IPsec VPN アカウンティング

IPsec VPN アカウンティング機能を使用すれば、セッションが開始される時と終了する時を指示することによって、セッションをアカウンティングできます。

VPN セッションとは、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）Security Association（SA; セキュリティ アソシエーション）および、IKE SA によって作成される 1 つ以上の SA ペアとして定義されます。セッションは、最初の IP Security（IPsec; IP セキュリティ）ペアが作成されると開始し、すべての IPsec SA が削除されると停止します。

セッション識別情報およびセッション使用状況情報は、標準 RADIUS アトリビュートとベンダー固有アトリビュートを介して、Remote Authentication Dial-In User Service（RADIUS）サーバに渡されます。

IPsec VPN アカウンティングの機能仕様

機能の履歴	
リリース	**変更点**
12.2(15)T	この機能が追加されました。
サポートされているプラットフォーム	
Cisco 2610 ～ 2613、Cisco 2620 ～ Cisco 2621、Cisco 2650 ～ Cisco 2651、Cisco 3620、Cisco 3640、Cisco 3660、Cisco 3725、Cisco 3745、Cisco 7100、Cisco 7200、Cisco 7400、Cisco ubr7100、Cisco ubr7200	

プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索するには

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明の場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

IPsec VPN アカウンティングの前提条件

- RADIUS と Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）アカウンティングの設定方法を理解している必要があります。
- IPsec アカウンティングの設定方法を理解している必要があります。

IPsec VPN アカウンティングに関する情報

IPsec VPN アカウンティングを設定するには、次の概念を理解しておく必要があります。

RADIUS アカウンティング

多くの大規模ネットワークでは、監査のために、ユーザ アクティビティを記録する必要があります。多く使用される方式は、RADIUS アカウンティングです。

RADIUS アカウンティングを使用すれば、セッションが開始される時と終了する時を指示することによって、セッションをアカウンティングできます。さらに、セッション識別情報およびセッション使用状況情報が、RADIUS アトリビュートおよび VSA を介して、RADIUS サーバに渡されます。

RADIUS 開始アカウンティング

RADIUS 開始パケットには、一般的には、サービスを要求する者、およびサービスのプロパティの構成を特定する多くのアトリビュートが格納されています。表 1 に、開始に必要なアトリビュートを示します。

表 1　RADIUS アカウンティング開始パケット アトリビュート

RADIUS アトリビュート値	アトリビュート	説明
1	user-name	Extended Authentication（XAUTH; 拡張認証）で使用されるユーザ名。XAUTH が使用されない場合、ユーザ名が NULL になる場合があります。
4	nas-ip-address	ユーザにサービスを提供する Network Access Server（NAS; ネットワーク アクセス サーバ）の IP アドレスの識別。RADIUS サーバのスコープ内の NAS に対して一意である必要があります。
5	nas-port	ユーザにサービスを提供する NAS の物理ポート番号。

表 1　RADIUS アカウンティング開始パケット アトリビュート （続き）

RADIUS アトリビュート値	アトリビュート	説明
8	framed-ip-address	IPsec セッション用に割り当てられたプライベート アドレス。
40	acct-status-type	ステータス タイプ。このアトリビュートでは、このアカウンティング要求がマーキングするのが、セッションの開始（start）、終了（stop）、または更新のいずれかなのかを示します。
41	acct-delay-time	クライアントが特定のレコードの送信を試行した秒数。
44	acct-session-id	ログ ファイル内の開始レコードと終了レコードのマッチングを容易にする一意のアカウンティング ID。
26	vrf-id	Virtual Route Forwarder（VRF）の名前を表す文字列。
26	isakmp-initiator-ip	リモート IKE の発信側（V4）のエンドポイント IP アドレス。
26	isakmp-group-id	アカウンティングに使用される VPN グループ プロファイルの名前。
26	isakmp-phase1-id	セッションの発信側の識別を可能にする、IKE によって使用されるフェーズ 1 識別情報（ID）（たとえば、ドメイン名（DN）、完全修飾ドメイン名（FQDN）、IP アドレスなど）。

RADIUS 終了アカウンティング

RADIUS 終了パケットには、セッションの使用状況を識別する多くのアトリビュートが格納されています。表 2 に、RADIUS 終了パケットに必要な追加アトリビュートを示します。開始パケットなしで終了パケットだけを送信することは、そのように設定すれば可能です。終了パケットだけを送信すれば、これにより、AAA サーバに送信されるレコードの数を簡単に減らせます。

表 2　RADIUS アカウンティング終了パケット アトリビュート

RADIUS アトリビュート値	アトリビュート	説明
42	acct-input-octets	サービスが提供されている間に Unity クライアントから受信されたオクテット数。
43	acct-output-octets	このサービスの配信中に Unity クライアントに送信されたオクテット数。
46	acct-session-time	Unity クライアントがサービスを受信した時間の長さ（秒単位）。
47	acct-input-packets	このサービスの配信中に Unity クライアントから受信したパケット量。
48	acct-output-packets	このサービスの配信中に Unity クライアントに送信したパケット量。
49	acct-terminate-cause	未使用。

表 2　RADIUS アカウンティング終了パケット アトリビュート （続き）

RADIUS アトリビュート値	アトリビュート	説明
52	acct-input-gigawords	このサービスの間に Acct-Input-Octets カウンタの値が 2^{32}（2 の 32 乗）を超えた回数。
52	acct-output-gigawords	このサービスの間に Acct-Input-Octets カウンタの値が 2^{32}（2 の 32 乗）を超えた回数。

RADIUS 更新アカウンティング

RADIUS 更新アカウンティングがサポートされています。パケットおよびオクテット カウントが更新内に表示されます。

IKE および IPsec サブシステムの相互作用

アカウンティング開始

IPsec アカウンティングが設定されている場合、IKE フェーズが終了すると、アカウンティング開始レコードがセッション用に生成されます。キー再生成中は、新しいアカウンティング レコードは生成されません。

次に、ルータ上で生成されており、定義されている AAA サーバに送信されるアカウント開始レコードを示します。

```
*Aug 23 04:06:20.131: RADIUS(00000002): sending
*Aug 23 04:06:20.131: RADIUS(00000002): Send Accounting-Request to 10.1.1.4:1646 id 4, len
220
*Aug 23 04:06:20.131: RADIUS:  authenticator 38 F5 EB 46 4D BE 4A 6F - 45 EB EF 7D B7 19
FB 3F
*Aug 23 04:06:20.135: RADIUS:  Acct-Session-Id     [44]  10  "00000001"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  31
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   25  "isakmp-group-id=cclient"
*Aug 23 04:06:20.135: RADIUS:  Framed-IP-Address   [8]   6   10.13.13.1
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   29  "isakmp-initator-ip=11.1.2.2"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
*Aug 23 04:06:20.135: RADIUS:  User-Name           [1]   13  "joe@cclient"
*Aug 23 04:06:20.135: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 04:06:20.135: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 04:06:20.135: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 04:06:20.135: RADIUS:  NAS-IP-Address      [4]   6   10.1.1.147
*Aug 23 04:06:20.135: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 04:06:20.139: RADIUS: Received from id 21645/4 10.1.1.4:1646, Accounting-response,
len 20
*Aug 23 04:06:20.139: RADIUS:  authenticator B7 E3 D0 F5 61 9A 89 D8 - 99 A6 8A 8A 98 79
9D 5D
```

アカウンティング終了

リモート ピアでのフロー（IPsec SA ペア）がなくなると、アカウンティング終了パケットが生成されます。

アカウンティング終了レコードには次の情報が格納されます。

- パケット出力
- パケット入力
- オクテット出力
- ギガワード入力
- ギガワード出力

次に、ルータ上で生成されたアカウント開始レコードを示します。アカウント開始レコードは、定義されている AAA サーバに送信されます。

```
*Aug 23 04:20:16.519: RADIUS(00000003): Using existing nas_port 0
*Aug 23 04:20:16.519: RADIUS(00000003): Config NAS IP: 100.1.1.147
*Aug 23 04:20:16.519: RADIUS(00000003): sending
*Aug 23 04:20:16.519: RADIUS(00000003): Send Accounting-Request to 100.1.1.4:1646 id 19,
len 238
*Aug 23 04:20:16.519: RADIUS:  authenticator 82 65 5B 42 F0 3F 17 C3 - 23 F3 4C 35 A2 8A
3E E6
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   29  "isakmp-initator-ip=11.1.1.2"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Time   [46]  6   709
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Octets   [42]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Octets  [43]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Packets  [47]  6   1004
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Packets [48]  6   1004
*Apr 23 04:20:16.519: RADIUS:  Acct-Input-Giga-Word[52]  6   0
*Apr 23 04:20:16.519: RADIUS:  Acct-Output-Giga-Wor[53]  6   0
*Aug 23 04:20:16.519: RADIUS:  Acct-Terminate-Cause[49]  6   none                       [0]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  32
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   26  "disc-cause-ext=No Reason"
*Aug 23 04:20:16.519: RADIUS:  Acct-Status-Type    [40]  6   Stop                       [2]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 04:20:16.519: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 04:20:16.519: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 04:20:16.519: RADIUS:  NAS-IP-Address      [4]   6   100.1.1.147
*Aug 23 04:20:16.519: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 04:20:16.523: RADIUS: Received from id 21645/19 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 04:20:16.523: RADIUS:  authenticator F1 CA C1 28 CE A0 26 C9 - 3E 22 C9 DA EA B8
22 A0
```

アカウンティング更新

アカウンティング更新をイネーブルにすると、セッションが「up」である間にアカウンティング更新が送信されます。アカウンティング更新をイネーブルにするには、**aaa accounting update** コマンドを使用します。

次に、ルータから送信されるアカウンティング更新を示します。

IPsec VPN アカウンティングの設定方法

```
Router#
*Aug 23 21:46:05.263: RADIUS(00000004): Using existing nas_port 0
*Aug 23 21:46:05.263: RADIUS(00000004): Config NAS IP: 100.1.1.147
*Aug 23 21:46:05.263: RADIUS(00000004): sending
*Aug 23 21:46:05.263: RADIUS(00000004): Send Accounting-Request to 100.1.1.4:1646 id 22,
len 200
*Aug 23 21:46:05.263: RADIUS:  authenticator 30 FA 48 86 8E 43 8E 4B - F9 09 71 04 4A F1
52 25
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Id     [44]  10  "00000003"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   29  "isakmp-initator-ip=11.1.1.2"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Time   [46]  6   109
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Octets   [42]  6   608
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Octets  [43]  6   608
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Packets  [47]  6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Packets [48]  6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Status-Type    [40]  6   Watchdog                  [3]
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 21:46:05.263: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 21:46:05.263: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 21:46:05.263: RADIUS:  NAS-IP-Address      [4]   6   100.1.1.147
*Aug 23 21:46:05.263: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 21:46:05.267: RADIUS: Received from id 21645/22 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 21:46:05.267: RADIUS:  authenticator 51 6B BB 27 A4 F5 D7 61 - A7 03 73 D3 0A AC
1C
```

ここでは、次の各手順について説明します。

IPsec VPN アカウンティングの設定

IPsec VPN アカウンティングを設定するには、次の必須作業を実行する必要があります。

前提条件

IPsec VPN アカウンティングを設定する前に、まず IPsec を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name method*

5. **aaa authorization network** *list-name method*
6. **aaa accounting network** *list-name* **start-stop [broadcast] group** *group-name*
7. **aaa session-id common**
8. **crypto isakmp profile** *profile-name*
9. **vrf** *ivrf*
10. **match identity group** *group-name*
11. **client authentication list** *list-name*
12. **isakmp authorization list** *list-name*
13. **client configuration address** [**initiate** | **respond**]
14. **accounting** *list-name*
15. **exit**
16. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
17. **set transform-set** *transform-set-name*
18. **set isakmp-profile** *profile-name*
19. **reverse-route** [**remote-peer**]
20. **exit**
21. **crypto map** *map-name* **ipsec-isakmp dynamic** *dynamic-template-name*
22. **radius-server host** *ip-address* [**auth-port** *port-number*] **[acct-port** *port-number*]
23. **radius-server key** *string*
24. **radius-server vsa send accounting**
25. **interface** *interface-id*
26. **crypto map** *map-name*

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 new-model** **例：** `Router (config)# aaa new-model`	アカウンティング サーバに送信される定期的中間アカウンティング レコード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 authentication login** *list-name method* **例：** `Router (config)# aaa authentication login cisco-client group radius`	RADIUS またはローカル経由で、認証、認可、および拡張認可（XAUTH）のアカウンティング（AAA）認証を実行します。
ステップ 5	**aaa authorization network** *list-name method* **例：** `Router (config)# aaa authorization network cisco-client group radius`	RADIUS またはローカルから、リモート クライアント上の AAA 認証パラメータを設定します。
ステップ 6	**aaa accounting network list-name start-stop [broadcast] group** *group-name* **例：** `Router (config)# aaa accounting network acc start-stop broadcast group radius`	課金、または RADIUS や TACACS+ を使用する際のセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。
ステップ 7	**aaa session-id common** **例：** `Router (config)# aaa session-id common`	コール内の各 AAA アカウンティング サービス タイプに、同じセッション ID を使用するかどうか、または、各アカウンティング サービス タイプに対して異なるセッション ID を割り当てるかどうかを指定します。
ステップ 8	**crypto isakmp profile** *profile-name* **例：** `Route (config)# crypto isakmp profile cisco`	IPsec ユーザ セッションを監査し、isakmp-profile サブモードを開始します。
ステップ 9	**vrf** *ivrf* **例：** `Router (conf-isa-prof)# vrf cisco`	オンデマンド アドレス プールを、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）インスタンス名に関連付けます。
ステップ 10	**match identity group** *group-name* **例：** `Router(conf-isa-prof)# match identity group cisco`	ISAKMP プロファイルのピアの ID を一致させます。
ステップ 11	**client authentication list** *list-name* **例：** `Router(conf-isa-prof)# client authentication list cisco`	Internet Security Association and Key Management Protocol（ISAKMP）プロファイル内の IKE 拡張認証（XAUTH）を設定します。
ステップ 12	**isakmp authorization list** *list-name* **例：** `Router(conf-isa-prof)# isakmp authorization list cisco-client`	ISAKMP プロファイル内の AAA サーバを使用して、IKE 共有秘密およびその他のパラメータを設定します。一般に、共有秘密およびその他のパラメータは、モード設定（MODECFG）を介して、リモート ピアへプッシュされます。
ステップ 13	**client configuration address [initiate | respond]** **例：** `Router(conf-isa-prof)# client configuration address respond`	ISAKMP プロファイル内で IKE モード設定（MODECFG）を設定します。

	コマンドまたはアクション	目的
ステップ 14	**accounting** *list-name* **例：** `Router(conf-isa-prof)# accounting acc`	この ISAKMP プロファイルを介して接続しているすべてのピアの AAA アカウンティング サービスをイネーブルにします。
ステップ 15	**exit** **例：** `Router(conf-isa-prof)# exit`	isakmp-profile サブモードを終了します。
ステップ 16	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **例：** `Router(config)# crypto dynamic-map mymap 10 ipsec-isakmp`	ダイナミック クリプト マップ テンプレートを作成し、クリプト マップ コンフィギュレーション コマンド モードを開始します。
ステップ 17	**set transform-set** *transform-set-name* **例：** `Router(config-crypto-map)# set transform-set aswan`	クリプト マップ テンプレートで使用可能なトランスフォーム セットを指定します。
ステップ 18	**set isakmp-profile** *profile-name* **例：** `Router(config-crypto-map)# set isakmp-profile cisco`	ISAKMP プロファイル名を設定します。
ステップ 19	**reverse-route [remote-peer]** **例：** `Router(config-crypto-map)# reverse-route`	ルート（IP アドレス）を、VPN リモート トンネル エンドポイントの背後の宛先に対して注入できるようにします。また、トンネル エンドポイント自体に対するルートを設定することも可能です（クリプト マップの **remote-peer** キーワードを使用します）。
ステップ 20	**exit** **例：** `Router(config-crypto-map)# exit`	ダイナミック クリプト マップ コンフィギュレーション モードを終了します。
ステップ 21	crypto map *map-name* ipsec-isakmp dynamic *dynamic-template-name* **例：** `Router(config)# crypto map mymap ipsec-isakmp dynamic dmap`	クリプト マップ コンフィギュレーション モードを開始します。
ステップ 22	**radius-server host** *ip-address* [**auth-port** *port-number]* [**acct-port** *port-number*] **例：** `Router(config)# radius-server host 172.16.1.4`	RADIUS サーバ ホストを指定します。
ステップ 23	**radius-server key** *string* **例：** `Router(config)# radius-server key nsite`	ルータと RADIUS デーモンとの間におけるすべての RADIUS 通信用の認証および暗号化キーを設置得します。

	コマンドまたはアクション	目的
ステップ 24	**radius-server vsa send accounting** **例：** `Router(config)# radius-server vsa send accounting`	VSA を認識および使用するようにネットワーク アクセス サーバを設定します。
ステップ 25	**interface** *type slot/port* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 26	**crypto map** *map-name* **例：** `Router(config-if)# crypto map mymap`	インターフェイスに対して以前に定義されたクリプト マップ セットを適用します。

アカウンティング更新の設定

セッションが「up」中にアカウンティング更新を送信するには、次の任意の作業を実行します。

前提条件

アカウンティング更新を設定する前に、まず IPsec VPN アカウンティングを設定する必要があります。「IPsec VPN アカウンティングの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting update periodic** *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。 • 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 accounting update periodic** *number* **例：** `Router (config)# aaa accounting update periodic 1-2147483647`	（任意）アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。

IPsec VPN アカウンティングのトラブルシューティング

IPsec アカウンティング イベントに関するメッセージを表示するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **debug crypto isakmp aaa**

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 crypto isakmp aaa** **例：** `Router# debug crypto isakmp aaa`	IKE に関するメッセージを表示します。 • **aaa** キーワードによって、アカウンティング イベントが指定されます。

IPsec VPN アカウンティングの設定例

アカウンティングおよび ISAKMP プロファイル例

次に、アカウンティングおよび ISAKMP プロファイルを持つリモート アクセス クライアントをサポートするための設定する例を示します。

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
```

```
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
authentication pre-share
group 2
!
crypto isakmp policy 10
hash md5
authentication pre-share
lifetime 200
crypto isakmp key cisco address 172.31.100.2

crypto iakmp client configuration group cclient
 key jegjegjhrg
 pool addressA

crypto-isakmp profile groupA
 vrf cisco
 match identity group cclient
 client authentication list cisco-client
 isakmp authorization list cisco-client
 client configuration address respond
 accounting acc
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto dynamic-map remotes 1
set peer 172.31.100.2
set security-association lifetime seconds 120
set transform-set esp-des-md5
reverse-route

!
crypto map test 10 ipsec-isakmp dynamic remotes
!
voice call carrier capacity active
!
interface Loopback0
ip address 10.20.20.20 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0
ip address 10.2.80.203 255.255.255.0
no ip mroute-cache
load-interval 30
duplex full
!
interface FastEthernet1/0
ip address 192.168.219.2 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 172.28.100.1 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
crypto map test
!
no fair-queue
```

```
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.20.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73

ip local pool addressA 192.168.1.1 192.168.1.253
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
exec prompt timestamp
line aux 0
line vty 5 15
 ntp server 172.31.150.52
end
```

ISAKMP プロファイルなしのアカウンティング例

次に、ISAKMP プロファイルが使用されていない時にアカウンティング リモート アクセス ピアをサポートする Cisco IOS 設定全体の例を示します。

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
```

```
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
 lifetime 200
crypto isakmp key cisco address 172.31.100.2
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto map test client accounting list ipsecaaa
crypto map test 10 ipsec-isakmp
 set peer 172.31.100.2
 set security-association lifetime seconds 120
 set transform-set esp-des-md5
 match address 101
!
voice call carrier capacity active
!
interface Loopback0
 ip address 10.20.20.20 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.2.80.203 255.255.255.0
 no ip mroute-cache
 load-interval 30
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.219.2 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 172.28.100.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.30.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
no ip http server
ip pim bidir-enable
!
```

```
!
ip access-list extended encrypt
 permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
line aux 0
line vty 5 15
!
exception core-file ioscrypto/core/sheep-core
exception dump 172.25.1.129
ntp clock-period 17208229
ntp server 172.71.150.52
!
end
```

その他の参考資料

IPsec VPN アカウンティングのその他の関連資料については、次の参考資料を参照してください。

関連資料

内容	参照先
AAA アカウンティングの設定	• 「*Configuring Accounting*」
IPsec VPN アカウンティングの設定	• 「*Configuring Security for VPNs with IPsec*」
基本 AAA RADIUS の設定	• 『*Cisco IOS Security Configuration Guide: User Services*』の「Configuring RADIUS」の項（Cisco.com）
ISAKMP プロファイルの設定	「*VRF Aware IPsec*」
TACACS+ および RADIUS での権限レベル	• 「*Configuring TACACS+*」 • 『*Cisco IOS Security Configuration Guide: User Services*』の「Configuring RADIUS」の項（Cisco.com）
IP セキュリティ、RADIUS、および AAA 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

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **client authentication list**
- **client configuration address**
- **crypto isakmp profile**
- **crypto map（グローバル IPsec）**
- **debug crypto isakmp**
- **isakmp authorization list**
- **match identity**
- **set isakmp-profile**
- **vrf**

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『*Master Command List*』を参照してください。

用語集

IKE：Internet Key Exchange（IKE; インターネット キー エクスチェンジ）。IKE によって、キーが必要なサービス（IP セキュリティ（IPsec）など）のための共有セキュリティ ポリシーおよび認証キーが確立されます。IPsec トラフィックを通過させる前に、ルータ、ファイアウォール、ホストそれぞれでピアの ID を検証する必要があります。それには、事前共有鍵を両ホストに手動で入力するか、Certification Authority（CA; 認証局）サービスを使用します。

IPsec：IP Security（IP セキュリティ）。IPsec はオープン規格のフレームワークであり、これにより、参加ピア間でデータ機密性、データ整合性、およびデータ認証が提供されます。IPsec では、これらのセキュリティ サービスが IP レイヤで実現されます。IPsec では、ローカル ポリシーに基づいたプロトコルやアルゴリズムのネゴシエーションの処理や、IPsec に使用される暗号鍵や認証鍵の生成が、IKE を通じて行われます。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。

ISAKMP：Internet Security Association and Key Management Protocol（インターネット セキュリティ アソシエーションおよびキー管理プロトコル）。ISAKMP は、セキュリティ アソシエーションのネゴシエーション、確立、変更、および削除を行うインターネット IPsec プロトコル（RFC 2408）です。また、キー生成および認証データ（特定のキー生成メカニズムとは独立しています）、キー確立プロトコル、暗号化アルゴリズム、または認証メカニズムも交換されます。

L2TP セッション：レイヤ 2 転送プロトコル。L2TP は、単一の PPP 接続のトンネリングがサポートされた、L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）と L2TP Network Server（LNS; L2TP ネットワーク サーバ）の間における通信トランザクションです。PPP 接続、L2TP セッション、および L2TP コールの間に 1 対 1 の関係があります。

NAS：Network Access Server（NAS; ネットワーク アクセス サーバ）。NAS は、パケットの世界（インターネットなど）と回線の世界（公衆電話交換網（PSTN））との間のインターフェイスとなるシスコのプラットフォーム（または複数のプラットフォームの集まり。AccessPath システムなど）です。

PFS：**Perfect Forward Secrecy（完全転送秘密）。PFS は、導き出される共有秘密値に関連する暗号特性です。PFS を使用すると、1 つの鍵が損なわれても、これ以降の鍵は前の鍵の取得元から取得されないため、前および以降の鍵には影響しません。**

QM：Queue Manager（QM; キュー マネージャ）。Cisco IP Queue Manager（IP QM）は、インテリジェントで、IP ベースの、コール処理およびルーティング ソリューションであり、Cisco IP Contact Center（PCC）ソリューションの一部として、強力なコール処理オプションが提供されます。

RADIUS：Remote Authentication Dial-In User Service。RADIUS は、モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

RSA：Rivest、Shamir、および Adelman。Rivest、Shamir、および Adelman は、暗号化および認証に使用可能な公開鍵暗号化システムの発明者達です。

SA：Security Association（SA; セキュリティ アソシエーション）。SA は、データ フローに適用されるセキュリティ ポリシーおよびキー関連情報のインスタンスです。

TACACS+：Terminal Access Controller Access Control System Plus。TACACS+ は、ユーザによるルータまたはネットワーク アクセス サーバへのアクセス試行の集中的な確認を可能にするセキュリティ アプリケーションです。

TED：Tunnel Endpoint Discovery。TED は、ルータによる IPsec エンドポイントの検出を可能にする Cisco IOS ソフトウェア機能です。

VPN：Virtual Private Network（VPN; バーチャル プライベート ネットワーク）。VPN を使用すると、ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN では、「トンネリング」が使用され、すべての情報が IP レベルで暗号化されます。

VRF：VPN Routing/Forwarding（VRF; VPN ルーティング/転送）インスタンス。VRF は、IP ルーティング テーブル、取得された転送テーブル、その転送テーブルを使用する一連のインターフェイス、転送テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、PE ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。

VSA：Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）。VSA は、特定のベンダーによって実装されたアトリビュートです。Vendor-Specific アトリビュートが使用された結果、AV ペアがカプセル化されます。基本的は、Vendor-Specific = プロトコル :Attribute = 値となります。

XAUTH：Extended Authentication（XAUTH; 拡張認証）。XAUTH は、IKE フェーズ 1 と IKE フェーズ 2 の間における任意の交換です。XAUTH では、ルータが、（ピアの認証ではなく）実際のユーザの認証試行において、追加の認証情報を要求します。

（注） この用語集に記載されていない用語については、『*Internetworking Terms and Acronyms*』を参照してください。