ASA/PIX 8.x： CLI および ASDM によるダウンロード可能 ACL を使用した VPN アクセスの Radius の承認（ACS 4.x）の設定例

目次

概要

このドキュメントでは、セキュリティ アプライアンスをネットワーク アクセスのためにユーザを認証するように設定する方法について説明します。 暗黙的に RADIUS 許可をイネーブルにすることができるため、この項ではセキュリティ アプライアンスの RADIUS 許可の設定に関する情報は含まれません。 セキュリティ アプライアンスが RADIUS サーバから受信したアクセス リスト情報をどのように処理するかについて説明します。

アクセス リストをセキュリティ アプライアンスにダウンロードするように RADIUS サーバを設定できます。または、認証時にアクセス リスト名をダウンロードするようにも設定できます。 ユーザは、ユーザ固有のアクセス リストで許可された操作だけを認可されます。

ダウンロード可能なアクセス リストは、Cisco Secure ACS を使用して各サーバに適切なアクセス リストを提供する場合に最もスケーラブルな方法です。 ダウンロード可能アクセス リスト機能および Cisco Secure ACS の詳細については、『ダウンロード可能アクセス制御リストを送信する RADIUS サーバの設定』および『ダウンロード可能 IP ACL』を参照してください。

バージョン 8.3 以降の Cisco Adaptive Security Appliance（ASA）での ASDM を使用した同等な設定の詳細について『ASA 8.3.x 以降： バージョン 8.3 以降で共通の Cisco ASA での設定については、CLI および ASDM によるダウンロード可能 ACL を使用した VPN アクセスの Radius の承認（ACS 5.x）の設定例を参照してください。

前提条件

要件

このドキュメントでは、ASA が完全に動作していて、Cisco ASDM か CLI で設定を変更できるように設定されていることを想定しています。

注: 「ASDM 用の HTTPS アクセスの許可」または「PIX/ASA 7.x： 内部および外部インターフェイスの SSH の設定例」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 適応型セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降
- Cisco Adaptive Security Device Manager バージョン 5.x 以降
- Cisco VPN Client バージョン 4.x 以降
- Cisco Secure Access Control Server 4.x

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、Cisco PIX セキュリティ アプライアンス バージョン 7.x 以降にも適用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ダウンロード可能 IP ACL を使用すると、多数のユーザまたはユーザ グループに適用可能な ACL 定義のセットを作成できます。 これらの ACL 定義のセットは、ACL コンテンツと呼ばれます。 また、NAF を組み込むと、ユーザがアクセスするために使用する AAA クライアントに送信される ACL コンテンツを制御できます。 つまり、ダウンロード可能 IP ACL は 1 つ以上の ACL コンテンツ定義で構成され、各定義は NAF と関連付けられるか、または（デフォルトで）すべての

AAA クライアントに関連付けられます。 NAF は、AAA クライアントの IP アドレスに応じて、指定された ACL コンテンツの適用を制御します。 NAF の詳細、およびダウンロード可能な IP ACL を NAF が規制する方法については、ネットワーク アクセス フィルタの概要を参照してください。

ダウンロード可能 IP ACL は、次のように動作します。

1. ACS は、ネットワークへのユーザ アクセスを許可する場合、ダウンロード可能 IP ACL がそのユーザまたはそのユーザのグループに割り当てられているかどうかを判別します。
2. ACS は、ユーザまたはユーザのグループに割り当てられたダウンロード可能 IP ACL を確認する場合、RADIUS 認証要求を送信した AAA クライアントに関連付けられた ACL コンテンツ エントリが存在するかどうかを判別します。
3. ACS は、ユーザ セッションの RADIUS アクセス受け付けパケットの一部として、名前付き ACL および名前付き ACL のバージョンを指定する属性を送信します。
4. AAA クライアントが、現行バージョンの ACL がキャッシュにない（つまり、ACL が新しいか、変更されている）と応答すると、ACS は新しい ACL またはアップデートされた ACL をデバイスに送信します。

また、各ユーザまたはユーザ グループの RADIUS Cisco cisco-av-pair 属性 [26/9/1] での ACL の設定の代わりに、ダウンロード可能 IP ACL を使用することもできます。 ダウンロード可能 IP ACL を作成して名前を付けた後は、その名前を参照して、該当するユーザまたはユーザ グループのそれぞれにダウンロード可能 IP ACL を割り当てることができます。 ユーザまたはユーザ グループごとに RADIUS Cisco cisco-av-pair 属性を設定するよりも、このほうが効率的です。

さらに、NAF を使用することにより、同じユーザまたはユーザのグループに対して、使用している AAA クライアントに関して異なる ACL コンテンツを適用できます。 ACS からダウンロード可能 IP ACL を使用するように AAA クライアントを設定すれば、それ以外に AAA クライアントを設定する必要はありません。 ダウンロード可能 ACL は、確立されているバックアップ方式または複製方式によって保護されます。

ACS Web インターフェイスに ACL 定義を入力するとき、キーワードや名前エントリを使用しないでください。 その他のあらゆる点において、ダウンロード可能 IP ACL を適用しようとしている AAA クライアントの標準的な ACL コマンド構文およびセマンティクスを使用してください。 ACS に入力する ACL 定義は、1 つまたは複数の ACL コマンドによって構成されます。 各コマンドはそれぞれ別の行に入力されます。

ダウンロード可能 IP ACL には、名前付き ACL コンテンツを 1 つ以上追加できます。 デフォルトで、各 ACL コンテンツはすべての AAA クライアントに適用されます。ただし、NAF を定義している場合は、関連付ける NAF にリストされた AAA クライアントへの各 ACL コンテンツの適用を制限できます。 つまり、NAF を使用すると、単一のダウンロード可能 IP ACL 内で、ネットワーク セキュリティ計画に応じて複数の異なるネットワーク デバイスまたはネットワーク デバイス グループに各 ACL コンテンツを適用することができます。

また、ダウンロード可能 IP ACL 内にある ACL コンテンツの順序を変更することもできます。 ACS は、テーブルの先頭から ACL コンテンツの検査を開始して、使用されている AAA クライアントを含む NAF で最初に見つかった ACL コンテンツをダウンロードします。 順序を設定するときは、最も広範に適用できる ACL の内容をリストの上部に配置すると、システムを効率的にできます。 部分的に重複する AAA クライアントが NAF に含まれている場合には、より具体的な ACL コンテンツからより一般的な ACL コンテンツの順に配置しなければならないことを認識する必要があります。 たとえば、ACS は、[All-AAA-Clients] の NAF 設定に関連付けられた ACL コンテンツをすべてダウンロードし、リスト内のそれよりも下位の ACL コンテンツはすべて無視します。

特定の AAA クライアントでダウンロード可能 IP ACL を使用するには、AAA クライアントが次の指示に従う必要があります。

- 認証に RADIUS を使用する
- ダウンロード可能 IP ACL をサポートしている

ダウンロード可能 IP ACL をサポートする Cisco デバイスの例を次に示します。

- ASA および PIX デバイス
- VPN 3000 シリーズ コンセントレータ
- IOS バージョン 12.3(8)T 以降を実行するシスコ デバイス

次の例は、[ACL Definitions] ボックスで VPN 3000/ASA/PIX 7.x+ ACL の入力に使用する必要がある形式を示しています。

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらは RFC 1918 でのアドレスであり、ラボ環境で使用されたものです。

リモート アクセス VPN（IPSec）の設定

ASDM の手順

リモート アクセス VPN を設定するには、次の手順を実行します。

1. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [IKE Policies] > [Add] を選択し、ISAKMP ポリシーを作成します。
2. ISAKMP ポリシーの詳細情報を次のように設定します。[OK]、[Apply] の順にクリックします。
3. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec]

> [IKE Parameters] を選択し、外部インターフェイス上の IKE を有効にします。

4. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [IPSec Transform Sets] > [Add] の順に選択し、次のように **ESP-3DES-SHA** トランスフォームを作成します。[OK]、[Apply] の順にクリックします。
5. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPSec] > [Crypto Maps] > [Add] の順に選択し、次のような Priority 1 のダイナミック ポリシーを持つ暗号マップを作成します。[OK]、[Apply] の順にクリックします。
6. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択して [Add] をクリックし、VPN クライアント ユーザの VPN クライアントを追加します。
7. [Configuration] > [Remote Access VPN] > [AAA Setup] > [AAA Server Groups] を選択して [Add] をクリックし、AAA サーバのグループ名とプロトコルを追加します。AAA サーバの IP アドレス (ACS) とこのサーバが接続するインターフェイスを追加します。 [RADIUS Parameters] エリアでサーバ秘密キーも追加します。 [OK] をクリックします。
8. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [IPSec Connection Profiles] > [Add] を選択し、次のようにトンネル グループを追加します (たとえば、**TunnelGroup1** を追加し、事前共有鍵を cisco123 に設定します) 。[Basic] タブの [User Authentication] フィールドで、サーバ グループとして [vpn] を選択します。VPN クライアント ユーザの [Client Address Pools] として [vpnclient] を選択します。[OK] をクリックします。
9. IPSec アクセスの [outside] インターフェイスを有効にします。 [Apply] をクリックして、次に進みます。

CLI による ASA/PIX の設定

後述のステップを実行して DHCP サーバを設定し、コマンドラインから VPN Client に IP アドレスを割り当てます。 使用する各コマンドについての詳細は、『リモート アクセス VPN の設定』または『Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、コマンド リファレンス』を参照してください。

ASA デバイスでの実行コンフィギュレーション

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif DMZ security-level 100 ip
address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.1
255.255.255.0 !--- Output is suppressed. passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-
k8.bin ftp mode passive access-list 101 extended permit
ip 10.1.1.0 255.255.255.0 192.168.5.0 255.255.255.0 !---
Radius Attribute Filter access-list new extended deny ip
any host 10.1.1.2 access-list new extended permit ip any
any pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.1-192.168.5.10
mask 255.255.255.0 no failover icmp unreachable rate-
```

```
limit 1 burst-size 1 !--- Specify the location of the
ASDM image for ASA to fetch the image for ASDM access.
asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 global (outside) 1 192.168.1.5 nat
(inside) 0 access-list 101 nat (inside) 1 0.0.0.0
0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy !---
Create the AAA server group "vpn" and specify the
protocol as RADIUS. !--- Specify the CSACS server as a
member of the "vpn" group and provide the !--- location
and key. aaa-server vpn protocol radius max-failed-
attempts 5 aaa-server vpn (DMZ) host 172.16.1.1 retry-
interval 1 timeout 30 key cisco123 http server enable
http 0.0.0.0 0.0.0.0 inside no snmp-server location no
snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. !--- A Triple DES encryption with !---
the sha hash algorithm is used. crypto ipsec transform-
set ESP-3DES-SHA esp-3des esp-sha-hmac !--- Defines a
dynamic crypto map with !--- the specified encryption
settings. crypto dynamic-map outside_dyn_map 1 set
transform-set ESP-3DES-SHA !--- Binds the dynamic map to
the IPsec/ISAKMP process. crypto map outside_map 1
ipsec-isakmp dynamic outside_dyn_map !--- Specifies the
interface to be used with !--- the settings defined in
this configuration. crypto map outside_map interface
outside !--- PHASE 1 CONFIGURATION ---! !--- This
configuration uses ISAKMP policy 2. !--- The
configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 2 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 no
crypto isakmp nat-traversal telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection basic-threat
threat-detection statistics access-list ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
! group-policy DfltGrpPolicy attributes vpn-tunnel-
protocol IPSec webvpn group-policy GroupPolicy1 internal
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (VPN) with the tunnel group. tunnel-group
TunnelGroup1 type remote-access tunnel-group
TunnelGroup1 general-attributes address-pool vpnclient
authentication-server-group vpn !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

Cisco VPN Client の設定

ASA の設定に成功したことを確認するには、Cisco VPN Client を使用して Cisco ASA に接続してみます。

1. [Start] > [Programs] > [Cisco Systems VPN Client] > [VPN Client] の順に選択します。
2. **[New]** をクリックして、[Create New VPN Connection Entry] ウィンドウを開きます。
3. 新しい接続の詳細情報を入力します。接続エントリの名前と説明を入力します。 Host ボックスに、**ASA の Outside の IP アドレス**を入力します。 次に、ASA で設定されている VPN トンネル グループ名（TunnelGroup1）とパスワード（事前共有鍵 - cisco123）を入力します。 [Save] をクリックします。
4. 使用する接続をクリックし、VPN Client メイン ウィンドウの [Connect] をクリックします。
5. プロンプトが表示されたら、**Username : cisco**、[Password:] に **password1** と入力し、[OK] をクリックしてリモート ネットワークに接続します。
6. VPN Client が中央サイトの ASA に接続されます。
7. 接続が正常に確立されたら、Status メニューから [Statistics] を選択し、トンネルの詳細情報を確認します。

個々のユーザのダウンロード可能 ACL を使用した ACS の設定

Cisco Secure ACS 上のダウンロード可能なアクセス リストを共有プロファイル コンポーネントとして設定し、そのアクセス リストをグループまたは個々のユーザに割り当てることができます。

ダイナミック アクセス リストを実装するには、これをサポートするように RADIUS サーバを設定する必要があります。 ユーザが認証されると、RADIUS サーバからセキュリティ アプライアンスにダウンロード可能なアクセス リストまたはアクセス リスト名が送信されます。 所定のサービスへのアクセスがアクセス リストによって許可または拒否されます。 認証セッションがタイムアウトになると、このアクセス リストはセキュリティ アプライアンスから削除されます。

この例では、IPsec VPN ユーザ **cisco** が正常に認証され、ダウンロード可能なアクセス リストが RADIUS サーバからセキュリティ アプライアンスに送信されます。 ユーザ「cisco」は 10.1.1.2 サーバのみにアクセスでき、その他すべてのアクセスを拒否します。 ACL を確認するには、「ユーザ/グループのダウンロード可能 ACL」を参照してください。

Cisco Secure ACS で RADIUS を設定するには、次の手順を実行してください。

1. 左側で [Network Configuration] を選択し、[Add Entry] をクリックして、RADIUS サーバ データベースに ASA のエントリを追加します。
2. クライアント IP アドレス フィールドに **172.16.1.2** と入力し、共有秘密キー フィールドに **"cisco123"** と入力します。 [Authenticate Using] ドロップダウン ボックスから [RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)] を選択します。 [Submit] をクリックします。
3. Cisco Secure データベースの [User] フィールドにユーザ名を入力してから、[Add/Edit] をクリックします。この例でのユーザ名は **cisco** です。
4. 次のウィンドウで、**cisco** のパスワードを入力します。 この例でも、パスワードは **password1** です。 終了したら、[Submit] をクリックします。
5. [Advanced Options] ページでは、ACS で表示される高度なオプションを決定できます。 使用しない高度なオプションを非表示にすると、ACS Web インターフェイスの他の領域に表

示されるページをシンプルにできます。 [Interface Configuration] をクリックし、次に [Advanced Options] をクリックして [Advanced Options] ページを表示します。[User-Level Downloadable ACLs] および [Group-Level Downloadable ACLs] チェックボックスをオンにします。[User-Level Downloadable ACLs]：このオプションをオンにすると、[Downloadable ACLs] セクションが [User Setup] ページでイネーブルになります。[Group-Level Downloadable ACLs]：このオプションをオンにすると、[Downloadable ACLs] セクションが [Group Setup] ページでイネーブルになります。

6. ナビゲーション バーの [Shared Profile Components] をクリックし、[Downloadable IP ACLs] を選択します。**注:** [Downloadable IP ACLs] が [Shared Profile Components] ページに表示されない場合は、[Interface Configuration] セクションの [Advanced Options] ページで、[User-Level Downloadable ACLs] オプションまたは [Group-Level Downloadable ACLs] オプション、あるいはその両方をイネーブルにする必要があります。
7. [Add] をクリックします。 [Downloadable IP ACLs] ページが表示されます。
8. [Name] ボックスに、新しい IP ACL の名前を入力します。**注:** IP ACL の名前には、最大で 27 文字まで使用できます。 名前にスペースまたは次の文字を含めることはできません。 ハイフン (-) 、左角カッコ ([ ) 、右角カッコ ( ]) 、スラッシュ (/) 、引用符 (") 、左山形カッコ (<) 、右山形カッコ (>) 、ハイフン (-) 。[Description] ボックスに、新しい IP ACL の説明を入力します。 説明には、最大で 1,000 文字まで使用できます。新しい IP ACL に ACL コンテンツを追加するには、[Add] をクリックします。
9. [Name] ボックスに、新しい ACL コンテンツの名前を入力します。**注:** ACL コンテンツの名前には、最大で 27 文字まで使用できます。 名前にスペースまたは次の文字を含めることはできません。 ハイフン (-) 、左角カッコ ([ ) 、右角カッコ ( ]) 、スラッシュ (/) 、引用符 (") 、左山形カッコ (<) 、右山形カッコ (>) 、ハイフン (-) 。[ACL Definitions] ボックスに、新しい ACL 定義を入力します。**注:** ACS Web インターフェイスに ACL 定義を入力するとき、キーワードや名前エントリを使用しないでください。 代わりに、permit または deny キーワードで開始します。ACL コンテンツを保存するには、[Submit] をクリックします。
10. [Downloadable IP ACLs] ページが表示され、新しい ACL コンテンツが [ACL Contents] カラムに名前順で示されます。 ACL コンテンツに NAF を関連付けるには、新しい ACL コンテンツの右側にある [Network Access Filtering] ボックスから NAF を選択します。 デフォルトでは、NAF は [(All-AAA-Clients)] に設定されます。 NAF を割り当てない場合、ACS は ACL コンテンツをすべてのネットワーク デバイスに関連付けます。この処理がデフォルトです。ACL コンテンツの順序を設定するには、ACL 定義のオプション ボタンをクリックしてから、[Up] または [Down] をクリックして、リスト内の ACL コンテンツの位置を変更します。IP ACL を保存するには、[Submit] をクリックします。**注:** ACL コンテンツの順序は非常に重要です。 ACS は先頭から順に検査を開始し、該当する NAF 設定 ([All-AAA-Clients] デフォルト設定を含む) を持つ最初の ACL 定義だけをダウンロードします。通常、ACL コンテンツのリストは、最も具体的な (限定された) NAF の ACL コンテンツから最も一般的な ([All-AAA-Clients]) NAF の ACL コンテンツの順に検査されます。**注:** ACS によって新しい IP ACL が入力され、すぐに有効になります。 たとえば、IP ACL を PIX Firewall 用に使用する場合、ユーザ プロファイルまたはグループ プロファイルにそのダウンロード可能 IP ACL が割り当てられたユーザを認証しようとしている PIX Firewall すべてに対して、IP ACL を送信できます。
11. [User Setup] ページに移動し、[User] ページを編集します。 [Downloadable ACLs] セクションで [Assign IP ACL:] チェックボックスをオンにします。 チェックボックスをオンにします。 リストから IP ACL を選択します。 ユーザ アカウント オプションの設定が完了したら、[Submit] をクリックしてオプションを記録します。

グループのダウンロード可能 ACL を使用した ACS の設定

「個々のユーザのダウンロード可能 ACL を使用した ACS の設定」のステップ 1 から 9 を完了した後、以下のステップに従って Cisco Secure ACS でグループ用のダウンロード可能 ACL を設定します。

この例の IPsec VPN ユーザ「cisco」は VPN グループに属しています。 VPN グループ ポリシーはグループ内のすべてのユーザに適用されます。

VPN グループ ユーザ「**cisco**」は正常に認証され、RADIUS サーバがダウンロード可能なアクセス リストをセキュリティ アプライアンスに送信します。 ユーザ「cisco」は 10.1.1.2 サーバのみにアクセスでき、その他すべてのアクセスを拒否します。 ACL を確認するには、「ユーザ/グループのダウンロード可能 ACL」を参照してください。

1. ナビゲーション バーの [Group Setup] をクリックします。 [Group Setup Select] ページが表示されます。
2. Group 1 の名前を **VPN** に変更してから、[Submit] をクリックします。
3. [Group] リストでグループを選択し、[Edit Settings] をクリックします。
4. [Downloadable ACLs] セクションの [Assign IP ACL:] チェックボックスをオンにします。 リストから IP ACL を選択します。
5. グループ設定を保存するには、[Submit] をクリックします。
6. [User Setup] に進み、グループ **VPN** に追加するユーザを編集します。 終了したら、[Submit] をクリックします。**これで、VPN グループに設定されたダウンロード可能 ACL がこのユーザにも適用されるようになります。**
7. 他のグループ設定を続ける場合は、必要に応じて、この章の手順を実行します。

ユーザ グループの IETF RADIUS の設定

ユーザ認証時に、セキュリティ アプライアンスで作成済みのアクセス リストの名前を RADIUS サーバからダウンロードするには、IETF RADIUS filter-id 属性（属性番号 11）を次のように設定します。

```
filter-id=acl_name
```

VPN グループ ユーザ **cisco** は正常に認証され、セキュリティ アプライアンスで作成済みのアクセス リストの ACL 名（new）が RADIUS サーバによってダウンロードされます。 ユーザ「cisco」は、10.1.1.2 サーバを**除き**、ASA のネットワーク内のすべてのデバイスにアクセスできます。 ACL を確認するには、「Filter-Id ACL」を参照してください。

この例では、ASA でのフィルタリング用に **new** という名前の ACL を設定しています。

```
access-list new extended deny ip any host 10.1.1.2 access-list new extended permit ip any any
```

IETF RADIUS 設定パラメータは、次の条件が満たされる場合に限り表示されます。 次のように設定済みであること

- [Network Configuration] で、AAA クライアントが RADIUS プロトコルのいずれかを使用する
- Web インターフェイスの [Interface Configuration] セクションの [RADIUS (IETF)] ページで、グループ レベルの RADIUS 属性がイネーブルになっている。

RADIUS 属性は、ACS から要求側の AAA クライアントに各ユーザ用のプロファイルとして送信されます。

現在のグループの各ユーザに対する認可として適用される IETF RADIUS 属性を設定するには、次の操作を実行します。

1. ナビゲーション バーの [Group Setup] をクリックします。[Group Setup Select] ページが表示されます。
2. [Group] リストでグループを選択し、[Edit Settings] をクリックします。[Group Settings] ページの一番上にそのグループの名前が表示されます。
3. [IEFT RADIUS Attributes] にスクロールします。 各 IETF RADIUS 属性に対して、現在のグループを認可する必要があります。 [[011] Filter-Id] 属性のチェックボックスをオンにしてから、この属性の認可として ASA 定義の ACL 名（new）をフィールドに追加します。 ASA の *show running configuration* の出力を参照してください。
4. グループ設定を保存してすぐに適用するには、[Submit]、[Apply] の順にクリックします。**注**: グループ設定を保存して後で適用するには、[Submit] をクリックします。 変更を実装する準備ができたら、[System Configuration] > [Service Control] を選択します。 次に、[Restart] を選択します。

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

show crypto コマンド

- **show crypto isakmp sa**：ピアの現在の IKE セキュリティ アソシエーション（SA）すべてを表示します。`ciscoasa# sh crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 192.168.10.2 Type : user Role : responder Rekey : no State : AM_ACTIVE ciscoasa#`
- **show crypto ipsec sa**：現在の SA が使用している設定を表示します。`ciscoasa# sh crypto ipsec sa interface: outside Crypto map tag: outside_dyn_map, seq num: 1, local addr: 192.168.1.1 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0) current_peer: 192.168.10.2, username: cisco dynamic allocated peer ip: 192.168.5.1 #pkts encaps: 65, #pkts encrypt: 65, #pkts digest: 65 #pkts decaps: 65, #pkts decrypt: 65, #pkts verify: 65 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.10.2 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: EEF0EC32 inbound esp sas: spi: 0xA6F92298 (2801345176) transform: esp-3des esp-sha-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 86016, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 28647 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xEEF0EC32 (4008766514) transform: esp-3des esp-sha-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 86016, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 28647 IV size: 8 bytes replay detection support: Y`

ユーザ/グループのダウンロード可能 ACL

ユーザ cisco のダウンロード可能 ACL を確認します。 ACL は、CSACS からダウンロードされます。

```
ciscoasa(config)# sh access-list access-list cached ACL log flows: total 0, denied 0 (deny-flow-
```

```
max 4096) alert-interval 300 access-list 101; 1 elements access-list 101 line 1 extended permit
ip 10.1.1.0 255.255.255.0 192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411 access-list #ACSACL#-
IP-VPN_Access-49bf68ad; 2 elements (dynamic) access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1
extended permit ip any host 10.1.1.2 (hitcnt=2) 0x334915fe access-list #ACSACL#-IP-VPN_Access-
49bf68ad line 2 extended deny ip any any (hitcnt=40) 0x7c718bd1
```

filter-id ACL

[011] Filter-Id がグループ VPN に適用され、このグループのユーザは ASA で定義された ACL (new) に従ってフィルタリングされます。

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0,
   denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
   255.255.255.0 192.168.5.0 255.255.255.0
   (hitcnt=0) 0x8719a411
access-list new; 2 elements
access-list new line 1 extended deny ip any host 10.1.1.2 (hitcnt=4) 0xb247fec8 access-list new
line 2 extended permit ip any any (hitcnt=39) 0x40e5d57c
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。 デバッグ出力例も紹介しています。

注: リモートアクセス IPSec VPN の詳細は、『一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について』を参照してください。

セキュリティ アソシエーションのクリア

トラブルシューティングを行う際には、変更を加えた後、既存のセキュリティ アソシエーションを必ずクリアしてください。 PIX の特権モードで、次のコマンドを使用します。

- **clear [crypto] ipsec sa**：アクティブな IPSec SA を削除します。 crypto キーワードはオプションです。
- **clear [crypto] ipsec sa**：アクティブな IKE SA を削除します。 crypto キーワードはオプションです。

トラブルシューティングのためのコマンド

Output Interpreter Tool (OIT) (登録ユーザ専用) では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug crypto ipsec 7**：フェーズ 2 の IPSec ネゴシエーションを表示します。
- **debug crypto isakmp 7**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに関するサポート ページ
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、コマンド リファレンス
- Cisco PIX 500 シリーズ セキュリティ アプライアンス サポート ページ
- Cisco Adaptive Security Device Manager
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- Cisco VPN Client に関するサポート ページ
- Cisco Secure Access Control Server for Windows
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems