アクセス要求のアトリビュート スクリーニング

アクセス要求のアトリビュート スクリーニング機能を使用すると、認証用または認可用に RADIUS サーバへのアウトバウンドのアクセス要求のアトリビュートをフィルタ処理するように Network Access Server（NAS; ネットワーク アクセス サーバ）を設定することができます。

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、「アクセス要求のアトリビュート スクリーニングの機能情報」（P.9）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

アクセス要求のアトリビュート スクリーニングの前提条件

- アトリビュート リストの設定を十分理解していることが必要です。

アクセス要求のアトリビュート スクリーニングの制約事項

- アトリビュート 1（Username）、アトリビュート 2（User-Password）、アトリビュート 3（Chap-Password）をフィルタ処理することはできません。

アクセス要求のアトリビュート スクリーニングについて

アクセス要求のアトリビュート スクリーニング機能を設定するために、次の概念を理解しておく必要があります。

- 「アウトバウンドのアクセス要求のアトリビュートをフィルタ処理する NAS の設定」（P.2）

アウトバウンドのアクセス要求のアトリビュートをフィルタ処理する NAS の設定

アクセス要求のアトリビュート スクリーニング機能を使用すると、認証用または認可用に RADIUS サーバへのアウトバウンドのアクセス要求のアトリビュートをフィルタ処理するように NAS を設定することができます。フィルタの設定は、NAS で行ったり、ダウンロード可能な Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）によって Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバからダウンロードしたりすることができます。

次に、ダウンロード可能な VSA の例をいくつか示します。

```
Cisco:Cisco-Avpair=”ppp-authen-type=chap”
Cisco:Cisco-Avpair=”ppp-authen-list=group 1”
Cisco:Cisco-Avpair=”ppp-author-list=group 1”
Cisco:Cisco-Avpair=”vpdn:tunnel-id=B53”
Cisco:Cisco-Avpair=”vpdn:ip-addresses=10.0.58.35”
```

（注） フィルタ処理するアトリビュートがわかっている必要があります。ある一定の主要アトリビュートをフィルタ処理すると、認証に失敗することがあります（たとえば、アトリビュート 60 はフィルタ処理すべきではありません）。

アクセス要求のアトリビュート スクリーニングの設定方法

ここでは、次の各手順について説明します。

- 「アクセス要求のアトリビュート スクリーニングの設定」（P.3）
- 「ダウンロード可能なフィルタをサポートするためのルータの設定」（P.4）
- 「Attribute Filtering for Access Requests のモニタリングとメンテナンス」（P.5）

アクセス要求のアトリビュート スクリーニングの設定

アクセス要求のアトリビュート スクリーニングを設定する手順は、次のとおりです。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute list** *listname*
4. **attribute** *value1* **[***value2* **[***value3...***]]**
5. **aaa group server radius** *group-name*
6. **authorization** [**request** | **reply**] [**accept** | **reject]** *listname*

   または

   accounting [**request** | **reply**] **[accept** | **reject]** *listname*

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。 • 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	**radius-server attribute list** *listname* **例：** `Router (config)# radius-server attribute list attrlist`	アトリビュート リストを定義します。
ステップ 4	**attribute** *value1* **[***value2***[***value3***...]]** **例：** `Router (config)# attribute 6-10, 12`	許可リストまたは拒否リストにアトリビュートを追加します。
ステップ 5	**aaa group server radius** *group-name* **例：** `Router (config)# aaa group server radius rad1`	アトリビュート リストを AAA サーバ グループに適用し、server-group 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 6	**authorization** [**request** | **reply**][**accept** | **reject**] *listname*
	
	または
	accounting [**request** | **reply**] [**accept** | **reject**] *listname*
	
	例：
	`Router (config-sg-radius)# authorization request accept attrlist`
	
	または
	
	例：
	`Router (config-sg-radius)# accounting request accept attrlist`
		認証用または認可用に RADIUS サーバへのアウトバウンドの Access Request のアトリビュートをフィルタ処理します。
		• **request** キーワードでは、認可の発信 Access Request に使用するフィルタを定義します。
		• **reply** キーワードでは、認可の着信 Accept パケットと着信 Reject パケットのフィルタと、発信アカウンティング要求のフィルタを定義します。

ダウンロード可能なフィルタをサポートするためのルータの設定

次の作業を行って、ダウンロード可能なフィルタをサポートするようにルータを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default group radius**
5. **radius-server attribute list** *list-name*
6. **attribute** *value1* [*value2* [*value3...*]]

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。 • 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	**aaa authorization template** **例：** `Router (config)# aaa authorization template`	Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing and Forwarding（VRF; VPN ルーティングおよび転送）に基づいて、ローカルまたはリモートのカスタマー テンプレートの使用をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa authorization network default group radius** **例：** `Router (config)# aaa authorization network default group radius`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。
ステップ 5	**radius-server attribute list** *list-name* **例：** `Router (config)# radius-server attribute list attlist`	許可リストまたは拒否リストの名前を定義します。
ステップ 6	**attribute** *value1* [*value2* [*value3*...]] **例：** `Router (config)# attribute 10-14, 24`	許可リストまたは拒否リストにアトリビュートを追加します。

トラブルシューティングのヒント

アトリビュートのフィルタ処理が機能しない場合は、アトリビュート リストが正しく定義されているかどうかを確認します。

Attribute Filtering for Access Requests のモニタリングとメンテナンス

アトリビュートのフィルタ処理をモニタリングおよびメンテナンスするために、**debug radius** コマンドを使用できます。

手順の概要

1. **enable**
2. **debug radius**

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。 • 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	**debug radius** **例：** `Router# debug radius`	RADIUS の情報（フィルタ処理の情報など）を表示します。

Attribute Filtering for Access Requests の設定例

ここでは、次の設定例について説明します。

Attribute Filtering for Access Requests の例

次の例は、「all-attr」で定義されているアトリビュート 30-31 がアウトバウンドのすべての Access Request メッセージで拒否されることを示しています。

```
aaa group server radius ras
 server 172.19.192.238 auth-port 1745 acct-port 1746
 authorization request reject all-attr
!
.
.
.
radius-server attribute list all-attr
 attribute 30-31
!
.
.
.
```

ユーザ プロファイルのアトリビュート フィルタ処理の例

次の例は、Access Request のアトリビュート フィルタ処理を設定した後のユーザ プロファイルです。

```
cisco.com Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
Cisco:Cisco-Avpair = :1:"rad-serv=172.19.192.87 key rad123",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=authorization request reject range1",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=accounting request reject range1",
Cisco:Cisco-Avpair = "ppp-authen-type=chap"
Cisco:Cisco-Avpair = "ppp-authen-list=group 1",
Cisco:Cisco-Avpair = "ppp-author-list=group 1",
Cisco:Cisco-Avpair = "ppp-acct-list=start-stop group 1",
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"


user2@cisco.com
Service-Type = Outbound,
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"
```

aaa authorization template コマンドが設定されているため、上記のように user2@cisco.com のセッションが Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）Network Server（LNS; ネットワーク サーバ）で「確立」されると、RADIUS 要求が Cisco.com のサーバに送信されます。その後、Cisco.com のサーバは、認証が成功すれば、Cisco.com のプロファイルの一部として設定されている VSA とともに、Access Accept メッセージを送信します。Cisco.com のプロファイルの一部としてフィルタが設定されている場合は、それらのフィルタが解析され、user2@cisco.com の RADIUS 要求に適用されます。

上記のプロファイルの例では、フィルタ range1 が認可要求およびアカウンティング要求に適用されます。

debug radius コマンドの例

フィルタ処理しようとしているアトリビュートが拒否される場合、次のような **debug radius** の出力ステートメントが表示されます。

```
RADIUS: attribute 31 rejected
```

フィルタ処理できないアトリビュートをフィルタ処理すると、次のような出力ステートメントが表示されます。

```
RADIUS: attribute 1 cannot be rejected
```

その他の参考資料

ここでは、Attribute Filtering for Access Requests の関連資料について説明します。

関連資料

内容	参照先
RADIUS の設定	『Configuring RADIUS』機能マニュアル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
RADIUS アトリビュート リスト	『RADIUS Attribute Screening』機能マニュアル

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

アクセス要求のアトリビュート スクリーニングの機能情報

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　アクセス要求のアトリビュート スクリーニングの機能情報

機能名	リリース	機能情報
アクセス要求のアトリビュート スクリーニング	12.3(3)B 12.3(7)T 12.2(28)SB 12.2(33)SRC	アクセス要求のアトリビュート スクリーニング機能を使用すると、認証用または認可用に RADIUS サーバへのアウトバウンドのアクセス要求のアトリビュートをフィルタ処理するように Network Access Server（NAS; ネットワーク アクセス サーバ）を設定することができます。 この機能は、12.3(3)B で導入されました。 この機能は、Cisco IOS Release 12.3(7)T に統合されました。 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。 この機能によって導入または変更されたコマンドは、**authorization (server-group)** です。