RADIUS 集中型フィルタ管理

RADIUS 集中型フィルタ管理機能は、ACL の設定と管理を容易にするフィルタ サーバを導入しています。このフィルタ サーバは、集中型 RADIUS リポジトリおよび管理ポイントとして機能します。ユーザは、Access Control List（ACL; アクセス コントロール リスト）フィルタを集中的に管理および設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS 集中型フィルタ管理の機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS 集中型フィルタ管理の前提条件

- 新しい RADIUS VSA をサポートしていないサーバにディレクトリ ファイルを追加しなければならない場合があります。サンプル ディレクトリとベンダー ファイルについては、このマニュアルの「RADIUS 辞書とベンダー ファイル：例」を参照してください。

  ディレクトリ ファイルを追加する必要がある場合は、RADIUS サーバが非標準であり、新しく導入された VSA を送信可能であること確認してください。
- リモート ユーザがダイヤルインして IP 接続を確立できるように、RADIUS ネットワーク認証をセットアップすることができます。

RADIUS 集中型フィルタ管理の制約事項

この機能では複数の方式リストがサポートされていません。単一のグローバル フィルタ方式リストが設定できるだけです。

RADIUS 集中型フィルタ管理に関する情報

RADIUS 集中型フィルタ管理機能以前は、ホールセール プロバイダー（ACL などの顧客サービスに対して特別料金を課している）が、顧客の網羅的な ACL の適用を阻止できました。この行為は、ルータの性能や他の顧客に影響を与える可能性があります。この機能は、ACL 管理用の集中型管理ポイント（フィルタ サーバ）を導入しています。フィルタ サーバは、ACL 設定用の集中型 RADIUS リポジトリとして機能します。

フィルタ サーバとして使用されている RADIUS サーバがアクセス認証に使用されているサーバと同じかどうかに関係なく、Network Access Server（NAS; ネットワーク アクセス サーバ）はフィルタ サーバに対して別のアクセス要求を開始します。設定されていれば、NAS は、認証ユーザ名と 2 つめのアクセス要求用のフィルタ サーバ パスワードとして、フィルタ ID 名を使用します。RADIUS サーバは、フィルタ ID 名を認証して、access-accept 応答内に必要なフィルタリング設定を返そうとします。

ACL のダウンロードには時間がかかるため、NAS 上でローカル キャッシュが維持されます。ローカル キャッシュ上に ACL 名が存在する場合は、フィルタ サーバに問い合わせることなくその設定が使用されます。

（注） キャッシュが適切に設定されていれば、遅延は最小限に抑えられるはずです。ただし、フィルタが必要な最初のダイヤルイン ユーザは必ず待たされることになります。これは、初めての場合は、ACL 設定が読み込まれるためです。

キャッシュ管理

グローバル フィルタ キャッシュは最後に ACL をダウンロードした NAS 上で維持されます。そのため、ユーザは、過負荷状態の RADIUS サーバに対して同じ ACL 設定情報を何度も要求する必要がありません。ユーザは、次の基準が満たされている場合にキャッシュをフラッシュする必要があります。

- エントリが新しいアクティブ コールに関連付けられた後に、そのエントリに関連付けられたアイドル タイマーがリセットされる（そのように設定されている場合）。
- アイドル時間スタンプの期限が切れたエントリが削除される。

- グローバル キャッシュのエントリが指定された最大数に到達した後に、アイドル タイマーがアイドル時間限界に最も近いエントリが削除される。

1 つのタイマーがすべてのキャッシュ エントリの管理に使用されます。このタイマーは、最初のキャッシュ エントリの作成時に開始され、リブートされるまで定期的に実行されます。タイマーの期間は、キャッシュ アイドル タイマーの設定時に指定された最小粒度に対応し、毎分期限切れになります。タイマーが 1 つしかないことによって、ユーザは、キャッシュ エントリごとに別々のタイマーを管理する必要がありません。

（注） 単一のタイマーは、タイマーの期限切れの精度に欠けます。約 50% のタイマー粒度に平均誤差が含まれています。タイマー粒度を下げると平均誤差も下がりますが、性能が低下する可能性があります。キャッシュ管理には正確なタイミングが必要ないため、誤差遅延を受け入れる必要があります。

新しいベンダー固有アトリビュートのサポート

この機能は、次の 2 つのカテゴリに分類可能な 3 つの新しい Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）のサポートを導入しています。

- ユーザ プロファイルの拡張
  - Filter-Required（50）：指定されたフィルタが見つからなかった場合にコールを許可するかどうかを指定します。存在する場合は、このアトリビュートが、すべての Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）フィルタ方式リストの後に適用されます。
- 疑似ユーザ プロファイルの拡張
  - Cache-Refresh（56）：エントリが新しいセッションから参照されるたびにキャッシュ エントリをリフレッシュするかどうかを指定します。このアトリビュートは、**cache refresh** コマンドに対応します。
  - Cache-Time（57）：キャッシュ エントリのアイドル タイムアウトを分単位で指定します。このアトリビュートは、**cache clear age** コマンドに対応します。

（注） すべての RADIUS アトリビュートが、すべての Command-Line Interface（CLI; コマンドライン インターフェイス）設定よりも優先されます。

RADIUS 用の集中型フィルタ管理の設定方法

次の項を使用して、集中型フィルタ管理機能を設定します。

- 「RADIUS ACL フィルタ サーバの設定」
- 「フィルタ キャッシュの設定」
- 「フィルタ キャッシュの確認」

RADIUS ACL フィルタ サーバの設定

RADIUS ACL フィルタ サーバを有効にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authorization cache filterserver default` *methodlist[methodlist2...]*	AAA 認可キャッシュと、RADIUS フィルタ サーバからの ACL 設定のダウンロードを有効にします。 • **default**：デフォルト認可リスト • *methodlist* [*methodlist2...*]：**password** コマンド ページに列挙されたキーワードの 1 つ。

フィルタ キャッシュの設定

この項の次の手順に従って、AAA フィルタ キャッシュを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa cache filter**
4. **password** {**0** | **7**} *password*
5. **cache disable**
6. **cache clear age** *minutes*
7. **cache refresh**
8. **cache max** *number*

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
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	`Router(config)# aaa cache filter`	フィルタ キャッシュ設定を有効にして、AAA フィルタ コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 4	`Router(config-aaa-filter)# password {0 | 7} password`	（任意）フィルタ サーバ認証要求に使用されるオプション パスワードを指定します。 **0**：暗号化されていないパスワードが後に続くことを示します。 **7**：非表示パスワードが後に続くことを示します。 *password*：暗号化されていない（クリア テキスト）パスワード。 **（注）** パスワードが指定されなかった場合は、デフォルト パスワード（「cisco」）が有効になります。
ステップ 5	`Router(config-aaa-filter)# cache disable`	（任意）キャッシュを無効にします。
ステップ 6	`Router(config-aaa-filter)# cache clear age minutes`	（任意）キャッシュ エントリの期限が切れ、キャッシュがクリアされるタイミングを分単位で指定します。 *minutes*：0 ～ 4294967295 の任意の値。 **（注）** 時間が指定されなかった場合は、デフォルト（1400 分（1 日））が有効になります。
ステップ 7	`Router(config-aaa-filter)# cache refresh`	（任意）新しいセッションの開始時点でキャッシュ エントリをリフレッシュします。このコマンドは、デフォルトで有効になっています。この機能を無効にするには、**no cache refresh** コマンドを使用します。
ステップ 8	`Router(config-aaa-filter)# cache max number`	（任意）キャッシュで特定のサーバ用に維持できるエントリの絶対数を制限します。 *number*：キャッシュに含めることが可能なエントリの最大数。0 ～ 4294967295 の任意の値。 **（注）** 数値が指定されなかった場合は、デフォルト（100 エントリ）が有効になります。

フィルタ キャッシュの確認

キャッシュ ステータスを表示するには、**show aaa cache filterserver** EXEC コマンドを使用します。**show aaa cache filterserver** コマンドの出力サンプルを次に示します。

```
Router# show aaa cache filterserver

Filter     Server          Age Expires Refresh Access-Control-Lists
-------------------------------------------------------------------------------
aol        10.2.3.4          0    1440     100 ip in icmp drop
                                               ip out icmp drop
                                               ip out forward tcp dstip 1.2.3...
msn        10.3.3.4         N/A   Never       2 ip in tcp drop
msn2       10.4.3.4         N/A   Never       2 ip in tcp drop
vone       10.5.3.4         N/A   Never       0 ip in tcp drop
```

（注） **show aaa cache filterserver** コマンドは、特定のフィルタが参照またはリフレッシュされた回数を表示します。この機能は、実際に使用されるフィルタを決定するために管理者が使用します。

トラブルシューティングのヒント

フィルタ キャッシュ設定のトラブルシューティングを支援するために、**debug aaa cache filterserver** 特権 EXEC コマンドを使用します。**debug aaa cache filterserver** コマンドのサンプル出力を確認するには、このマニュアルの「デバッグ出力：例」を参照してください。

フィルタ キャッシュのモニタリングと維持

フィルタ キャッシュをモニタおよび維持するには、次の EXEC コマンドの少なくとも 1 つを使用します。

コマンド	目的
Router# **clear aaa cache filterserver acl** [*filter-name*]	特定のフィルタまたはすべてのフィルタのキャッシュ ステータスをクリアします。
Router# **show aaa cache filterserver**	キャッシュ ステータスを表示します。

RADIUS 集中型フィルタ管理の設定例

ここでは、次の設定例について説明します。

NAS の設定：例

次の例は、キャッシュ フィルタリング用の NAS の設定方法を示しています。この例では、最初に、サーバ グループの「mygroup」に接続されます。応答がない場合は、デフォルト RADIUS サーバに接続されます。それでも応答がない場合は、ローカル フィルタ ケアに接続されます。最終的に、フィルタが解決できなければ、コールが受け入れられます。

```
aaa authorization cache filterserver group mygroup group radius local none
!
aaa group server radius mygroup
 server 10.2.3.4
 server 10.2.3.5
!
radius-server host 10.1.3.4
!
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
!
```

RADIUS サーバの設定：例

次の例は、NAS にダイヤルしているリモート ユーザの「user1」のサンプル RADIUS 設定です。

```
myfilter Password = "cisco"
        Service-Type = Outbound,
        Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32
        icmp",
        Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 tcp
        dstport = telnet",
        Ascend:Ascend-Cache-Refresh = Refresh-No,
        Ascend:Ascend-Cache-Time = 15

user1 Password = "cisco"
        Service-Type = Framed,
        Filter-Id = "myfilter",
        Ascend:Ascend-Filter-Required = Filter-Required-Yes,
```

RADIUS 辞書とベンダー ファイル：例

次の例は、新しい VSA 用のサンプル RADIUS 辞書ファイルです。この例では、辞書ファイルが Merit サーバ用です。

```
dictionary file:
Ascend.attr Ascend-Filter-Required 50 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Refresh   56 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Time      57 integer (*, 0, NOENCAPS)

Ascend.value Ascend-Cache-Refresh Refresh-No  0
Ascend.value Ascend-Cache-Refresh Refresh-Yes 1

Ascend.value Ascend-Filter-Required  Filter-Required-No  0
Ascend.value Ascend-Filter-Required  Filter-Required-Yes 1

vendors file:
50     50
56     56
57     57
```

デバッグ出力：例

debug aaa cache filterserver コマンドのサンプル出力を次に示します。

```
Router# debug aaa cache filterserver

AAA/FLTSV: need "myfilter" (fetch), call 0x612DAC64
AAA/FLTSV: send req, call 0x612DAC50
AAA/FLTSV: method SERVER_GROUP myradius
AAA/FLTSV: recv reply, call 0x612DAC50 (PASS)
AAA/FLTSV: create cache
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: skip attr "filter-cache-refresh"
AAA/FLTSV: skip attr "filter-cache-time"
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" refresh? no
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" cachetime 15
```

```
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: PASS call 0x612DAC64
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (1 entry)
AAA/CACHE: destroy "AAA filtserv cache" entry "myfilter"
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
```

その他の参考資料

次の項で、RADIUS 集中型フィルタ管理に関する参考資料を紹介します。

関連資料

内容	参照先
認可の設定	「Configuring Authorization」フィーチャ モジュール
RADIUS の設定	「Configuring RADIUS」フィーチャ モジュール
認可コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
なし	—

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

RADIUS 集中型フィルタ管理の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　RADIUS 集中型フィルタ管理の機能情報

機能名	リリース	機能情報
RADIUS 集中型フィルタ管理	12.2(13)T 12.2(28)SB 12.2(33)SRC 1	RADIUS 集中型フィルタ管理機能は、ACL の設定と管理を容易にするフィルタ サーバを導入しています。このフィルタ サーバは、集中型 RADIUS リポジトリおよび管理ポイントとして機能します。ユーザは、Access Control List（ACL; アクセス コントロール リスト）フィルタを集中的に管理および設定できます。 この機能は、Cisco IOS Release 12.2(13)T で導入されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 **aaa authorization cache filterserver**、**aaa cache filter**、**cache clear age**、**cache disable**、**cache refresh**、**clear aaa cache filterserver acl**、**debug aaa cache filterserver**、**password**、および **show aaa cache filterserver** の各コマンドが、この機能で導入または変更されました。