テンプレート ACL の設定

ユーザー プロファイルが RADIUS 属性 242 またはベンダー固有属性（VSA ）Cisco AVPairs を使用して設定されると、同様のユーザーごとのアクセス コントロール リスト（ACL）は、単一のテンプレート ACL に置き換えられることがあります。つまり、1 つの ACL で多数の類似した ACL を表します。IPv6 テンプレート ACL を使用することで、ACL をサポートするために必要なメモリおよび Ternary Content Addressable Memory（TCAM）リソースを最小限に抑えながら、1 ユーザーあたりの ACL の合計数を増やすことができます。

各サブスクライバが独自の ACL を所有するネットワークでは、ユーザーの IP アドレスを除いて、ACL をユーザーごとに同じとするのが普通です。テンプレート ACL 機能は、システム リソースを節約する 1 つの ACL に多くの一般的なアクセス コントロール要素（ACE ）で ACL をグループ化します。

- テンプレート ACL の前提条件 （1 ページ）
- テンプレート ACL の制約事項 （1 ページ）
- テンプレート ACL の設定に関する情報 （2 ページ）
- テンプレート ACL の設定方法 （6 ページ）
- テンプレート ACL の設定例 （7 ページ）
- その他の参考資料 （9 ページ）
- ACL テンプレートに関する機能情報 （10 ページ）

テンプレート ACL の前提条件

- Cisco ASR 1000 シリーズ ルータ
- Cisco IOS XE リリース 2.4 以降のリリース

テンプレート ACL の制約事項

テンプレート ACL は、RADIUS 属性 242 または VSA Cisco-AVPairs（ip:inacl/outacl）を通じて設定されたユーザーごとの ACL に対してのみ有効になります。その他のタイプの ACL は、テンプレート ACL 機能によって処理されません。

テンプレート ACL 機能は、IPv4 ACL でのみ使用できます。

テンプレート ACL 機能は、ユーザーごとの ACL の次のタイプには利用はできません。

- 時間ベース ACL
- ダイナミック ACL
- 評価 ACL
- 再帰 ACL
- ISG IP セッションで設定された ACL
- IPv6 ACL

テンプレート ACL 機能の無効化

テンプレート ACL 機能を無効にすると、システムは、すべての既存のテンプレート ACL インスタンスを ACL と置き換えます。システムに必要な数の ACL を設定するための十分なリソース（具体的には、TCAM リソース）がない場合、システムは、エラー メッセージを生成し、テンプレート ACL 機能を無効にする要求は失敗します。

テンプレート ACL の設定に関する情報

テンプレート ACL 機能設計

サービス プロバイダーが、AAA サーバーを使用して、RADIUS 属性 242 または Cisco VSA AVPairs を使用する、権限のあるセッションに対する ACL を設定する場合、セッション数は、システムで許容される最大の ACL 数を簡単に上回ります。

各サブスクライバが ACL を有するネットワークでは、ユーザーの IP アドレスを除いて、ACL が各ユーザーに対して同じになることは普通です。テンプレート ACL は、システム リソースを高速で編集し、多くの共通 ACE を持つ ACL を節約する 1 つの ACL にグループ化することで、この問題を軽減します。

テンプレート ACL 機能は、デフォルトで有効になっており、RADIUS 属性 242 または Cisco VSA AVPairs VSA を使用した ACL 設定は、テンプレート ステータスの対象となります。

テンプレート ACL 機能を有効にすると、システムは、すべての設定済みセッション単位の ACL をスキャンおよび評価して、必要なテンプレート ACL を作成します。

テンプレート ACL の無効化

テンプレート ACL 機能を無効にすると、システムは、すべての既存のテンプレート ACL インスタンスを ACL と置き換えます。システムに必要な数の ACL を設定するための十分なリソース（特に TCAM リソース）がない場合、システムは、エラー メッセージを生成し、テンプレート ACL 機能を無効にする要求が失敗します。

そのため、テンプレート ACL 機能を無効にする前に、**show access-list template summary** コマンドを使用して、システム内のテンプレート ACL の数を表示し、この数がシステムの制限を超えているかを確認します。

テンプレート ACL 機能を無効にすると、新しい ACL は、テンプレーティングの対象にはなりません。

複数の ACL

テンプレート ACL 機能を有効にすると、システムは、2 ユーザーごとの ACL が類似している場合を特定し、2 つのユーザーごとの ACL を 1 つのテンプレート ACL に統合します。

たとえば、次の例は、2 人の個別のユーザーに対する 2 つの ACL を示します。

```
ip access-list extended Virtual-Access1.1#1 (PeerIP: 10.1.1.1)
permit igmp any host 10.1.1.1
permit icmp host 10.1.1.1 any
deny ip host 10.31.66.36 host 10.1.1.1
deny tcp host 10.1.1.1 host 10.31.66.36
permit udp any host 10.1.1.1
permit udp host 10.1.1.1 any
permit udp any host 192.168.2.1
permit udp any host 192.168.222.1
permit icmp host 10.55.15.4 host 192.168.2.1
permit udp 10.22.11.0 0.0.0.255 host 192.168.211.2
permit tcp any host 192.168.222.1
permit ip host 10.55.15.4 host 192.168.2.1
permit tcp 10.22.11.0 0.0.0.255 host 192.168.211.2
ip access-list extended Virtual-Access1.1#2 (PeerIP: 10.13.11.2)
permit igmp any host 10.13.11.2
permit icmp host 10.13.11.2 any
deny ip host 10.31.66.36 host 10.13.11.2
deny tcp host 10.13.11.2 host 10.31.66.36
permit udp any host 10.13.11.2
permit udp host 10.13.11.2 any
permit udp any host 192.168.2.1
permit udp any host 192.168.222.1
permit icmp host 10.55.15.4 host 192.168.2.1
permit udp 10.22.11.0 0.0.0.255 host 192.168.211.2
permit tcp any host 192.168.222.1
permit ip host 10.55.15.4 host 192.168.2.1
permit tcp 10.22.11.0 0.0.0.255 host 192.168.211.2
```

テンプレート ACL 機能を有効にすると、システムは、これら 2 つの ACL が類似していることを認識し、次のように、テンプレート ACL を作成します。

```
ip access-list extended Template_1
permit igmp any host <PeerIP>
permit icmp host <PeerIP> any
deny ip host 10.31.66.36 host <PeerIP>
deny tcp host <PeerIP> 10.31.66.36
permit udp any host <PeerIP>
permit udp host <PeerIP> any
permit udp any host 192.168.2.1
permit udp any host 192.168.222.1
permit icmp host 10.55.15.4 host 192.168.2.1
permit udp 10.22.11.0 0.0.0.255 host 192.168.211.2
permit tcp any host 192.168.222.1
```

```
permit ip host 10.55.15.4 host 192.168.2.1
permit tcp 10.22.11.0 0.0.0.255 host 192.168.211.2
```

この例では、ピアの IP アドレスは次のように関連付けられています。

- Virtual-Access1.1#1 10.1.1.1
- Virtual-Access1.1#2 10.13.11.2

2 つの ACL は、1 つのテンプレート ACL に統合され、次のように参照されます。

Template_1(10.1.1.1) への Virtual-Access1.1#1 マップ

Template_1(10.13.11.2) への Virtual-Access1.1#2 マップ

VSA Cisco-AVPairs

テンプレート ACL 処理は、Cisco-AVPairs を使用して設定される ACL に対して発生します。ACL 番号を使用して定義される AVPairs のみが、テンプレーティングプロセスの対象になります。

テンプレーティングの対象となるために、入力 ACL のための AVPairs は、次の形式に従う必要があります。

ip:inacl#number={standard-access-control-list | extended-access-control-list}

例：ip:inacl#10=deny ip any 10.13.16.0 0.0.0.255

テンプレーティングの対象になるためには、出力 ACL のための AVPairs は、次の形式に従う必要があります:

ip:outacl#number={standard-access-control-list | extended-access-control-list}

例：ip:outacl#200=permit ip any any

Cisco-AVPairs の詳細については、『Cisco IOS ISG RADIUS CoA インターフェイス ガイド』の「Cisco ベンダー固有 AVPair Attributes」のセクションを参照してください。

RADIUS 属性 242

RADIUS 属性 242 を使用して設定される ACL に対して、テンプレート ACL 処理が発生します。属性 242 は、IP データ フィルタに対して、次の形式があります。

Ascend-Data-Filter = “ip <dir> <action> [dstip <dest_ipaddr\subnet_mask>] [srcp <src_ipaddr\subnet_mask>] [<proto> [dstport <cmp> <value>] [srcport <cmp> <value>] [<est>]]”

次の表で、IP データ フィルタの属性 242 エントリ内の要素について説明します。

表 *1: IP* データ フィルタ構文要素

要素	説明
ip	IP アドレスを指定します。

要素	説明
<dir>	フィルタの方向を指定します。有効値は、**in**（ルータに着信するパケットのフィルタリング）または、**out**（ルータから発信するパケットのフィルタリング）です。
<action>	ルータがフィルタに一致したパケットに取るべきアクションを指定します。有効な値は **forward** または **drop** です。
dstip <dest_ipaddr\subnet_mask>	宛先 IP アドレス フィルタリングを有効にします。宛先アドレスが **<dest_ipaddr>** の値に一致するパケットに適用されます。アドレスのサブネット マスクの部分が存在する場合、ルータはマスクされたビットのみを比較します。0.0.0.0 に **<dest_ipaddr>** を設定するか、またはこのキーワードがなければ、フィルタは、すべての IP パケットに一致します。
srcp<src_ipaddr\subnet_mask>	送信元 IP アドレス フィルタリングを有効にします。送信元アドレスが **<src_ipaddr>** の値に一致するパケットに適用されます。アドレスのサブネット マスクの部分が存在する場合、ルータはマスクされたビットのみを比較します。0.0.0.0 に **<src_ipaddr>** を設定するか、またはこのキーワードがなければ、フィルタは、すべての IP パケットに一致します。
<proto>	名前または番号として指定するプロトコルを指定します。プロトコル フィールドがこの値に一致するパケットに適用されます。使用できる名前と番号は **icmp**（**1**）、**tcp**（**6**）、**udp**（**17**）、および **ospf**（**89**）です。この値をゼロ（0）に設定すると、フィルタは、一切のプロトコルに一致します。
dstport <cmp> <value>	宛先ポートフィルタリングを有効にします。このキーワードは、**<proto>** が **tcp**（**6**）または **udp**（**17**）に設定されている場合に限り有効です。宛先ポートを指定しないと、フィルタは、一切のポートと一致します。 **<cmp>** は、指定された **<value>** と実際の宛先ポートとを比較する方法を定義します。この値として **<**、**=**、**>**、または **!** を使用できます。 **<value>** 名前も番号も使用可能です。使用できる名前と番号は **ftp-data (20)**、**ftp (21)**、**telnet (23)**、**nameserver (42)**、**domain (53)**、**tftp (69)**、**gopher (70)**、**finger (79)**、**www (80)**、**kerberos (88)**、**hostname (101)**、**nntp (119)**、**ntp (123)**、**exec (512)**、**login (513)**、**cmd (514)**、および **talk (517)** です。
srcport <cmp> <value>	送信元ポートフィルタリングを有効にします。このキーワードは、**<proto>** が **tcp**（**6**）または **udp**（**17**）に設定されている場合に限り有効です。送信元ポートを指定しないと、フィルタは、一切のポートと一致します。 **<cmp>** は、指定された **<value>** と実際の宛先ポートとを比較する方法を定義します。この値として **<**、**=**、**>**、または **!** を使用できます。 **<value>** 名前も番号も使用可能です。使用できる名前と番号は **ftp-data**（**20**）、**ftp**（**21**）、**telnet**（**23**）、**nameserver**（**42**）、**domain**（**53**）、**tftp**（**69**）、**gopher**（**70**）、**finger**（**79**）、**www**（**80**）、**kerberos**（**88**）、**hostname**（**101**）、**nntp**（**119**）、**ntp**（**123**）、**exec**（**512**）、**login**（**513**）、**cmd**（**514**）、および **talk**（**517**）です。

要素	説明
<est>	1 に設定すると、TCP セッションがすでに確立されている場合にのみ、パケット フィルタと一致していると指定します。この引数は、**<proto>** が **tcp (6)** に設定されている場合に限り有効です。

「RADIUS 属性 242 IP データ フィルタ エントリ」は、4 つの属性 242 IP データフィルタエントリを示します。

RADIUS 属性 242 IP データフィルタエントリ

```
Ascend-Data-Filter=”ip in drop”
Ascend-Data-Filter=”ip out forward tcp”
Ascend-Data-Filter=”ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16
dstport!=telnet”
Ascend-Data-Filter=”ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16 icmp”
```

テンプレート ACL の設定方法

ACL が RADIUS 属性 242 または VSA Cisco-AVPairs を使用して設定されると、ACL は、デフォルトでは有効になりません。

テンプレート ACL の最大サイズの設定

デフォルトでは、テンプレートの ACL ステータスは 100 台以下のルールの ACL に限定されます。ただし、この制限を低い値に設定できます。テンプレート ACL とみなされるため、既存の ACL は、以下のようなルールの最大数を設定するには、このセクションの手順を実行してください:

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list template** *number*
4. **exit**
5. **show access-list template summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**access-list template** *number* 例： `Router(config)# access-list template 50`	テンプレート ACL の処理をイネーブルにします。 指定された数のルール（またはより少ないルール）の ACL だけがテンプレートのステータスの対象となります。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル 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	**show access-list template summary** 例： `Router# show access-list template summary`	（任意）ACL テンプレートに関する要約情報が表示されます。

トラブルシューティングのヒント

次のコマンドを使用すると、テンプレート ACL をトラブルシューティングできます。

- **show access-list template**
- show platform hardware qfp active classification class-group-manager class-group client acl all
- **show platform hardware qfp active feature acl** {**control** | **node** *acl-node-id*}
- show platform software access-list

テンプレート ACL の設定例

テンプレート ACL の最大サイズの例

次の例では、テンプレートのステータスを 50 と対象するために ACL が含むことができるルールの最大数の設定方法を示しています。ルールの数は同じか、または 50 よりも少ない ACL のみがテンプレート ステータスの対象となります。

```
Router> enable

Router# configure terminal
```

```
Router(config)# access-list template 50
Router(config)# exit
```

ACL のテンプレートの概要情報を示す例

以下の例は、システム内の全 ACL 用の要約情報を表示する方法を示しています。このコマンドからの出力には、次の情報が含まれています。

- テンプレート ACL ごとのルールの最大数
- 発見されたアクティブなテンプレート数
- これらのテンプレートによって置き換えられた ACL 数
- レッドブラックツリー内の要素数

```
Router# show access-list template summary
Maximum rules per template ACL = 100
Templates active = 9
Number of ACLs those templates represent = 14769
Number of tree elements = 13
```

レッドブラックツリー要素

ツリー要素の数は、レッドブラックツリー内の要素の数です。各テンプレートは、レッドブラックツリー内の一意のエントリを 1 つ含みます。システムは、ピア IP アドレスをマスクする各 ACL 上の巡回冗長検査（CRC）を計算し、レッドブラックツリーに CRC を送信します。次に例を示します。

システムに 9 つのテンプレート（14769 個の ACL を表す）、および 13 のツリーの要素があります。レッドブラックツリー内で各テンプレートに一意のエントリが 1 つしかない場合、その他 4 つのツリー要素は、システムには、テンプレート化されていない 4 個のユーザーあたりの ACL が含まれているということです。

ACL のテンプレート ツリー情報を示す例

以下の例は、システム内の全 ACL 用のレッドブラックツリー情報を表示する方法を示しています。

このコマンドからの出力には、次の情報が含まれています。

- レッドブラックツリー上の ACL 名
- 元の CRC32 値
- ACL のユーザー数
- 計算された CRC32 値

```
Router# show access-list template tree
```

```
ACL name      OrigCRC   Count  CalcCRC
4Temp_1073741891108      59DAB725   98  59DAB725
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』
セキュア シェル	セキュア シェルおよびセキュア シェル バージョン 2 サポート設定の機能モジュール。
認証と認可の設定	認証設定、認可設定、およびアカウンティング設定の機能モジュール。

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACL テンプレートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2: ACL* テンプレートに関する機能情報

機能名	リリース	機能情報
ACL テンプレート	12.2(28) SB 12.2(31) SB2 Cisco IOS XE リリース 2.4	12.2(28)SB では、この機能が Cisco 10000 シリーズ ルータで追加されました。 12.2(31)SB2 では、PRE3 のサポートが追加されました。 この機能は、Cisco IOS XE Release 2.4 で、Cisco ASR 1000 シリーズ ルータに実装されました。 次のコマンドが導入または変更されました。**access-list template, show access-list template**

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。