズを設定します。 • ns-mac-qos：X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール（GEM）のMACポートQoS TCAMリージョンのサイズを設定します。 • ns-mac-vqos：X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール（GEM）のMAC VLAN QoS TCAMリージョンのサイズを設定します。 • ns-qos：X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール（GEM）のIPv4ポートQoS TCAMリージョンのサイズを設定します。 • ns-vqos：X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール

	コマンドまたはアクション	目的
		（GEM）のIPv4 VLAN QoS TCAM リージョンのサイズを設定します。 • **qos**：IPv4 ポート QoS TCAM リージョン サイズを設定します。 • **qos-lite**：IPv4 ポート QoS lite TCAM リージョン サイズを設定します。 • **racl**：IPv4 ルータの ACL（RACL）TCAM リージョン サイズを設定します。 • **redirect**：リダイレクト TCAM リージョンのサイズを設定します。 • **span**：SPAN TCAM リージョン サイズを設定します。 • **svi**：入力 SVI カウンタ TCAM リージョン サイズを設定します。 • **vacl**：IPv4 VACL TCAM リージョン サイズを設定します。 • vpc-convergence：vPCコンバージェンスTCAMリージョンのサイズを設定します。 • **vqos**：IPv4 VLAN QoS TCAM リージョン サイズを設定します。 • **vqos-lite**：IPv4 VLAN QoS lite TCAM リージョン サイズを設定します。 • *tcam-size*：TCAM サイズ。サイズは 256 の倍数です。サイズが 256 より大きい場合は、512 の倍数でなければなりません。 このコマンドの **no** 形式を使用して、デフォルトの TCAM リージョン サイズに戻します。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
ステップ 4	（任意） **show hardware access-list tcam region** 例： `switch(config)# show hardware access-list tcam region`	デバイスで次のリロード時に適用される TCAM サイズを表示します。
ステップ 5	**reload** 例： `switch(config)# reload`	デバイスがリロードされます。 （注） 新しいサイズの値は、**copy running-config startup-config** + **reload** を入力するか、すべてのラインカード モジュールをリロードした後にのみ有効になります。

例

次に、Cisco Nexus 9500 シリーズ スイッチで RACL TCAM リージョンのサイズを変更する例を示します。

```
switch(config)# hardware access-list tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

次に、変更を確認するために、TCAM リージョンのサイズを表示する例を示します。

次に、デフォルトの RACL TCAM リージョン サイズに戻す例を示します。

```
switch(config)# no hardware profile tcam region racl 512
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

テンプレートを使用した ACL TCAM リージョン サイズの設定

すべての Cisco Nexus 9200、9300、および 9500 シリーズ スイッチでは、この手順またはACL TCAM リージョン サイズの構成手順を使用して ACL TCAM リージョン サイズを構成できます。ただし、NFE2 対応デバイス（X9432C-S 100G ライン カードや C9508-FM-S ファブリック モジュールなど）は、**hardware access-list tcam region** コマンドをサポートしていないため、ACL TCAM リージョン サイズを設定する必要があります。

（注）

- TCAM テンプレートを適用すると、**hardware access-list tcam region** コマンドは機能しません。コマンドを使用するには、テンプレートをコミット解除する必要があります。
- QoS TCAM カービングの設定については、『*Cisco Nexus 9000* シリーズ *NX-OS* サービス品質設定ガイド』を参照してください。
- TCAM プロファイル テンプレートは、C9508-FM-S ファブリック モジュールではサポートされません。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **hardware profile tcam resource template** *template-name* **ref-template** {**nfe** | **nfe2** | {**l2-l3** | **l3**}}
	例：
	`switch(config)# hardware profile tcam resource template SR_MPLS_CARVE ref-template nfe2`
	`switch(config-tcam-temp)#`
		ACL TCAM リージョン サイズを設定するテンプレートを作成します。
		nfe：Network Forwarding Engine（NFE）対応 Cisco Nexus 9300 および 9500 シリーズ、デフォルト TCAM テンプレート。
		nfe2：NFE2 対応 Cisco Nexus 9500 シリーズ、デバイスのデフォルト TCAM テンプレート。
		l2-l3：レイヤ 2 およびレイヤ 3 設定のデフォルト TCAM テンプレート。
		l3：Cisco Nexus 9200 シリーズ スイッチで。

ステップ 3	（任意） *region tcam-size* 例： `switch(config-tcam-temp)# mpls 256`	必要なTCAMリージョンとそのサイズをテンプレートに追加します。テンプレートに追加するリージョンごとにこのコマンドを入力します。使用可能なリージョンのリストについては、ACL TCAM リージョン サイズの構成を参照してください。
ステップ 4	**exit** 例：	TCAM テンプレート コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
	`switch(config-tcam-temp)# exit` `switch(config#)`	
ステップ 5	[**no**] **hardware profile tcam resource service-template** *template-name* 例： `switch(config)# hardware profile tcam resource service-template SR_MPLS_CARVE`	すべてのラインカードおよびファブリックモジュールにカスタムテンプレートを適用します。
ステップ 6	（任意） **show hardware access-list tcam template** {**all** | **nfe** | **nfe2** | **l2-l3** | **l3** | *template-name*} 例： `switch(config)# show hardware access-list tcam template SR_MPLS_CARVE`	すべての TCAM テンプレートまたは特定のテンプレートの設定を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 8	**reload** 例： `switch(config)# reload`	デバイスがリロードされます。 （注） この設定は、**copy running-config startup-config** + **reload** を入力した後にのみ有効になります。

TCAM カービングの設定

デフォルトのTCAMリージョン設定はプラットフォームによって異なり、すべてのTCAMリージョンに対応しているわけではありません。希望のリージョンを有効にするには、1 つのリージョンの TCAM サイズを減らしてから、希望のリージョンの TCAM サイズを増やします。

（注） QoS TCAM カービングの設定については、『*Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。

次の表に、異なるプラットフォームの入出力 TCAM リージョンのデフォルト サイズを示します。

表 *5:* デフォルト *TCAM* リージョン設定（入力）：*Cisco Nexus 9500* シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1536	1	1536
IPv4 レイヤ 3 QoS	256	2	512
SPAN	256	1	256
CoPP	256	2	512
システム	256	2	512
リダイレクト	256	1	256
vPC コンバージェンス	512	1	512
			4 K

表 *6:* デフォルト *TCAM* リージョン設定（出力）：*Cisco Nexus 9500* シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	768	1	768
システム	256	1	256
			1 K

表 *7:* デフォルト *TCAM* リージョン設定（入力）：*Cisco Nexus 9300* シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4ポートACL	512	1	512
IPv4ポートQoS	256	2	512
IPv4 VACL	512	1	512
IPv4 RACL	512	1	512
SPAN	256	1	256
CoPP	256	2	512
ACIリーフラインカードのIPv4ポートQoS	256	1	256
ACIリーフラインカードのIPv4 VLAN QoS	256	1	256
ACIリーフラインカードのIPv4レイヤ3 QoS	256	1	256
システム	256	2	512
リダイレクト	512	1	512

リージョン名	サイズ	幅	合計サイズ
vPC コンバージェンス	256	1	256
			4 K

表 *8 :* デフォルト *TCAM* リージョン設定（出力）：*Cisco Nexus 9300* シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 VACL	512	1	512
IPv4 RACL	256	1	256
システム	256	1	256
			1 K

次に、Cisco Nexus 9500シリーズスイッチでIPv6 RACL TCAMサイズを256に設定する例を示します。サイズが 256 の IPv6 RACL は、IPv6 がダブル幅であるため、512 エントリを使用します。

（注） 別のリージョンのTCAM設定を変更したり、別のデバイスのTCAM設定を変更したりするには、同様の手順に従います。

Cisco Nexus 9500 シリーズ スイッチで入力 IPv6 RACL TCAM リージョンのサイズを設定するには、2 つのオプションのいずれか 1 つを実行します。

オプション #1

入力 IPv4 RACL を 1024 エントリ減らし（1536 - 1024 = 512）、入力 IPv6 RACL を 512 エントリ増やします。このオプションが優先されます。

```
switch(config)# hardware access-list tcam region racl 512
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

表 *9 : IPv4 RACL*（入力）を減らした後の更新された *TCAM* リージョン設定

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1024	1	1024
IPv6 RACL	256	2	256 個のエントリ スライスが使用できないため、1024 個の[1]
IPv4 レイヤ 3 QoS	256	2	512
SPAN	256	1	256
CoPP	256	2	512

リージョン名	サイズ	幅	合計サイズ
システム	256	2	512
リダイレクト	256	1	256
vPC コンバージェンス	512	1	512
			4 K

[1] 2 x 512 エントリ スライスが割り当てられます。

オプション #2

IPv4 3 QoS のサイズを 0 に減らして削除し、入力 IPv6 RACL を追加します。このオプションは、IPv4 レイヤ 3 QoS を使用していない場合に使用できます。

```
switch(config)# hardware access-list tcam region l3qos 0
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

表 *10 :* レイヤ *3 QoS*（入力）を削除した後の更新された *TCAM* リージョン設定

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1536	1	1536
IPv6 RACL	256	2	512
IPv4 レイヤ 3 QoS	0	2	0
SPAN	256	1	256
CoPP	256	2	512
システム	256	2	512
リダイレクト	256	1	256
vPC コンバージェンス	512	1	512
			4 K

サイズ 256 の出力 IPv6 RACL をイネーブルにするには、出力 IPv4 RACL を 256 に減らし、出力 IPv6 RACL を追加します。

```
switch(config)# hardware access-list tcam region e-racl 256
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region e-ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

表 *11 : IPv4 RACL*（出力）を減らした後のデフォルト *TCAM* リージョン設定

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	256	1	256

リージョン名	サイズ	幅	合計サイズ
IPv6 RACL	256	2	512
システム	256	1	256
			1 K

（注） 各 IPv6 ACL は 1,000 ACE に制限されています。これは、すべての IPv6 ACL（RACL、QoS、または SPAN フィルタ）に適用されます。このような制限は IPv4 ACL には適用されません。

TCAM リージョンのサイズを調整した後、**show hardware access-list tcam region** コマンドを入力して、デバイスの次回リロード時に適用可能な TCAM サイズを表示します。

注目 すべてのモジュールの同期を維持するには、すべてのラインカードモジュールをリロードするか、**copy running-config startup-config** + **reload** を入力してデバイスをリロードする必要があります。TCAM リージョン設定が複数であっても、リロードする必要があるのは1回だけです。TCAM リージョン設定がすべて完了するのを待ってから、デバイスをリロードできます。

設定によっては、TCAMサイズを超えたり、スライスが不足したりすることがあります。

TCAM リージョンの設定時に、すべての TCAM リージョンの 4K 入力制限を超えると、次のメッセージが表示されます。

```
ERROR: Aggregate TCAM region configuration exceeded the available Ingress TCAM space.
Please re-configure.
```

スライスの数を超えると、次のメッセージが表示されます。

```
ERROR: Aggregate TCAM region configuration exceeded the available Ingress TCAM slices.
Please re-configure.
```

TCAM リージョンの設定時に、すべての TCAM リージョンの 1K 出力制限を超えると、次のメッセージが表示されます。

```
ERROR: Aggregate TCAM region configuration exceeded the available Egress TCAM space.
Please re-configure.
```

特定の機能の TCAM が設定されていない状態で TCAM カービングを必要とする機能を適用しようとすると、次のメッセージが表示されます。

```
 ERROR: Module x returned status: TCAM region is not configured. Please configure TCAM
region and retry the command.
```

（注） 256 というデフォルトのリダイレクト TCAM リージョン サイズは、多数の BFD または DHCP リレー セッションを実行している場合は十分でない可能性があります。より多くの BFD または DHCP リレー セッションに対応するために、TCAM サイズを 512 に増やす必要がある場合があります。

（注） N9K-C9508（Fretta）システムに少なくとも 1 つの「N9K-X9624D-R2」ラインカードがある場合、「e-racl」tcam 領域サイズは最大 16K です。

関連トピック

ACL TCAM リージョン サイズの設定 （30 ページ）

UDF ベース ポート ACL の設定

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**udf** *udf-name offset-base offset length*
	例：
	`switch(config)# udf pktoff10 packet-start 10 2`
	例：
	`switch(config)# udf pktoff10 header outer l3 20 2`
		次のように UDF を定義します。
		• *udf-name*：UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。
		• *offset-base*：UDF オフセット ベースを以下のように指定します。ここで **header** は、オフセットを考慮したパケット ヘッダーです。{**packet-start** | **header** {**outer** | **inner** {**l3** | **l4**}}}.
		• オフセット：オフセット ベースからのオフセット バイト数を指定します。オフセット ベース（レイヤ 3/レイヤ 4 ヘッダー）の最初のバイトを照合するには、オフセットを 0 に設定します。
		• 長さ：オフセット からバイトの数を指定します。1 または 2 バイトのみがサポートされています。追加のバイトに一致させるためには、複数の UDF を定義する必要があります。

	コマンドまたはアクション	目的
		複数の UDF を定義できますが、シスコは必要な UDF のみ定義することを推奨します。
ステップ 3	**hardware access-list tcam region ing-ifacl qualify** {**udf** *udf-name*} 例： `switch(config)# hardware access-list tcam region ing-ifacl qualify udf pktoff10`	IPv4 ポート ACLに適用する ing-ifacl TCAM リージョンに UDF をアタッチします。 TCAM リージョンに接続できる UDF の数は、プラットフォームによって異なります。Cisco Nexus 9200 スイッチの場合は最大 2 つの UDF、Cisco Nexus 9300 スイッチの場合は最大 8 つのUDF、Cisco Nexus 9300-EX スイッチの場合は を接続できます。 （注） UDF 修飾子が追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。十分な空きスペースがあることを確認してください。 それ以外の場合このコマンドは拒否されます。必要な場合、未使用のリージョンから TCAM スペースが減りますので、このコマンドを再入力します。詳細については、「ACL TCAM リージョン サイズの設定」を参照してください。 （注） このコマンドの **no** 形式は、UDF を TCAM リージョンから切り離し、リージョンをシングル幅に戻します。
ステップ 4	必須: **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 5	必須: **reload** 例： `switch(config)# reload`	デバイスがリロードされます。 （注） UDF 設定は **copy running-config startup-config** + **reload** を入力した後のみ有効になります。

	コマンドまたはアクション	目的

ステップ 6	**ip access-list** *udf-acl*
	例：
	`switch(config)# ip access-list udfacl`
	`switch(config-acl)#`
		IPv4 アクセス コントロール リスト（ACL）を作成して、IP アクセス リスト コンフィギュレーション モードを開始します。

ステップ 7	次のいずれかのコマンドを入力します。
	• **permit udf** *udf-name value mask*
	• **permit ip** *source destination* **udf** *udf-name value mask*
	例：
	`switch(config-acl)# permit udf pktoff10 0x1234 0xffff`
	例：
	`switch(config-acl)# permit ip any any udf pktoff10 0x1234 0xffff`
		ACL を設定し、UDF（例 1）でのみ、または外部パケット フィールドについて現在のアクセス コントロール エントリ（ACE）と併せて UDF で一致させるように設定します（例 2）値とマスクの引数の範囲は 0x0 ～ 0xFFFF です。
		シングル ACL は、UDFがある場合とない場合の両方とも、ACE を有することができます。各 ACE には一致する異なる UDF フィールドがあるか、すべての ACE を UDF の同じリストに一致させることができます。

ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ルータ ACL としての IP ACL の適用

IPv4 ACL または IPv6 ACL は、次のタイプのインターフェイスに適用できます。

- 物理層 3 インターフェイスおよびサブインターフェイス
- レイヤ 3 イーサネット ポート チャネル インターフェイス
- VLAN インターフェイス
- 管理インターフェイス

これらのインターフェイス タイプに適用された ACL はルータ ACL と見なされます。

Note 出力ルータ ACL は Cisco Nexus 9300 シリーズ スイッチ アップリンク ポートではサポートされません。

Before you begin

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*[**.** *number*]
	• **interface port-channel** *channel-number*
	• **interface vlan** *vlan-id*
	• **interface mgmt** *port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		指定したインターフェイス タイプのコンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。 • **ip access-group** *access-list* {**in** | **out**} • **ipv6 traffic-filter** *access-list* {**in** | **out**} **Example:** `switch(config-if)# ip access-group acl1 in`	IPv4 ACL または IPv6 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。
ステップ 4	**ip access-list match-local-traffic** **Example:** `switch(config-if)# ip access-list match-local-traffic`	ローカルで生成された一致するトラフィックを一覧表示します。スイッチを通過するトラフィックには影響しません。
ステップ 5	(Optional) **show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	ACL の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

IP ACL の作成 （23 ページ）

ポート ACL としての IP ACL の適用

IPv4 ACL または Ipv6 ACL は、レイヤ 2 インターフェイス（物理ポートまたはポート チャネル）に適用できます。これらのインターフェイス タイプに適用された ACL は、ポート ACL と見なされます。

Note インターフェイスを **mac packet-classify** で設定する場合は、**mac packet-classify** コマンドをインターフェイス設定から削除するまで、IP ポート ACL をインターフェイスに適用できません。

Before you begin

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot/port*
	• **interface port-channel** *channel-number*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		指定したインターフェイス タイプのコンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。 • **ip port access-group** *access-list* **in** • **ipv6 port traffic-filter** *access-list* **in** **Example:** `switch(config-if)# ip port access-group acl-l2-marketing-group in`	IPv4 または IPv6 ACL をインターフェイスまたはポートチャネルに適用します。ポート ACL では、インバウンド フィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 4	(Optional) **show running-config aclmgr** **Example:**	ACL の設定を表示します。

	Command or Action	Purpose
	`switch(config-if)# show running-config aclmgr`	
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

IP ACL の作成 （23 ページ）
MAC パケット分類のイネーブル化または無効化

IP ACL の VACL としての適用

IP ACL は VACL として適用できます。

Related Topics

VACL の設定

ACL ロギングの設定

ACL ロギング プロセスを設定するには、最初にアクセス リストを作成してから、指定された ACL を使用してインターフェイス上のトラフィックのフィルタリングをイネーブルにし、最後に ACL ロギング プロセス パラメータを設定します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**ip access-list** *name*
	例：
	`switch(config)# ip access-list logging-test`
	`switch(config-acl)#`
		IPv4 ACL を作成し、IP ACL コンフィギュレーション モードを開始します。*name* 引数は 64 文字以内で指定します。

ステップ 3	{**permit** | **deny**} **ip** *source-address destination-address* **log** 例：	条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。システムがルールに一致する各パケットに関する情報ロギング

	コマンドまたはアクション	目的
	`switch(config-acl)# permit ip any 10.30.30.0/24 log`	メッセージを生成できるようにするには、logキーワードを含める必要があります。 *Source-address* および *destination-address* 引数には、IP アドレスとネットワークワイルドカード、IP アドレスと可変長サブネットマスク、ホストアドレス、または任意のアドレスを指定する **any** などがあります。

ステップ 4	**exit**
	例：
	`switch(config-acl)# exit`
	`switch(config)#`
		設定を更新し、IP ACL コンフィギュレーション モードを終了します。

ステップ 5	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 6	**ip access-group** *name* **in** 例： `switch(config-if)# ip access-group logging-test in`	指定された ACL を使用してインターフェイス上の IPv4 トラフィックのフィルタリングをイネーブルにします。着信トラフィックに ACL を適用できます。

ステップ 7	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定を更新し、インターフェイス コンフィギュレーションモードを終了します。

ステップ 8	**logging ip access-list cache interval** *interval* 例： `switch(config)# logging ip access-list cache interval 490`	ACL ロギング プロセスのログ更新間隔（秒単位）を設定します。デフォルト値は 300 秒です。範囲は 5 ～ 86400 秒です。
ステップ 9	**logging ip access-list cache entries** *number-of-flows* 例： `switch(config)# logging ip access-list cache entries 8001`	ACL ロギング プロセスでモニタするフローの最大数を指定します。デフォルト値は 8000 です。サポートされる値の範囲は 0 ～ 1048576 です。

	コマンドまたはアクション	目的
ステップ 10	**logging ip access-list cache threshold** *threshold* 例： `switch(config)# logging ip access-list cache threshold 490`	アラート期限が切れる前に、指定されたパケット数がログ記録された段階で、Syslog メッセージが生成されます。
ステップ 11	**logging ip access-list detailed** 例： `switch(config)# logging ip access-list detailed`	**show logging ip access-list cache** コマンドの出力で表示される次の情報を有効にします。アクセス制御エントリ（ACE）シーケンス番号、ACE アクション、ACL名、ACL方向、ACLフィルタタイプ、およびACL適用インターフェイス。
ステップ 12	**hardware rate-limiter access-list-log** パケット 例： `switch(config)# hardware rate-limiter access-list-log 200`	ACLロギングのためにスーパーバイザモジュールにコピーされるパケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 13	**acllog match-log-level** *severity-level* 例： `switch(config)# acllog match-log-level 5`	ACLの一致を記録する最小シビラティ（重大度）レベルを指定します。デフォルトは 6（情報）です。範囲は 0（緊急）～ 7（デバッグ）です。
ステップ 14	（任意） **show logging ip access-list cache** [**detail**] 例： `switch(config)# show logging ip access-list cache`	送信元 IP および接続先 IP アドレス、送信元ポートおよび接続先ポート情報、送信元インターフェイスなど、アクティブなログフローに関する情報を表示します。アクティブなフローのその他の情報では、特にサポートされていないすべてのオプションは表示されません。 **logging ip access-list detailed** コマンドを入力すると、出力には、アクセスコントロールエントリ（ACE）のシーケンス番号、ACEのアクション、ACLの名前、ACL の方向、ACL のフィルタ タイプ、およびACLの適用インターフェイスの情報も含まれます。

要求をリダイレクトするための HTTP メソッドによる ACL の設定

特定のHTTPメソッドを代行受信し、特定のポートに接続されているサーバにリダイレクトするように ACL を設定できます。

次の HTTP メソッドをリダイレクトできます。

- connect
- delete
- get
- head
- post
- put
- トレース

始める前に

hardware access-list tcam region ifacl 512 double-wide コマンドを使用して、IFACL 領域の倍幅 TCAM を有効にします。このコマンドは、グローバル コンフィギュレーションに適用されます。この設定を有効にするには、スイッチをリロードします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**ip access-list** *name*
	例：
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。*name* 引数は 64 文字以内で指定します。

ステップ 3	[*sequence-number*] **permit** *protocol source destination* **http-method** *method* [**tcp-option-length** *length*] [**redirect** *interface*] 例： `switch(config-acl)# permit tcp 1.1.1.1/32 any http-method get`	特定の HTTP メソッドをサーバにリダイレクトするように ACL を設定します。 次の HTTP メソッドがサポートされています。 • connect：CONNECT メソッド [0x434f4e4e] で HTTP パケットを照合します。

	コマンドまたはアクション	目的
		• delete：DELETE メソッド [0x44454c45] で HTTP パケットを照合します。 • get：GET メソッド [0x47455420] で HTTP パケットを照合します。 • head：HEAD メソッド [0x48454144] で HTTP パケットを照合します。 • post：POST メソッド [0x504f5354] で HTTP パケットを照合します。 • put：PUT メソッド [0x50555420] で HTTP パケットを 照合します。 • trace：TRACE メソッド [0x54524143] で HTTP パケットを照合します。 **tcp-option-length** オプションは、パケット内の TCP オプション ヘッダーの長さを指定します。アクセス コントロール エントリ（ACE）には、最大 4 つの TCP オプション長（4 バイトの倍数）を設定できます。長さの範囲は 0 ～ 40 です。このオプションを設定しない場合、長さは 0 に指定され、TCP オプション ヘッダーのないパケットだけが ACE と一致します。このオプションを使用すると、可変長 TCP オプション ヘッダーを持つパケットでも HTTP 方式を照合できます。 **リダイレクト** オプションは、特定のポートに接続されているサーバに HTTP メソッドをリダイレクトします。HTTP リダイレクト機能は、レイヤ 3 ポートでは機能しません。
ステップ 4	（任意） **show ip access-lists** *name* **例**： `switch(config-acl)# show ip access-lists acl-01`	IP ACL の設定を表示します。
ステップ 5	（任意） **show run interface** *interface slot/port*	インターフェイスの設定を表示します。

	コマンドまたはアクション	目的
	例： `switch(config-acl)# show run interface ethernet 2/2`	

例

次の例では、パケットの TCP オプション ヘッダーの長さを指定し、ポート チャネル 4001 に接続されているサーバに post HTTP メソッドをリダイレクトします。

```
switch(config)# ip access-list http-redirect-acl
switch(config-acl)# 10 permit tcp any any http-method get tcp-option-length 4 redirect
port-channel4001
switch(config-acl)# 20 permit tcp any any http-method post redirect port-channel4001
switch(config-acl)# statistics per-entry
switch(config)# interface Ethernet 1/33
switch(config-if)# ip port access-group http-redirect-acl in
```

IP ACL の設定の確認

IP ACL の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show hardware access-list tcam region	デバイスで次のリロード時に適用される TCAM サイズを表示します。
show ip access-lists	IPv4 ACL の設定を表示します。
show ipv6 access-lists	IPv6 ACL の設定を表示します。
show logging ip access-list cache [**detail**]	送信元IPおよび宛先IPアドレス、送信元ポートおよび宛先ポート情報、送信元インターフェイスなど、アクティブなログフローに関する情報を表示します。アクティブなフローのその他の情報では、特にサポートされていないすべてのオプションは表示されません。

コマンド	目的
show logging ip access-list status	拒否フローの最大数、現在の有効なログ間隔、と現在の有効なしきい値を表示します。
show running-config acllog	ACL のログ実行設定を表示します。
show running-config aclmgr [**all**]	IP ACL の設定および IP ACL が適用されるインターフェイスを含めて、ACL の実行コンフィギュレーションを表示します。 **Note** このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config acllog	ACL のログスタートアップ設定を表示します。
show startup-config aclmgr [**all**]	ACL のスタートアップ コンフィギュレーションを表示します。 **Note** このコマンドは、スタートアップコンフィギュレーションのユーザ設定 ACL を表示します。**all** オプションを使用すると、スタートアップコンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

IP ACL の統計情報のモニタリングとクリア

IP ACL の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドのいずれかを使用します。

コマンド	目的
show ip access-lists	IPv4 ACL の設定を表示します。IPv4 ACL に **statistics per-entry** コマンドが含まれている場合は、**show ip access-lists** コマンドの出力に、各ルールと一致したパケットの数が含まれます。
show ipv6 access-lists	IPv6 ACL の設定を表示します。IPv6 ACL に **statistics per-entry** コマンドが含まれている場合は、**show ipv6 access-lists** コマンドの出力に、各ルールと一致したパケットの数が含められます。
clear ip access-list counters	すべての IPv4 ACL または特定の IPv4 ACL の統計情報をクリアします。
clear ipv6 access-list counters	すべての IPv6 ACL または特定の IPv6 ACL の統計情報をクリアします。

IP ACL の設定例

acl-01 という名前の IPv4 ACL を作成し、これをポート ACL としてイーサネット インターフェイス 2/1（レイヤ 2 インターフェイス）に適用する例を示します。

```
ip access-list acl-01
  permit ip 192.168.2.0/24 any
interface ethernet 2/1
  ip port access-group acl-01 in
```

acl-120 という名前の IPv6 ACL を作成し、これをルータ ACL としてイーサネット インターフェイス 2/3（レイヤ 3 インターフェイス）に適用する例を示します。

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

次に、single-source という名前の VTY ACL を作成し、それを VTY 回線上の入力 IP トラフィックに対して適用する例を示します。この ACL は、通過するすべての TCP トラフィックを許可し、その他のすべての IP トラフィックをドロップします。

```
ip access-list single-source
  permit tcp 192.168.7.5/24 any
  exit
```

```
line vty
ip access-class single-source in
show ip access-lists
```

次に、IPv4 ACL ロギングの設定例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list logging-test
switch(config-acl)# permit ip any 2001:DB8:1::1/64 log
switch(config-acl)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ip access-group logging-test in
switch(config-if)# exit
switch(config)# logging ip access-list cache interval 400
switch(config)# logging ip access-list cache entries 100
switch(config)# logging ip access-list cache threshold 900
switch(config)# hardware rate-limiter access-list-log 200
switch(config)# acllog match-log-level 5
```

システム ACL について

システム ACL の設定については、次の注意事項と制限事項を参照してください。

- システム PACL は、レイヤ 2 インターフェイスでのみサポートされます。
- IPv4 PACL TCAM リージョン（ifacl）を -R ライン カードの合計物理 TCAM 容量（12k）よりも多く設定すると、-R ライン カードのみの電源が切断されます。
- ACE 統計情報は、システム ACL ではまだサポートされていません。
- IPv6 は、システム ACL ではまだサポートされていません。
- システム ACL は、ブレークアウト ポートではサポートされません。
- -R シリーズ ラインカードを搭載した Cisco Nexus シリーズ スイッチでの Quality of Service、ACL、または TCAM カービング設定については、『Cisco Nexus 3600 NX-OS Quality of Service 設定ガイド、リリース 7.x』を参照してください。

TCAM リージョンの分割

システム ACL を設定する前に、まず TCAM リージョンを分割します。1k 未満の ACL を設定する場合は、TCAM リージョンを分割する必要がないことに注意してください。詳細については、「ACL TCAM リージョン サイズの設定 （30 ページ）」を参照してください。

システム ACL の設定

IPv4 ACL を作成したら、システム ACL を設定します。

始める前に

デバイスで IPv4 ACL を作成します。詳細については、「IP ACL の作成 （23 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**config t**	コンフィギュレーション モードを開始します。
ステップ 2	**system acl**	システムACLを設定します。
ステップ 3	**ip port access-group** <*pacl name*> **in**	インターフェイスにレイヤ 2 PACL を適用します。ポート ACL では、インバウンド フィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。

システム ACL の設定および show コマンドの例

システム ACL のshowコマンドについては、次の設定例を参照してください。

1K スケールのシステム PACL の設定（デフォルト TCAM を使用）

1K スケールのシステム PACL の設定については、次の例を参照してください（デフォルト TCAM を使用）。

ステップ 1：PACL を作成します。

```
config t
ip access-list PACL-DNA
    10 permit ip 1.1.1.1/32 any
    20 permit tcp 3.0.0.0/8 255.0.0.0 eq 1500
    25 deny udp any any eq 500
    26 deny tcp any eq 490 any
    …·· …·

    1000 deny any any
```

ステップ 2：PACL をシステム レベルに適用します。

```
configuration terminal
system acl
    ip port access-group PACL-DNA in
```

スイッチに設定されているシステム ACLを検証するには、**sh run aclmgr | sec system** コマンドを使用します。

```
switch# sh run aclmgr | sec system
```

```
system acl
 ip port access-group test in
switch#
```

スイッチに設定されている PACL を検証するには、**sh ip access-lists <name> [summary]** コマンドを使用します。

```
switch# sh ip access-lists test

IP access list test
        10 deny udp any any eq 27
        20 permit ip 1.1.1.1/32 100.100.100.100/32
        30 permit ip 1.2.1.1/32 100.100.100.100/32
        40 permit ip 1.3.1.1/32 100.100.100.100/32
        50 permit ip 1.4.1.1/32 100.100.100.100/32
        60 permit ip 1.5.1.1/32 100.100.100.100/32
        70 permit ip 1.6.1.1/32 100.100.100.100/32
        80 permit ip 1.7.1.1/32 100.100.100.100/32
        90 permit ip 1.8.1.1/32 100.100.100.100/32

switch# sh ip access-lists test summary
IPV4 ACL test
        Total ACEs Configured: 12279
        Configured on interfaces:
        Active on interfaces:
                - ingress
                - ingress

switch#
```

PACL IPv4（ifacl）TCAMリージョン サイズを検証するには、**show hardware access-list tcam region** コマンドを使用します。

```
switch# show hardware access-list tcam region
*********************************WARNING*********************************
*****************The output shows NFE tcam region info******************
***Please refer to 'show hardware access-list tcam template' for NFE2***
*************************************************************************
                              IPV4 PACL [ifacl] size = 12280
                          IPV6 PACL [ipv6-ifacl] size =    0
                            MAC PACL [mac-ifacl] size =    0
                             IPV4 Port QoS [qos] size =  640
                        IPV6 Port QoS [ipv6-qos] size =  256
                          MAC Port QoS [mac-qos] size =    0
                       FEX IPV4 PACL [fex-ifacl] size =    0
                   FEX IPV6 PACL [fex-ipv6-ifacl] size =    0
                     FEX MAC PACL [fex-mac-ifacl] size =    0
                      FEX IPV4 Port QoS [fex-qos] size =    0
                  FEX IPV6 Port QoS [fex-ipv6-qos] size =    0
                    FEX MAC Port QoS [fex-mac-qos] size =    0
                                IPV4 VACL [vacl] size =    0
                            IPV6 VACL [ipv6-vacl] size =    0
                              MAC VACL [mac-vacl] size =    0
                             IPV4 VLAN QoS [vqos] size =    0
                         IPV6 VLAN QoS [ipv6-vqos] size =    0
                           MAC VLAN QoS [mac-vqos] size =    0
                                IPV4 RACL [racl] size =    0
                            IPV6 RACL [ipv6-racl] size =  128
                   IPV4 Port QoS Lite [qos-lite] size =    0
              FEX IPV4 Port QoS Lite [fex-qos-lite] size =    0
```

```
                    IPV4 VLAN QoS Lite [vqos-lite] size =    0
                     IPV4 L3 QoS Lite [l3qos-lite] size =    0
                           Egress IPV4 QoS [e-qos] size =    0
                      Egress IPV6 QoS [e-ipv6-qos] size =    0
                        Egress MAC QoS [e-mac-qos] size =    0
                           Egress IPV4 VACL [vacl] size =    0
                      Egress IPV6 VACL [ipv6-vacl] size =    0
                        Egress MAC VACL [mac-vacl] size =    0
                         Egress IPV4 RACL [e-racl] size =    0
                    Egress IPV6 RACL [e-ipv6-racl] size =    0
                Egress IPV4 QoS Lite [e-qos-lite] size =    0
                             IPV4 L3 QoS [l3qos] size =  640
                       IPV6 L3 QoS [ipv6-l3qos] size =  256
                         MAC L3 QoS [mac-l3qos] size =    0
                                  Ingress System size =    0
                                   Egress System size =    0
                                     SPAN [span] size =   96
                                Ingress COPP [copp] size =  128
                     Ingress Flow Counters [flow] size =    0
switch#
```

ACL 関連のテクニカル サポート情報を表示するには、**show tech-support aclmgr** および **show tech-support aclqos** コマンドを使用します。

```
show tech-support aclmgr
show tech-support aclqos
```

オブジェクト グループの設定

IPv4 ACL および IPv6 ACL のルールに送信元と宛先のアドレスおよびプロトコル ポートを指定する際に、オブジェクト グループを使用できます。

オブジェクト グループに対する Session Manager のサポート

Session Manager はオブジェクト グループの設定をサポートしています。この機能を使用すると、設定セッションを作成し、オブジェクト グループの設定変更を実行コンフィギュレーションにコミットする前に確認できます。Session Manager の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

IPv4 アドレス オブジェクト グループの作成および変更

IPv4 アドレス グループ オブジェクトの作成および変更を実行できます。

Note Cisco Nexus リリース 7.0(3)I5(2) 以降では、**no host IPv4-address** コマンドはサポートされていません。DME サポートでは、no sequence コマンドを使用しない削除はサポートされていません。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**object-group ip address** *name*
	Example:
	`switch(config)# object-group ip address ipv4-addr-group-13`
	`switch(config-ipaddr-ogroup)#`
		IPv4 アドレス オブジェクト グループを作成し、IPv4 アドレス オブジェクト グループ コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。 • [*sequence-number*] **host** *IPv4-address* • [*sequence-number*] *IPv4-address*/*prefix-len* • [*sequence-number*] *IPv4-address network-wildcard* **Example:** `switch(config-ipaddr-ogroup)# host 10.99.32.6`	オブジェクト グループのエントリを作成します。作成するエントリごとに、**host** コマンドを使用して単一のホストを指定するか、または **host** コマンドを省略してホストのネットワークを指定します。 IPv4 オブジェクト グループのプレフィックス長を指定できます。これは、最初の連続ビットでのみ一致します。または、アドレスの任意のビットで一致するワイルドカード マスクを指定できます。
ステップ 4	次のいずれかのコマンドを入力します。 • **no** [*sequence-number*] • **no host** *IPv4-address* • **no** *IPv4-address*/*prefix-len* • **no** *IPv4-address network-wildcard* **Example:** `switch(config-ipaddr-ogroup)# no host 10.99.32.6`	オブジェクト グループのエントリを削除します。オブジェクト グループから削除するエントリごとに、**no** 形式の **host** コマンドを使用します。
ステップ 5	(Optional) **show object-group** *name* **Example:** `switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13`	オブジェクト グループの設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-ipaddr-ogroup)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IPv6 アドレス オブジェクト グループの作成および変更

IPv6 アドレス グループ オブジェクトの作成および変更を実行できます。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**object-group ipv6 address** *name*
	Example:
	`switch(config)# object-group ipv6 address ipv6-addr-group-A7`
	`switch(config-ipv6addr-ogroup)#`
		IPv6 アドレス オブジェクト グループを作成し、IPv6 アドレス オブジェクト グループ コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。 • [*sequence-number*] **host** *IPv6-address* • [*sequence-number*] *IPv6-address*/*prefix-len* **Example:** `switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1`	オブジェクト グループのエントリを作成します。作成するエントリごとに、**host** コマンドを使用して単一のホストを指定するか、または **host** コマンドを省略してホストのネットワークを指定します。 IPv6 オブジェクト グループのプレフィックス長を指定できます。これは、最初の連続ビットでのみ一致します。
ステップ 4	次のいずれかのコマンドを入力します。 • **no** *sequence-number* • **no host** *IPv6-address* • **no** *IPv6-address*/*prefix-len* **Example:** `switch(config-ipv6addr-ogroup)# no host 2001:db8:0:3ab0::1`	オブジェクト グループからエントリを削除します。オブジェクト グループから削除するエントリごとに、**no** 形式の **host** コマンドを使用します。
ステップ 5	(Optional) **show object-group** *name* **Example:** `switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7`	オブジェクト グループの設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-ipv6addr-ogroup)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

プロトコル ポート オブジェクト グループの作成および変更

プロトコル ポート オブジェクト グループの作成および変更を実行できます。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**object-group ip port** *name*
	Example:
	`switch(config)# object-group ip port NYC-datacenter-ports`
	`switch(config-port-ogroup)#`
		プロトコル ポート オブジェクト グループを作成し、ポート オブジェクト グループ コンフィギュレーション モードを開始します。

ステップ 3	[*sequence-number*] *operator port-number* [*port-number*] **Example:** `switch(config-port-ogroup)# eq 80`	オブジェクト グループのエントリを作成します。作成するエントリごとに、次の演算子コマンドを 1 つ使用します。 • **eq**：指定したポート番号に一致だけます。 • **gt**：指定したポート番号より大きい（等しいものは含まない）ポート番号に一致します。 • **lt**：指定したポート番号より小さい（等しいものは含まない）ポート番号に一致します。 • **neq**：指定したポート番号以外のすべてのポート番号に一致します。 • **range**：指定した 2 つのポート番号と、その間の範囲のポート番号に一致します。 **Note** **range** コマンドだけは、2 つの *port-number* 引数を必要とします。
ステップ 4	**no** {*sequence-number* | *operator port-number* [*port-number*]} **Example:** `switch(config-port-ogroup)# no eq 80`	オブジェクト グループからエントリを削除します。削除するエントリごとに、該当する演算子コマンドを **no** f形式で使用します。

	Command or Action	Purpose
ステップ 5	(Optional) **show object-group** *name* **Example:** `switch(config-port-ogroup)# show object-group NYC-datacenter-ports`	オブジェクト グループの設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-port-ogroup)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

オブジェクト グループの削除

IPv4 アドレス オブジェクト グループ、IPv6 アドレス オブジェクト グループ、またはプロトコル ポート オブジェクト グループを削除できます。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します
ステップ 2	**no object-group** {**ip address** | **ipv6 address** | **ip port**} *name* **Example:** `switch(config)# no object-group ip address ipv4-addr-group-A7`	指定のオブジェクト グループを削除します。
ステップ 3	(Optional) **show object-group** **Example:** `switch(config)# show object-group`	すべてのオブジェクト グループを表示します。削除されたオブジェクトグループは表示されません。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

オブジェクト グループの設定の確認

オブジェクト グループの設定情報を表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
show object-group	オブジェクト グループの設定を表示します。
show {**ip** | **ipv6**} **access-lists** *name* [**expanded**]	ACL設定の拡張統計情報を表示します。
show running-config aclmgr	オブジェクト グループを含めて、ACL の設定を表示します。

時間範囲の設定

時間範囲の Session Manager サポート

Session Manager は時間範囲の設定をサポートしています。この機能を使用すると、設定セッションを作成し、時間範囲の設定変更を実行コンフィギュレーションにコミットする前に確認できます。Session Manager の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

時間範囲の作成

デバイス上で時間範囲を作成し、これにルールを追加できます。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**time-range** *name*
	Example:
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		時間範囲を作成し、時間範囲コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 3	(Optional) [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **Example:** `switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59`	指定開始日時と終了日時の間（両端を含める）の 1 日以上の連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	(Optional) [*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **Example:** `switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00`	*list-of-weekdays* 引数で指定された曜日の、指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。*list-of-weekdays* 引数の値には次のキーワードも使用できます。 • **daily** ：1 週間のすべての曜日 • **weekdays** ：月曜日から金曜日まで • **weekend** ：土曜日から日曜日まで
ステップ 5	(Optional) [*sequence-number*] **absolute start** *time date* [**end** *time date*] **Example:** `switch(config-time-range)# absolute start 1:00 15 march 2013`	**start** キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。**end** キーワードを省略した場合、そのルールは開始日時を過ぎると常に有効になります。
ステップ 6	(Optional) [*sequence-number*] **absolute** [start *time date*] **end** *time date* **Example:** `switch(config-time-range)# absolute end 23:59:59 31 may 2013`	**end** キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。**start** キーワードを省略すると、そのルールは終了日時を過ぎるまでずっと有効です。
ステップ 7	(Optional) **show time-range** *name* **Example:** `switch(config-time-range)# show time-range workday-daytime`	時間範囲の設定を表示します。
ステップ 8	(Optional) **copy running-config startup-config** **Example:** `switch(config-time-range)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲の変更

既存の時間範囲のルールの追加および削除を実行できます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**time-range** *name*
	Example:
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		特定の時間範囲の時間範囲コンフィギュレーション モードを開始します。

ステップ 3	(Optional) [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **Example:** `switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59`	指定開始日時と終了日時の間（両端を含める）の 1 日以上の連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	(Optional) [*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **Example:** `switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00`	*list-of-weekdays* 引数で指定された曜日の、指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。*list-of-weekdays* 引数の値には次のキーワードも使用できます。 • **daily** ：1 週間のすべての曜日 • **weekdays** ：月曜日から金曜日まで • **weekend** ：土曜日から日曜日まで
ステップ 5	(Optional) [*sequence-number*] **absolute start** *time date* [**end** *time date*] **Example:** `switch(config-time-range)# absolute start 1:00 15 march 2013`	**start** キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。**end** キーワードを省略した場合、そのルールは開始日時を過ぎると常に有効になります。
ステップ 6	(Optional) [*sequence-number*] **absolute** [**start** *time date*] **end** *time date* **Example:** `switch(config-time-range)# absolute end 23:59:59 31 may 2013`	**end** キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。**start** キーワードを省略すると、そのルールは終了日時を過ぎるまでずっと有効です。

	Command or Action	Purpose
ステップ 7	(Optional) **no** {*sequence-number* | **periodic** *arguments* . . . | **absolute** *arguments*. . . } **Example:** `switch(config-time-range)# no 80`	時間範囲から特定のルールを削除します。
ステップ 8	(Optional) **show time-range** *name* **Example:** `switch(config-time-range)# show time-range workday-daytime`	時間範囲の設定を表示します。
ステップ 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-time-range)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

時間範囲のシーケンス番号の変更 （67 ページ）

時間範囲の削除

デバイスから時間範囲を削除できます。

Before you begin

その時間範囲が ACL ルールのいずれかに使用されているかどうかを確認します。削除できるのは、ACL ルールに使用されている時間範囲です。ACL ルールに使用されている時間範囲を削除しても、その ACL が適用されているインターフェイスの設定には影響しません。デバイスは削除された時間範囲を使用する ACL ルールを空であると見なします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**no time-range** *name* **Example:** `switch(config)# no time-range daily-workhours`	名前を指定した時間範囲を削除します。

	Command or Action	Purpose
ステップ 3	(Optional) **show time-range** **Example:** `switch(config-time-range)# show time-range`	すべての時間範囲の設定を表示します。削除された時間範囲は表示されません。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲のシーケンス番号の変更

時間範囲のルールに割り当てられているすべてのシーケンス番号を変更できます。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**resequence time-range** *name starting-sequence-number increment*
	Example:
	`switch(config)# resequence time-range daily-workhours 100 10`
	`switch(config)#`
		時間範囲のルールにシーケンス番号を割り当てます。指定した開始シーケンス番号は最初のルールに割り当てられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。

ステップ 3	(Optional) **show time-range** *name* **Example:** `switch(config)# show time-range daily-workhours`	時間範囲の設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲設定の確認

時間範囲の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show time-range	時間範囲の設定を表示します。
show running-config aclmgr	すべての時間範囲を含めて、ACL の設定を表示します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。