ASA 8.3 以降： 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

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。 RADIUS 認可は暗黙的に有効にできるので、このドキュメントではセキュリティ アプライアンスでの RADIUS 認可の設定については説明しません。 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。

Cisco Secure Access Control Server（ACS）を使用してユーザごとに適切なアクセス リストを提供するときは、ダウンロード可能アクセス リストが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。

Cisco ASA バージョン 8.2 以前での同様の設定について詳しくは、『ASA/PIX 8.x： CLI および ASDM でダウンロード可能 ACL を使用してネットワーク アクセスの RADIUS 認可（ACS）を設定する例』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、適応型セキュリティ アプライアンス（ASA）が完全に動作していて、Cisco Adaptive Security Device Manager（ASDM）か CLI 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 または Secure Shell（SSH）でデバイスをリモートから設定できるようにする方法については、『ASDM 用の HTTPS アクセスの許可』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 ASA ソフトウェア バージョン 8.3 以降
- Cisco ASDM バージョン 6.3 以降
- Cisco VPN Client バージョン 5.x 以降
- Cisco Secure ACS 5.x

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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。

ダウンロード可能 IP ACL は、次のように動作します。

1. ACS は、ユーザにネットワークへのアクセスを許可するとき、ダウンロード可能 IP ACL が結果セクションで認可プロファイルに割り当てられているかどうかを判断します。
2. ACS は、認可プロファイルに割り当てられているダウンロード可能 IP ACL を特定すると、

名前付き ACL を指定する属性（ユーザ セッションの一部として、RADIUS access-accept パケット内）および名前付き ACL のバージョンを送信します。
3. 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ると、その名前を参照すれば、どの認可プロファイルにもダウンロード可能 IP ACL を割り当てることができます。 この方法は、RADIUS Cisco cisco-av-pair 属性を認可プロファイル用に設定する場合よりも効率的です。

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。

ACS では、複数のダウンロード可能 IP ACL を定義し、さまざまな認可プロファイルでそれを使用できます。 アクセス サービス認可ルールの条件に基づいて、ダウンロード可能 IP ACL を含むさまざまな認可プロファイルをさまざまな AAA クライアントに送信できます。

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 ACL の内容をテーブルの上部から検討し、最初に見つかった ACL の内容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。

ダウンロード可能 IP ACL を特定の AAA クライアントで使用するには、AAA クライアントが次のルール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
- IOS バージョン 12.3(8)T 以降を実行する Cisco デバイス

ACL 定義ボックスに ASA ACL を入力するために使用する必要がある形式の例を次に示します。

```
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。

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. ホーム ウィンドウから [Wizards] > [VPN Wizards] > [IPsec(IKEv1) Remote Access VPN Wizard] を選択します。
2. 必要に応じて [VPN Tunnel Interface] を選択し（この例では [Outside]）、[Enable inbound IPsec sessions to bypass interface access lists] の横にあるチェックボックスがオンになっていることを確認します。
3. [Cisco VPN Client, Release 3.x or higher] として VPN クライアント タイプを選択します。 [Next] をクリックします。
4. [Authentication Method] を選択し、認証情報を指定します。 ここで使用する認証方法は [Pre-Shared Key] です。 表示されているスペースに**トンネル グループ**の名前も指定します。 ここで使用する [Pre-shared Key] は [cisco123]、[Tunnel Group Name] は [Cisco-Tunnel] です。 [Next] をクリックします。
5. リモート ユーザの認証用にローカル ユーザのデータベースか外部 AAA サーバ グループを選択します。 ここでは [Authenticate using an AAA server group] を選択します。 新しい AAA サーバ グループ名を作成するには、[AAA Server Group Name] フィールドの横にある [New] をクリックします。
6. サーバ グループ名、認証プロトコル、サーバ IP アドレス、インターフェイス名、サーバ秘密鍵を、表示されるそれぞれのスペースに指定し、[OK] をクリックします。
7. [Next] をクリックします。
8. 接続時にリモート VPN クライアントにダイナミックに割り当てられるローカル アドレスのプールを定義します。 ローカル アドレスの新しいプールを作成するには、[New] をクリックします。
9. [Add IP Pool] ウィンドウで、プール名、開始 IP アドレス、終了 IP アドレス、サブネット マスクを入力します。 [OK] をクリックします。
10. ドロップダウン リストからプール名を選択し、[Next] をクリックします。 この例のプール名は、手順 9 で作成した **Sample-Pool** です。
11. *オプション：* DNS と WINS のサーバ情報、およびリモート VPN Client にプッシュするデフォルトのドメイン名を指定します。
12. リモート VPN ユーザに公開するホストやネットワークが存在する場合は、これを指定します。 除外するインターフェイス名とネットワークを [Exempt Networks] フィールドに入力してから [Next] をクリックします。このリストを空白にしておくと、リモート VPN ユーザは ASA の Inside ネットワーク全体にアクセスできることになります。このウィンドウでは、スプリット トンネリングを有効にすることもできます。 スプリット トンネリング

では、ここまでで指定したリソースへのトラフィックは暗号化されますが、一般にインターネットに対してはトラフィックのトンネル化は行われず、非暗号化アクセスが行われます。 スプリット トンネリングが*有効にされていない*場合、リモート VPN ユーザからのすべてのトラフィックは ASA に対してトンネリングされます。 この場合、設定によっては、帯域幅とプロセッサへの負荷が増大する可能性があります。

13. このウィンドウにはユーザが行った操作の概要が表示されます。 設定に問題がなければ、[Finish] をクリックします。

CLI による ASA の設定

CLI 設定を以下に示します。

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 8.4(3)
!
!--- Specify the hostname for the Security Appliance.
hostname ciscoasa enable password y.tvDXf6yFbMTAdD
encrypted passwd 2KFQnbNIdI.2KYOU encrypted names ! !---
Configure the outside and inside interfaces. interface
Ethernet0/0 nameif dmz security-level 50 ip address
192.168.26.13 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! interface Ethernet0/2 nameif outside
security-level 0 ip address 172.16.1.1 255.255.255.0 !
!--- Output is suppressed. boot system disk0:/asa843-
k8.bin ftp mode passive object network
NETWORK_OBJ_10.1.1.0_24 subnet 10.1.1.0 255.255.255.0
object network NETWORK_OBJ_10.2.2.0_24 subnet 10.2.2.0
255.255.255.0 access-list OUTIN extended permit icmp any
any !--- This is the Access-List whose name will be sent
by !--- RADIUS Server(ACS) in the Filter-ID attribute.
access-list new extended permit ip any host 10.1.1.2
access-list new extended deny ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500

ip local pool Sample-Pool 10.2.2.1-10.2.2.254 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-647.bin no asdm history enable arp timeout
14400 !--- Specify the NAT from internal network to the
Sample-Pool. nat (inside,outside) source static
NETWORK_OBJ_10.1.1.0_24 NETWORK_OBJ_10.1.1.0_24
destination static NETWORK_OBJ_10.2.2.0_24
NETWORK_OBJ_10.2.2.0_24 no-proxy-arp route-lookup
access-group OUTIN in interface outside !--- Create the
AAA server group "ACS5" and specify the protocol as
```

```
RADIUS. !--- Specify the ACS 5.x server as a member of
the "ACS5" group and provide the !--- location and key.
aaa-server ACS5 protocol radius
aaa-server ACS5 (dmz) host 192.168.26.51
timeout 5
key *****

aaa authentication http console LOCAL
http server enable 2003
http 0.0.0.0 0.0.0.0 inside


!--- PHASE 2 CONFIGURATION ---! !--- The encryption &
hashing types for Phase 2 are defined here. We are using
!--- all the permutations of the PHASE 2 parameters.
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-
aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-
aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-
aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-
aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes
esp-md5-hmac


!--- Defines a dynamic crypto map with !--- the
specified transform-sets created earlier. We are
specifying all the !--- transform-sets. crypto dynamic-
map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-
set
   ESP-AES-128-SHA ESP-AES-128-MD5
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-
256-MD5 ESP-3DES-SHA
   ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5

!--- Binds the dynamic map to the IPsec/ISAKMP process.
crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_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 policies defined with all the permutation !-
-- of the 5 ISAKMP parameters. The configuration
commands here define the !--- Phase 1 policy parameters
that are used. crypto ikev1 enable outside

crypto ikev1 policy 10
authentication crack
encryption aes-256
```

```
hash sha
group 2
lifetime 86400

crypto ikev1 policy 20
authentication rsa-sig
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 40
authentication crack
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 70
authentication crack
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 80
authentication rsa-sig
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 90
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 100
authentication crack
encryption 3des
hash sha
```

```
group 2
lifetime 86400

crypto ikev1 policy 110
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 120
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 130
authentication crack
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 140
authentication rsa-sig
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 150
authentication pre-share
encryption des
hash sha
group 2
lifetime 86400


webvpn
group-policy Cisco-Tunnel internal
group-policy Cisco-Tunnel attributes
vpn-tunnel-protocol ikev1
default-domain value cisco.com
username admin password CdOTKv3uhDhHIw3A encrypted
privilege 15
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (ACS5) with the tunnel group. tunnel-group Cisco-
Tunnel type remote-access tunnel-group Cisco-Tunnel
general-attributes
address-pool Sample-Pool
authentication-server-group ACS5
default-group-policy Cisco-Tunnel

!--- Enter the pre-shared-key to configure the
authentication method. tunnel-group Cisco-Tunnel ipsec-
attributes
ikev1 pre-shared-key *****

prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d
: end
ASA#
```

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

ダウンロード可能アクセス リストを Cisco Secure ACS 5.x で名前付き権限オブジェクトとして設定してから、認可プロファイルに割り当てることができます。認可プロファイルは Access-Service のルールの結果セクションで選択されます。

この例では、IPsec VPN ユーザ **cisco** が正常に認証し、RADIUS サーバはダウンロード可能アクセス 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。

Cisco Secure ACS 5.x に RADIUS クライアントを設定するには、次の手順を実行します。

1. ASA 用のエントリを RADIUS サーバ データベースに追加するには、[Network Resources] > [Network Devices and AAA Clients] を選択し、[Create] をクリックします。
2. ローカルで有意な ASA 名（この例では **sample-asa**）を入力し、IP アドレス フィールドに「**192.168.26.13**」と入力します。 [Authentication Options] セクションで [RADIUS] チェックボックスをオンにして **RADIUS** を選択し、[Shared Secret] フィールドに「**cisco123**」と入力します。 [Submit] をクリックします。
3. ASA が RADIUS サーバ（ACS）データベースに正常に追加されます。
4. VPN 認証用の ACS のローカル データベースにユーザを作成するには、[Users and Identity Stores] > [Internal Identity Stores] > [Users] を選択し、[Create] をクリックします。
5. ユーザ名「**cisco**」を入力します。 パスワード タイプを [Internal Users] として選択し、パスワード（この例では **cisco123**）を入力します。 パスワードを確認し、[Submit] をクリックします。
6. ユーザ **cisco** が正常に作成されます。
7. ダウンロード可能 ACL を作成するには、[Policy Elements] > [Authorization and Permissions] > [Named Permission Objects] > [Downloadable ACLs] を選択し、[Create] をクリックします。
8. ダウンロード可能 ACL の**名前**および **ACL の内容** を指定します。 [Submit] をクリックします。
9. ダウンロード可能 ACL **Sample-DACL** が正常に作成されます。
10. VPN 認証の Access-Policies を設定するには、[Access Policies] > [Access Services] > [Service Selection Rules] を選択し、どのサービスが RADIUS プロトコルに対応しているかを判断します。 この例では **Rule 1** が **RADIUS** に一致し、デフォルト ネットワーク アクセスが RADIUS 要求に対応します。
11. 手順 10 で判断した**アクセス サービス**を選択します。 この例では**デフォルト ネットワーク アクセス**を使用します。 **許可された Protocols タブを**選択し、**PAP/ASCII を許可し、MS-CHAPv2 を**選択される**許可しなさい**ことを確かめて下さい。[Submit] をクリックします。
12. [Access Services] の [Identity Section] をクリックし、[Identity Source] として [Internal Users] が選択されていることを確認します。 この例では、デフォルト ネットワーク アクセスを受け入れます。
13. [Access Policies] > [Access Services] > [Default Network Access] > [Authorization] を選択し、[Customize] をクリックします。
14. 移動**システム: 使用できる列**からの**選択した列**への**ユーザ名は**、『OK』 をクリック し。
15. 新しいルールを作成するには、[Create] をクリックします。
16. **システム**の隣のチェックボックスことを確かめて下さい: **ユーザ名は**選択され、ドロップダウン リストから**等号を**選択し、ユーザ名 **cisco を**入力します。
17. [Select] をクリックします。

18. 新しい認可プロファイルを作成するには、[Create] をクリックします。
19. **認可プロファイル**の名前を指定します。 この例では、「**Sample-Profile**」を使用しています。
20. [Common Tasks] タブを選択し、[Downloadable ACL Name] のドロップダウン リストから [Static] を選択します。 新しく作成した **DACL**（[Sample-DACL]）を [Value] ドロップダウン リストから選択します。
21. [Submit] をクリックします。
22. [Sample-Profile]（新しく作成した認可プロファイル）の横にあるチェックボックスがオンになっていることを確認し、[OK] をクリックします。
23. 新しく作成した [Sample-Profile] が [Authorization Profiles] フィールドで選択されていることを確認し、[OK] をクリックします。
24. 新しいルール（**Rule-2**）がシステムで作成されることを確認して下さい: ユーザ名は結果として **cisco** 状態および**サンプルプロファイルに匹敵します**。 [Save Changes] をクリックします。 Rule 2 が正常に作成されます。

グループのダウンロード可能 ACL を使用した ACS の設定

Cisco Secure ACS でグループのダウンロード可能 ACL を設定するには、「ユーザごとのダウンロード可能 ACL 用の ACS の設定」の手順 1 から 12 を実行してから次の手順を実行します。

この例では、IPsec VPN ユーザ「cisco」は **Sample-Group** に所属しています。

Sample-Group ユーザ **cisco** が正常に認証し、RADIUS サーバはダウンロード可能アクセス 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. 新しいグループを作成するには、ナビゲーション バーの [Users and Identity Stores] > [Identity Groups] をクリックし、[Create] をクリックします。
2. グループ名（**Sample-Group**）を指定し、[Submit] をクリックします。
3. [User Identity Stores] > [Internal Identity Stores] > [Users] を選択し、ユーザ **cisco** を選択します。 このユーザのグループ メンバシップを変更するには、[Edit] をクリックします。
4. [Identity Group] の横にある [Select] をクリックします。
5. 新しく作成したグループ（**Sample-Group**）を選択し、[OK] をクリックします。
6. [Submit] をクリックします。
7. 新しいルールを作成するには、[Access Policies] > [Access Services] > [Default Network Access] > [Authorization] を選択し、[Create] をクリックします。
8. [Identity Group] の横にあるチェックボックスがオンになっていることを確認し、[Select] をクリックします。
9. [Sample-Group] を選択し、[OK] をクリックします。
10. [Authorization Profiles] セクションで [Select] をクリックします。
11. 新しい認可プロファイルを作成するには、[Create] をクリックします。
12. **認可プロファイル**の名前を指定します。 この例では「**Sample-Profile**」という名前を使用しています。
13. [Common Tasks] タブを選択し、[Downloadable ACL Name] のドロップダウン リストから [Static] を選択します。 新しく作成した **DACL**（[Sample-DACL]）を [Value] ドロップダウン リストから選択します。
14. [Submit] をクリックします。

15. 以前作成した認可プロファイル [Sample-Profile] を選択し、[OK] をクリックします。
16. [OK] をクリックします。
17. **Rule-1** が作成され、[Identity Group] が [Sample-Group]、[Result] が [Sample-Profile] になっていることを確認します。 [Save Changes] をクリックします。

ネットワーク デバイス グループのダウンロード可能 ACL 用の ACS の設定

Cisco Secure ACS でネットワーク デバイス グループのダウンロード可能 ACL を設定するには、「ユーザごとのダウンロード可能 ACL 用の ACS の設定」の手順 1 から 12 を実行してから次の手順を実行します。

この例では、RADIUS クライアント（ASA）がネットワーク デバイス グループ **VPN-Gateways** に所属します。ASA からのユーザ「cisco」の VPN 認証要求は正常に認証され、RADIUS サーバはダウンロード可能アクセス 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. 新しいネットワーク デバイス グループを作成するには、[Network Resources] > [Network Device Groups] > [Device Type] を選択し、[Create] をクリックします。
2. **ネットワーク デバイス グループ**名（この例では **VPN-Gateways**）を指定し、[Submit] をクリックします。
3. [Network Resources] > [Network Devices and AAA Clients] を選択し、以前作成した **RADIUS** クライアント **sample-asa** を選択します。 RADIUS クライアント（asa）の**ネットワーク デバイス グループ**のメンバシップを変更するには、[Edit] をクリックします。
4. [Device Type] の横にある [Select] をクリックします。
5. 新しく作成したネットワーク デバイス グループ（**VPN-Gateways**）を選択し、[OK] をクリックします。
6. [Submit] をクリックします。
7. [Access Policies] > [Access Services] > [Default Network Access] > [Authorization] を選択し、[Customize] をクリックします。
8. 移動 **NDG: 利用可能な**セクションからの**選択したセクション**への**デバイスの種類は**、『OK』 をクリック し。
9. 新しいルールを作成するには、[Create] をクリックします。
10. **NDG** の隣のチェックボックスことを確かめて下さい: **デバイスの種類は**選択され、ドロップダウン リストから選択します。 [Select] をクリックします。
11. 以前作成したネットワーク デバイス グループ **VPN-Gateways** を選択し、[OK] をクリックします。
12. [Select] をクリックします。
13. 新しい認可プロファイルを作成するには、[Create] をクリックします。
14. **認可プロファイル**の名前を指定します。 この例では「**Sample-Profile**」という名前を使用しています。
15. [Common Tasks] タブを選択し、[Downloadable ACL Name] のドロップダウン リストから [Static] を選択します。 値ドロップダウン リストから新しく作成された **DACL（サンプル DACL）を**選択して下さい。
16. [Submit] をクリックします。
17. 以前作成した **Sample-Profile** を選択し、[OK] をクリックします。
18. [OK] をクリックします。
19. **Rule-1 が** NDG として **VPNゲートウェイ**で作成されることを確認して下さい: 条件として

デバイスの種類、および結果として**サンプルプロファイル**。 [Save Changes] をクリックします。

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
```

Sample-Group ユーザ **cisco** は正常に認証し、RADIUS サーバはセキュリティ アプライアンスで作成済みのアクセス リストの ACL 名（new）をダウンロードします。 ユーザ「cisco」は、10.1.1.2 サーバを**除いて**、ASA のネットワーク内にある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、**new** という名前の ACL は ASA でのフィルタリングのために設定されています。

```
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。 次のように設定しておく必要があります。

- [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
- RADIUS（IETF）Filter-Id を含む認可プロファイルが、Access-Service のルールの結果セクションで選択されている

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。

Cisco Secure ACS で Filter-Id を設定するには、「ユーザごとのダウンロード可能 ACL 用の ACS の設定」の手順 1 から 6 および 10 から 12 を実行し、次に「グループのダウンロード可能 ACL 用の ACS の設定」の手順 1 から 6 を実行し、その後でこのセクションの手順を実行します。

IETF RADIUS 属性を設定して認可プロファイルのように適用するには、次の手順を実行します。

1. 新しい認可プロファイルを作成するには、[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] を選択し、[Create] をクリックします。
2. **認可プロファイル**の名前を指定します。 **Filter-Id** は、分かりやすくするためにこの例で選択した認可プロファイル名です。
3. [Common Tasks] タブをクリックし、[Filter-ID ACL] のドロップダウン リストから [Static] を選択します。 [Value] フィールドにアクセス リスト名「**new**」を入力し、[Submit] をクリックします。
4. 新しいルールを作成するには、[Access Policies] > [Access Services] > [Default Network Access] > [Authorization] を選択し、[Create] をクリックします。
5. [Identity Group] の横にあるチェックボックスがオンになっていることを確認し、[Select] を

クリックします。
6. [Sample-Group] を選択し、[OK] をクリックします。
7. [Authorization Profiles] セクションで [Select] をクリックします。
8. 以前作成した認可プロファイル [Filter-Id] を選択し、[OK] をクリックします。
9. [OK] をクリックします。
10. **Rule-1** が作成され、[Identity Group] が [Sample-Group]、[Result] が [Filter-Id] になっていることを確認します。 [Save Changes] をクリックします。

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 に接続します。

次の手順を実行します。

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。ASA で設定されている VPN トンネル グループ名（**Cisco-Tunnel**）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. 要求されたら、認証用に ASA で設定したユーザ名「**cisco**」とパスワード「**cisco123**」を入力し、[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. 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。

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

IKEv1 SAs:

   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: 172.16.1.50
    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: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr:
       172.16.1.1

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
      current_peer: 172.16.1.50, username: cisco
      dynamic allocated peer ip: 10.2.2.1

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
      #pkts decaps: 333, #pkts decrypt: 333, #pkts verify: 333
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 172.16.1.1/0, remote crypto endpt.: 172.16.1.50/0
      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 9A06E834
      current inbound spi : FA372121

    inbound esp sas:
      spi: 0xFA372121 (4197916961)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 28678
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x9A06E834 (2584143924)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 28678
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

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# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
           alert-interval 300
access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list #ACSACL#-IP-Sample-DACL-4f3b9117; 2 elements; name hash: 0x3c878038
   (dynamic)
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 1 extended permit ip any host
   10.1.1.2 (hitcnt=0) 0x5e896ac3
```

```
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 2 extended deny ip any any
   (hitcnt=130) 0x19b3b8f5
```

filter-id ACL

[011] Filter-Id はグループ Sample-Group に適用され、そのグループのユーザは ASA で定義されている ACL (new) によ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 OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list new; 2 elements; name hash: 0xa39433d3
access-list new line 1 extended permit ip any host 10.1.1.2 (hitcnt=4)
   0x58a3ea12
access-list new line 2 extended deny ip any any (hitcnt=27) 0x61f918cd
```

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 SA 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 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 System
- Requests for Comments (RFC)
- テクニカル サポートとドキュメント – Cisco Systems