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、アクセス コントロール リスト（ACL）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。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

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。サンプルのディクショナリとベンダー ファイルについて

は、このドキュメントの後半にある「RADIUSディクショナリとベンダーファイルの例」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。この機能では、ACL管理用の集中型管理ポイント（フィルタ サーバ）が導入されます。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、ネットワーク アクセス サーバ（NAS）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属性のサポート

この機能は、次の 2 つのカテゴリに分類可能な 3 つの新しいベンダー固有属性（VSA）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、この属性が、すべての認証、許可、アカウンティング（AAA）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 エントリを更新するかどうかを指定します。この属性は、**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。この属性は、**cache clear age** コマンドに対応します。

（注） すべての RADIUS 属性が、すべてのコマンドライン インターフェイス（CLI）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

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. Router(config)# **aaa cache filter**
4. Router(config-aaa-filter)# **password 0 7**} *password*
5. Router(config-aaa-filter)# **cache disable**
6. Router(config-aaa-filter)# **cache clear age** *minutes*
7. Router(config-aaa-filter)# **cache refresh**
8. Router(config-aaa-filter)# **cache max** *number*

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
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。
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、デフォルトでイネーブルになっています。この機能をディセーブルにするには、**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。次に、**show aaa cache filterserver** コマンドの出力例を示します。

```
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、このドキュメントの後半にある「デバッグ出力の例」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

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「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 ディクショナリとベンダー ファイルの例

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

次に、**debug aaa cache filterserver** コマンドの出力例を示します。

```
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

関連項目	マニュアル タイトル
認可の設定	「Configuring Authorization」機能モジュール。
RADIUS の設定	「Configuring RADIUS」機能モジュール
認可コマンド	『*Cisco IOS Security Command Reference*』

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 IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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	--

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS 集中型フィルタ管理の機能情報

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 *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	Cisco IOS XE Release 3.9S	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、アクセス コントロール リスト（ACL）フィルタを集中的に管理および設定できます。 この機能により、次のコマンドが導入または変更されました。**aaa authorization cache filterserver**、**aaa cache filter, cache clear age, cache disable, cache refresh**、**clear aaa cache filterserver acl**、**debug aaa cache filterserver**、**password**、**show aaa cache filterserver.**