CHAPTER 27

接続プロファイル、グループ ポリシー、およびユーザの設定

この章では、VPN の接続プロファイル（以前は「トンネル グループ」と呼ばれていました）、グループ ポリシー、およびユーザの設定方法について説明します。この章は、次の項で構成されています。

要約すると、最初に接続プロファイルを設定して、接続用の値を設定します。次に、グループ ポリシーを設定します。グループ ポリシーでは、ユーザの集合に関する値が設定されます。その後、ユーザを設定します。ユーザはグループの値を継承でき、さらに個別のユーザ単位に特定の値を設定することができます。この章では、これらのエンティティを設定する方法と理由について説明します。

接続プロファイル、グループ ポリシー、およびユーザの概要

グループとユーザは、バーチャル プライベート ネットワーク（VPN）のセキュリティ管理と ASA 1000V の設定における中核的な概念です。グループとユーザで指定される属性によって、VPN へのユーザ アクセスと VPN の使用方法が決定されます。*グループ*は、ユーザの集合を 1 つのエンティティとして扱うものです。*ユーザ*の属性は、*グループ ポリシー*から取得されます。*接続プロファイル*では、特定の接続用のグループ ポリシーを指定します。ユーザに対して特定のグループ ポリシーを割り当てない場合は、接続のデフォルト グループ ポリシーが適用されます。

（注） 接続プロファイルは、**tunnel-group** コマンドを使用して設定します。この章では、「接続プロファイル」と「トンネル グループ」という用語が同義的によく使用されています。

接続プロファイルとグループ ポリシーを使用すると、システム管理が簡略化されます。コンフィギュレーション タスクを効率化するために、ASA 1000V にはデフォルトの LAN-to-LAN 接続プロファイル、デフォルトのリモート アクセス接続プロファイル、SSL/IKEv2 VPN 用のデフォルトの接続プロファイル、およびデフォルトのグループ ポリシー（DfltGrpPolicy）が用意されています。デフォルトの接続プロファイルとグループ ポリシーでは、多くのユーザに共通すると考えられる設定が提供されます。ユーザを追加するときに、ユーザがグループ ポリシーからパラメータを「継承」するように指定できます。これにより、数多くのユーザに対して迅速に VPN アクセスを設定できます。

すべての VPN ユーザに同一の権限を許可する場合は、特定の接続プロファイルやグループ ポリシーを設定する必要はありませんが、VPN がそのように使用されることはほとんどありません。たとえば、経理グループ、カスタマー サポート グループ、および MIS（経営情報システム）グループが、プライベート ネットワークのそれぞれ異なる部分にアクセスできるようにする場合が考えられます。また、

MIS に所属する特定のユーザには、他の MIS ユーザにはアクセスできないシステムにアクセスを許可する場合があります。接続プロファイルとグループ ポリシーにより、このような柔軟な設定を安全に実行することができます。

（注）　ASA 1000V には、オブジェクト グループという概念もあります。これは、ネットワーク リストのスーパーセットです。オブジェクト グループを使用すると、ポートやネットワークに対する VPN アクセスを定義することができます。オブジェクト グループは、グループ ポリシーや接続プロファイルよりも、ACL と関連があります。オブジェクト グループの使用方法の詳細については、第 8 章「オブジェクトの設定」を参照してください。

セキュリティ アプライアンスでは、さまざまなソースから属性値を適用できます。次の階層に従って、属性値を適用します。

1. Dynamic Access Policy（DAP）レコード
2. Username
3. グループ ポリシー
4. 接続プロファイル用のグループ ポリシー
5. デフォルトのグループ ポリシー

そのため、属性の DAP 値は、ユーザ、グループ ポリシー、または接続プロファイル用に設定された値よりもプライオリティが高くなっています。

DAP レコードの属性をイネーブルまたはディセーブルにすると、ASA 1000V はその値を適用して実行します。たとえば、dap webvpn モードで HTTP プロキシをディセーブルにすると、セキュリティ アプライアンスはそれ以上値を検索しません。代わりに、**http-proxy** コマンドの **no** 値を使用すると、属性は DAP レコードに存在しないため、適用する値を検索するために、セキュリティ アプライアンスはユーザ名の AAA 属性、および必要に応じてグループ ポリシーに移動して適用する値を検出します。ASDM を使用して DAP を設定することをお勧めします。

接続プロファイル

接続プロファイルは、トンネル接続ポリシーを決定するレコードのセットで構成されます。これらのレコードは、トンネル ユーザが認証先サーバ、および接続情報の送信先となるアカウンティング サーバ（存在する場合）を特定します。また、これらのレコードには、接続用のデフォルト グループ ポリシーも指定され、さらにプロトコル固有の接続パラメータも含まれています。接続プロファイルには、トンネル自体の作成に関連する少数の属性が含まれます。接続プロファイルには、ユーザ関連の属性を定義するグループ ポリシーへのポインタも含まれます。

ASA 1000V では、LAN-to-LAN 接続プロファイル用にデフォルトの DefaultL2Lgroup が用意されています。これらのデフォルト接続プロファイルは変更できますが、削除はできません。また、環境に固有の接続プロファイルを 1 つ以上作成することもできます。接続プロファイルは、ASA 1000V のローカルな設定であり、外部サーバでは設定できません。

接続プロファイルの一般接続パラメータ

一般パラメータは、すべての VPN 接続に共通です。一般パラメータには、次のものがあります。

- 接続プロファイル名：接続プロファイル名は、接続プロファイルを追加または編集するときに指定します。
- 接続タイプ：接続タイプには IPsec LAN-to-LAN が含まれます。

- 認証、許可、アカウンティング サーバ：これらのパラメータでは、ASA 1000V が次の目的で使用するサーバのグループまたはリストを指定します。
  - ユーザの認証
  - ユーザがアクセスを認可されたサービスに関する情報の取得
  - アカウンティング レコードの保存

  サーバ グループは、1 つ以上のサーバで構成されます。
- 接続用のデフォルト グループ ポリシー：グループ ポリシーは、ユーザ関連の属性のセットです。デフォルト グループ ポリシーは、ASA 1000V がトンネル ユーザを認証または認可する際にデフォルトで使用する属性を含んだグループ ポリシーです。

接続プロファイルの設定

次の項では、接続プロファイルの内容および設定について説明します。

- 「接続プロファイルの最大数」（P.27-3）
- 「LAN-to-LAN 接続プロファイルの設定」（P.27-4）

デフォルトの接続プロファイルを変更し、3 つのトンネルグループ タイプのいずれかで新しい接続プロファイルを設定できます。接続プロファイル内で明示的に属性を設定しない場合、その属性の値はデフォルトの接続プロファイルから取得されます。デフォルトの接続プロファイル タイプはリモートアクセスです。その後のパラメータは、選択したトンネル タイプによって異なります。デフォルト接続プロファイルも含めて、すべての接続プロファイルの現在のコンフィギュレーションとデフォルトのコンフィギュレーションを確認するには、**show running-config all tunnel-group** コマンドを入力します。

接続プロファイルの最大数

1 つの ASA 1000V がサポートできる接続プロファイル（トンネル グループ）の最大数は、プラットフォームの同時 VPN セッションの最大数 + 5 の関数です。たとえば、ASA5505 は、同時に最大 25 の VPN セッションをサポートし、30 のトンネル グループ（25+5）を許可します。制限値を超えてトンネル グループを追加しようとすると、「ERROR: The limit of 30 configured tunnel groups has been reached」というメッセージが出力されます。

表 27-1 は、各 ASA プラットフォームの VPN セッションと接続プロファイルの最大数を示します。

表 27-1　VPN セッションおよび接続プロファイルの最大数（ASA プラットフォームごと）

	5505 基本 /Security Plus	5510/ 基本 /Security Plus	5520	5540	5550	5580-20	5580-40
VPN セッションの最大数	10/25	250	750	5000	5000	10,000	10,000
接続プロファイルの最大数	15/30	255	755	5005	5005	10,005	10,005

IPSec トンネルグループの一般属性の設定

IPSec LAN-to-LAN トンネルは、トンネルグループ属性のサブセットを使用します。すべてのコマンドの詳細については、コマンド リファレンスを参照してください。次の項では、LAN-to-LAN 接続プロファイルを設定する方法を、順を追って説明します。

LAN-to-LAN 接続プロファイルの設定

IPsec LAN-to-LAN VPN 接続プロファイルは、LAN-to-LAN IPsec クライアント接続だけに適用されます。設定するパラメータの多くは IPsec リモートアクセスの接続プロファイルのものと同じですが、LAN-to-LAN トンネルの方がパラメータの数は少なくなります。次の項では、LAN-to-LAN 接続プロファイルを設定する例を示します。

- 「LAN-to-LAN 接続プロファイルの名前とタイプの指定」（P.27-4）
- 「LAN-to-LAN 接続プロファイルの一般属性の設定」（P.27-4）
- 「LAN-to-LAN IPsec IKEv1 属性の設定」（P.27-5）

デフォルトの LAN-to-LAN 接続プロファイルのコンフィギュレーション

デフォルトの LAN-to-LAN 接続プロファイルの内容は、次のとおりです。

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 no accounting-server-group
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key
 peer-id-validate req
 no chain
 no ikev1 trust-point
 isakmp keepalive threshold 10 retry 2
```

LAN-to-LAN 接続プロファイルのパラメータはリモートアクセス接続プロファイルのパラメータより少なく、そのほとんどはどちらのグループでも同じです。実際に接続を設定する場合の利便性を考え、ここではこのグループのパラメータを個別に説明します。明示的に設定しないパラメータはすべて、デフォルトの接続プロファイルからその値を継承します。

LAN-to-LAN 接続プロファイルの名前とタイプの指定

接続プロファイルの名前とタイプを指定するには、次のように **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

LAN-to-LAN トンネルの場合、タイプは **ipsec-l2l** になります。たとえば、docs という名前の LAN-to-LAN 接続プロファイルを作成するには、次のコマンドを入力します。

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

LAN-to-LAN 接続プロファイルの一般属性の設定

接続プロファイルの一般属性を設定するには、次の手順を実行します。

ステップ 1　general-attributes キーワードを指定して、トンネルグループ一般属性モードに入ります。

```
hostname(config)# tunnel-group_tunnel-group-name general-attributes
hostname(config-tunnel-general)#
```

プロンプトが変化して、config-general モードに入ったことがわかります。トンネルグループの一般属性は、このモードで設定します。

たとえば、docs という名前の接続プロファイルの場合は、次のコマンドを入力します。

```
hostname(config)# tunnel-group_docs general-attributes
hostname(config-tunnel-general)#
```

ステップ 2　アカウンティングサーバ グループがある場合、使用するグループの名前を指定します。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドはアカウンティングサーバ グループ acctgserv1 の使用を指定しています。

```
hostname(config-tunnel-general)# accounting-server-group acctgserv1
hostname(config-tunnel-general)#
```

ステップ 3　デフォルト グループ ポリシーの名前を指定します。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

たとえば、次のコマンドは、デフォルト グループ ポリシーの名前に MyPolicy を指定しています。

```
hostname(config-tunnel-general)# default-group-policy MyPolicy
hostname(config-tunnel-general)#
```

LAN-to-LAN IPsec IKEv1 属性の設定

IPSec IKEv1 属性を設定するには、次の手順を実行します。

ステップ 1　トンネルグループ IPsec IKEv1 属性を設定するには、IPsec-attributes キーワードを指定して tunnel-group コマンドを入力し、トンネルグループ ipsec 属性コンフィギュレーション モードを開始します。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドでは、config-ipsec モードに入り、TG1 という名前の接続プロファイルのパラメータを設定できます。

```
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

プロンプトが変化して、トンネルグループ ipsec 属性コンフィギュレーション モードに入ったことがわかります。

ステップ 2　事前共有キーに基づく IKEv1 接続をサポートするために、事前共有キーを指定します。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key key
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、LAN-to-LAN 接続プロファイルの IKEv1 接続をサポートするために、事前共有キー XYZX を指定しています。

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-general)#
```

ステップ 3　ピアの証明書を使用してピアの ID を検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

使用できるオプションは、**req**（必須）、**cert**（証明書でサポートされている場合）、**nocheck**（調べない）です。デフォルトは **req** です。たとえば、次のコマンドは、peer-id-validate オプションを **nocheck** に設定しています。

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

ステップ 4　証明書チェーンを送信できるかどうかを指定します。次のアクションは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

この属性は、すべてのトンネル グループ タイプに適用できます。

ステップ 5　IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、トラストポイント名を mytrustpoint に設定しています。

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

この属性は、すべてのトンネル グループ タイプに適用できます。

ステップ 6　ISAKMP（IKE）キープアライブのしきい値と許可されるリトライ回数を指定します。**threshold** パラメータでは、ピアがキープアライブ モニタリングを開始するまでの最長アイドル時間を秒数（10 ～ 3600）で指定します。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間の間隔です（2 ～ 10 秒）。IKE キープアライブは、デフォルトでイネーブルです。IKE キープアライブをディセーブルにするには、**isakmp** コマンドの **no** 形式を入力します。

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

たとえば、次のコマンドは、ISAKMP キープアライブのしきい値を 15 秒に設定し、リトライ インターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold パラメータのデフォルト値は、LAN-to-LAN の場合は 10 です。retry パラメータのデフォルト値は 2 です。

中央サイト（「ヘッド エンド」）で、ISAKMP モニタリングを決して開始しないように指定する場合は、次のコマンドを入力します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

ステップ 7　ISAKMP ハイブリッド認証方式、XAUTH またはハイブリッド XAUTH を指定します。

isakmp ikev1-user-authentication コマンドは、ASA 1000V 認証にデジタル証明書を使用する必要がある場合、およびリモート VPN ユーザ認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。ハイブリッド XAUTH によって、IKE のフェーズ 1 が次の 2 つの手順に分割されます。2 つ合わせてハイブリッド認証と呼ばれます。

a. ASA 1000V は、標準の公開キー技術を使用して、リモート VPN ユーザに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。

b. 次に、XAUTH 交換がリモート VPN ユーザを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注） 認証タイプをハイブリッドに設定するには、事前に認証サーバを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

たとえば、次のコマンドは、example-group と呼ばれる接続プロファイルのハイブリッド XAUTH をイネーブルにします。

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication hybrid
hostname(config-tunnel-ipsec)#
```

グループ ポリシー

この項では、グループ ポリシーとその設定方法について説明します。内容は次のとおりです。

グループ ポリシーは、IPsec 接続用のユーザ指向の属性と値のペアがセットになったもので、デバイスに内部的（ローカル）に保存されるか、外部の RADIUS サーバに保存されます。接続プロファイルでは、トンネル確立後、ユーザ接続の条件を設定するグループ ポリシーが使用されます。グループ ポリシーを使用すると、ユーザまたはユーザのグループに属性セット全体を適用できるので、ユーザごとに各属性を個別に指定する必要がありません。

ユーザにグループ ポリシーを割り当てたり、特定のユーザのグループ ポリシーを変更したりするには、グローバル コンフィギュレーション モードで **group-policy** コマンドを入力します。

ASA 1000V には、デフォルトのグループ ポリシーが含まれています。変更はできても削除はできないデフォルトのグループ ポリシーに加え、自分の環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

内部グループ ポリシーと外部グループ ポリシーを設定できます。内部グループは ASA 1000V の内部データベースで設定されます。外部グループは RADIUS などの外部認証サーバに設定されます。グループ ポリシーには、次の属性があります。

- アイデンティティ
- サーバの定義
- トンネリング プロトコル
- IPsec 設定
- フィルタ

- 接続の設定

デフォルトのグループ ポリシー

ASA 1000V では、デフォルトのグループ ポリシーが提供されます。このデフォルト グループ ポリシーは変更できますが、削除はできません。デフォルトのグループ ポリシーは、DfltGrpPolicy という名前で ASA 1000V に常に存在していますが、このデフォルトのグループ ポリシーは、ASA 1000V でそれを使用するように設定しない限り有効にはなりません。その他のグループ ポリシーを設定する場合、明示的に指定しない属性の値はデフォルトのグループ ポリシーから取得されます。デフォルトのグループ ポリシーを表示するには、次のコマンドを入力します。

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

デフォルトのグループ ポリシーを設定するには、次のコマンドを入力します。

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```

（注） デフォルトのグループ ポリシーは、常に内部（internal）です。コマンドの構文は、`hostname(config)# group-policy DfltGrpPolicy {internal | external}` ですが、タイプを外部（external）に変更することはできません。

デフォルトのグループ ポリシーの任意の属性を変更する場合は、**group-policy attributes** コマンドを使用して属性モードに入り、その後、変更対象の属性を変更するためのコマンドを指定します。

```
hostname(config)# group-policy DfltGrpPolicy attributes
```

（注） 属性モードは内部グループ ポリシーにだけ適用されます。

ASA 1000V で提供されるデフォルトのグループ ポリシー DfltGrpPolicy は、次のとおりです。

```
show runn all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server none
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 ipv6-vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp disable
 ipsec-udp-port 10000
```

```
split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable
msie-proxy pac-url none
msie-proxy lockdown enable
vlan none
nac-settings none
address-pools none
ipv6-address-pools none
smartcard-removal-disconnect enable
scep-forwarding-url none
client-firewall none
client-access-rule none
```

デフォルト グループ ポリシーは変更可能です。また、環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

グループ ポリシーの設定

グループ ポリシーは、すべての種類のトンネルに適用できます。どちらの場合も、パラメータが明示的に指定されていなければ、そのグループはデフォルト グループ ポリシーの値を使用します。グループ ポリシーを設定するには、後続の項の手順を実行します。

外部グループ ポリシーの設定

外部グループ ポリシーの属性値には、指定する外部サーバの値が取得されます。外部グループ ポリシーの場合は、ASA 1000V が属性のクエリーを実行できる AAA サーバ グループを特定し、その外部 AAA サーバ グループから属性を取得するときに使用するパスワードを指定する必要があります。外部認証サーバを使用していて、外部グループ ポリシー属性が、認証する予定のユーザと同じ RADIUS サーバにある場合、それらの間で名前が重複しないようにする必要があります。

（注） ASA 1000V の外部グループ名は、RADIUS サーバのユーザ名を参照しています。つまり、ASA 1000V に外部グループ X を設定する場合、RADIUS サーバはクエリーをユーザ X に対する認証要求と見なします。そのため、外部グループは実際には、ASA 1000V にとって特別な意味を持つ、RADIUS サーバ上のユーザ アカウントということになります。認証する予定のユーザと同じ RADIUS サーバに外部グループ属性が存在する場合、それらの間で名前を重複させることはできません。

ASA 1000V は、外部 LDAP または RADIUS サーバでのユーザ認証をサポートしています。外部サーバを使用するように ASA 1000V を設定する前に、正しい ASA 1000V 認証属性でサーバを設定し、それらの属性のサブセットから個々のユーザに対する個別の許可を割り当てる必要があります。

外部グループ ポリシーを設定するには、次の手順を実行して、server-group 名と password とともにグループ ポリシーの名前とタイプを指定します。

```
hostname(config)# group-policy group_policy_name type server-group server_group_name
password server_password
hostname(config)#
```

（注）　外部グループ ポリシーの場合、サポートされる AAA サーバ タイプは RADIUS だけです。

たとえば、次のコマンドは、ExtGroup という名前の外部グループ ポリシーが作成します。このグループ ポリシーの属性は、ExtRAD という名前の外部 RADIUS サーバから取得され、属性を取得するときに使用されるパスワードが newpassword に指定されます。

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password newpassword
hostname(config)#
```

（注）　いくつかのベンダー固有属性（VSA）を設定できます。RADIUS サーバが Class 属性（#25）を返すように設定されている場合、ASA 1000V は、グループ名の認証にその属性を使用します。RADIUS サーバでは、属性は次の形式で指定する必要があります。OU=*groupname*。ここで、*groupname* は、ASA 1000V で設定されたグループ名と同一です。例、OU=Finance。

内部グループ ポリシーの設定

内部グループ ポリシーを設定するには、グループ ポリシーの名前とタイプを指定します。

```
hostname(config)# group-policy group_policy_name type
hostname(config)#
```

たとえば、次のコマンドは GroupPolicy1 という名前の内部グループ ポリシーを作成します。

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

デフォルトのタイプは **internal** です。

キーワード **from** を追加して既存のポリシーの名前を指定することにより、内部グループ ポリシーの属性をその既存のグループ ポリシーの値に初期設定することができます。

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
hostname(config-group-policy)#
```

グループ ポリシー属性の設定

内部グループ ポリシーの場合、特定の属性値を指定できます。まず、グローバル コンフィギュレーション モードで **group-policy attributes** コマンドを入力して、グループ ポリシー属性モードに入ります。

```
hostname(config)# group-policy name attributes
hostname(config-group-policy)#
```

プロンプトが変化して、モードが変更されたことがわかります。グループ ポリシー属性モードでは、指定したグループ ポリシーの属性と値のペアを設定することができます。グループ ポリシー属性モードで、デフォルト グループから継承しない属性と値のペアを明示的に設定します。これを行うためのコマンドは、次の項で説明します。

サイトツーサイト VPN 固有の属性の設定

この項の手順に従って、VPN 属性値を設定します。VPN 属性は、グループ ポリシーのトンネリング プロトコル、サイトツーサイト VPN セッションに適用する ACL、および接続のアイドル タイムアウトを定義します。

ステップ 1　このグループ ポリシーの VPN トンネル タイプを指定します。

vpn-tunnel-protocol {ikev1 | ikev2}

デフォルトは IPsec です。この属性を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を入力します。

このコマンドのパラメータの値は、次のとおりです。

- **ikev1** : 2 つのピア（Cisco VPN Client または別のセキュア ゲートウェイ）間の IPsec IKEv1 トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
- **ikev2** : 2 つのピア（AnyConnect Secure Mobility Client または別のセキュア ゲートウェイ）間の IPsec IKEv2 トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。

このコマンドを入力して、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザには、少なくとも 1 つのトンネリング モードを設定する必要があります。

次の例は、FirstGroup という名前のグループ ポリシーに IPsec IKEv1 トンネリング モードを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev1
hostname(config-group-policy)#
```

ステップ 2　グループ ポリシー モードで **vpn-filter** コマンドを使用して、VPN セッションに適用する ACL の名前を指定します。

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

ACL を設定して、このグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**vpn-filter** コマンドを入力して、これらの ACL を適用します。

vpn-filter none コマンドを入力して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を入力します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、ACL 名を指定する代わりに、**none** キーワードを入力します。**none** キーワードは、アクセス リストがないことを示します。このキーワードにより、ヌル値が設定され、アクセス リストが拒否されます。

次に、FirstGroup という名前のグループ ポリシーの、acl_vpn というアクセス リストを呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

vpn-filter コマンドは、トンネルから出た後の復号化後のトラフィックと、トンネルに入る前の暗号化前のトラフィックに適用されます。vpn-filter に使用される ACL を interface access-group にも使用することはできません。**vpn-filter** コマンドを、リモート アクセス VPN クライアント接続を制御するグループ ポリシーに適用する場合は、ACL の **src_ip** の位置のクライアント割り当て IP アドレスおよび ACL の **dest_ip** の位置のローカル ネットワークに対して ACL を設定する必要があります。

vpn-filter コマンドを、LAN-to-LAN VPN 接続を制御するグループ ポリシーに適用する場合は、ACL の **src_ip** の位置のリモート ネットワークおよび ACL の **dest_ip** の位置のローカル ネットワークに対して ACL を設定する必要があります。

vpn-filter 機能で使用するために ACL を設定する場合は、注意する必要があります。ACL は、復号化後のトラフィックに対して構築されていることに留意してください。ただし、ACL は反対方向のトラフィックに対しても適用されます。トンネル宛ての、暗号化前のこのトラフィックについては、ACL は **src_ip** の位置と **dest_ip** の位置を入れ替えたものに対して構築されています。

次の例では、vpn-filter をリモート アクセス VPN クライアントと共に使用します。
この例では、クライアント割り当て IP アドレスを 10.10.10.1/24、ローカル ネットワークを 192.168.1.0/24 としています。

次の ACE によって、リモート アクセス VPN クライアントがローカル ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255
192.168.1.0 255.255.255.0 eq 23
```

次の ACE によって、ローカル ネットワークがリモート アクセス クライアントに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq
23 192.168.1.0 255.255.255.0
```

（注） （注）ACE の access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23 によって、ローカル ネットワークは、発信元ポート 23 を使用している場合にリモート アクセス クライアントへの接続開始が許可されます。ACE の access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0 によって、リモート アクセス クライアントは、発信元ポート 23 を使用している場合にリモート アクセス クライアントへの接続開始が許可されます。

次の例では、vpn-filter を LAN-to-LAN VPN 接続と共に使用します。この例では、リモート ネットワークを 10.0.0.0/24、ローカル ネットワークを 192.168.1.0/24 としています。
次の ACE によって、リモート ネットワークがローカル ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0
192.168.1.0 255.255.255.0 eq 23
```

次の ACE によって、ローカル ネットワークがリモート ネットワークに Telnet を使用することが許可されます。

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23
192.168.1.0 255.255.255.0
```

（注）　（注）ACE の access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23 によって、ローカル ネットワークは、発信元ポート 23 を使用している場合にリモート ネットワークへの接続開始が許可されます。（注）ACE の access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0 によって、リモート ネットワークは、発信元ポート 23 を使用している場合にローカル ネットワークへの接続開始が許可されます。

ステップ 3　グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを入力して、アイドル タイムアウト期間を設定します。

```
hostname(config-group-policy)# vpn-idle-timeout {minutes | none}
hostname(config-group-policy)#
```

最小時間は 1 分で、最大時間は 35791394 分です。デフォルトは 30 分です。この期間中に接続上で通信アクティビティがない場合、ASA 1000V は接続を終了します。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、分を指定する代わりに **none** キーワードを指定して、このコマンドを入力します。また、none キーワードを指定すると、無制限のアイドル タイムアウト期間が許可されます。このキーワードにより、アイドル タイムアウトにヌル値が設定され、アイドル タイムアウトが拒否されます。

次の例は、FirstGroup という名前のグループ ポリシーに 15 分の VPN アイドル タイムアウトを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

ステップ 4　**vpn-idle-timeout alert-interval** {minutes | none} コマンドを使用して、アイドルタイムアウトのアラート メッセージがユーザに表示される時間を設定します。このアラート メッセージは、VPN セッションが非アクティブにより切断されるまでの時間（分）をユーザに伝えます。

次に、VPN セッションが非アクティブにより切断される 20 分前にユーザに通知するように、**vpn-idle-timeout alert-interval** を設定する例を示します。1 ～ 30 分の範囲で指定できます。

hostname(config-webvpn)# **vpn-idle-timeout alert-interval** 20

コマンドの none パラメータはユーザがアラートを受信しないことを示します。

コマンドの no 形式：**no vpn-idle-timeout alert-interval**

は、VPN アイドル タイムアウトのアラート間隔属性がデフォルト グループ ポリシーから継承することを示します。

トンネリング用のドメイン属性の設定

トンネリングされたパケットのデフォルト ドメイン名、またはスプリット トンネルを経由して解決されるドメインのリストを指定できます。次の項では、これらのドメインの設定方法について説明します。

トンネリングされたパケットのデフォルト ドメイン名の定義

ASA 1000V は、ドメイン フィールドを省略した DNS クエリーに付加するために、デフォルト ドメイン名を IPsec クライアントに渡します。デフォルト ドメイン名がない場合、ユーザはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。グループ ポリシーのユーザのデフォルト ドメイン名を指定するには、グループ ポリシー コンフィギュレーション モードで **default-domain** コマンドを入力します。ドメイン名を削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

value *domain-name* パラメータは、グループのデフォルト ドメイン名を指定します。デフォルト ドメイン名が存在しないことを指定するには、**none** キーワードを入力します。このコマンドにより、デフォルト ドメイン名にヌル値が設定され、デフォルト ドメイン名が拒否されます。また、デフォルトまたは指定されたグループ ポリシーからデフォルト ドメイン名が継承されなくなります。

すべてのデフォルト ドメイン名を削除するには、引数を指定せずに **no default-domain** コマンドを入力します。このコマンドにより、**none** キーワードを指定して **default-domain** コマンドを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのデフォルト ドメイン名が削除されます。**no** 形式を使用すると、ドメイン名の継承が許可されます。

次に、FirstGroup という名前のグループ ポリシーに対して、FirstDomain のデフォルト ドメイン名を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

スプリット トンネリング用のドメイン リストの定義

スプリット トンネルを介して解決されるドメインのリストを入力します。グループ ポリシー コンフィギュレーション モードで **split-dns** コマンドを入力します。リストを削除するには、このコマンドの **no** 形式を入力します。

スプリット トンネリング ドメインのリストがない場合、ユーザはデフォルトのグループ ポリシー内に存在するリストを継承します。ユーザがこのようなスプリット トンネリング ドメイン リストを継承しないようにするには、**none** キーワードを指定して **split-dns** コマンドを入力します。

すべてのスプリット トンネリング ドメイン リストを削除するには、引数を指定せずに **no split-dns** コマンドを入力します。これにより、**none** キーワードを指定して **split-dns** コマンドを発行して作成したヌル リストを含めて、設定済みのすべてのスプリット トンネリング ドメイン リストが削除されます。

パラメータ **value** *domain-name* では、ASA 1000V がスプリット トンネルを介して解決するドメイン名を指定します。**none** キーワードは、スプリット DNS リストが存在しないことを示します。また、このキーワードにより、スプリット DNS リストにヌル値が設定されます。そのため、スプリット DNS リストは拒否され、デフォルトまたは指定されたグループ ポリシーのスプリット DNS リストが継承されなくなります。このコマンドの構文は次のとおりです。

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2...
domain-nameN] | none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

ドメインのリスト内で各エントリを区切るには、スペースを 1 つ入力します。エントリ数に制限はありませんが、ストリング全体の長さは 255 文字以下にします。英数字、ハイフン（-）、およびピリオド（.）のみを使用できます。デフォルト ドメイン名がトンネルを介して解決される場合は、そのドメイン名をこのリストに明示的に含める必要があります。

次の例は、FirstGroup という名前のグループ ポリシーで、Domain1、Domain2、Domain3、Domain4 の各ドメインがスプリット トンネリングを介して解決されるように設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

DHCP 代行受信の設定

スプリット トンネル オプションが 255 バイトを超えていると、Microsoft XP で異常が発生し、ドメイン名が破損します。この問題を回避するには、ASA 1000V で送信ルートの数を 27 ～ 40 に制限します。ルートの数はルートのクラスによって異なります。

DHCP 代行受信を使用することにより、Microsoft Windows XP クライアントで ASA 1000V とともにスプリット トンネリングを使用できます。ASA 1000V は、Microsoft Windows XP クライアント DHCP Inform メッセージに直接応答して、クライアントにトンネル IP アドレス用のサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。Windows XP 以前の Windows クライアントの場合、DHCP 代行受信によってドメイン名とサブネット マスクが提供されます。これは、DHCP サーバを使用するのが効果的でない環境で役立ちます。

intercept-dhcp コマンドは、DHCP 代行受信をイネーブルまたはディセーブルにします。このコマンドの構文は次のとおりです。

[**no**] **intercept-dhcp**

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

netmask 変数で、トンネル IP アドレスのサブネット マスクを提供します。このコマンドの **no** 形式は、コンフィギュレーションから DHCP 代行受信を削除します。

次に、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

バックアップ サーバ属性の設定

バックアップ サーバを設定します（使用する予定がある場合）。IPsec バックアップ サーバを使用すると、VPN クライアントはプライマリ ASA 1000V が使用不可の場合も中央サイトに接続することができます。バックアップ サーバを設定すると、ASA 1000V は、IPsec トンネルを確立するときにクライアントにサーバ リストを渡します。クライアント上またはプライマリ ASA 1000V 上にバックアップ サーバを設定しない限り、バックアップ サーバは存在しません。

バックアップ サーバは、クライアント上またはプライマリ ASA 1000V 上に設定します。ASA 1000V 上にバックアップ サーバを設定すると、適応型セキュリティ アプライアンスは、バックアップ サーバ ポリシーをグループ内のクライアントにプッシュして、クライアント上にバックアップ サーバ リストが設定されている場合、そのリストを置き換えます。

（注） ホスト名を使用する場合は、バックアップ DNS サーバおよびバックアップ WINS サーバを、プライマリ DNS サーバおよびプライマリ WINS サーバとは別のネットワーク上に配置することを推奨します。このようにしないと、ハードウェア クライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得している場合、プライマリ サーバとの接続が失われ、バックアップ サーバに異なる DNS 情報と WINS 情報があると、DHCP リースが期限切れになるまでクライアントを更新できなくなります。また、ホスト名を使用している場合に DNS サーバが使用不可になると、大幅な遅延が発生するおそれがあります。

バックアップ サーバを設定するには、グループ ポリシー コンフィギュレーション モードで **backup-servers** コマンドを入力します。

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

バックアップ サーバを削除するには、バックアップ サーバを指定してこのコマンドの **no** 形式を入力します。backup-servers 属性を実行コンフィギュレーションから削除し、backup-servers の値を他のグループ ポリシーから継承できるようにするには、引数を指定せずにこのコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

clear-client-config キーワードは、クライアントでバックアップ サーバを使用しないことを指定します。ASA 1000V は、ヌルのサーバ リストをプッシュします。

keep-client-config キーワードは、ASA 1000V がバックアップ サーバ情報をクライアントに送信しないことを指定します。クライアントは、独自のバックアップ サーバ リストを使用します（設定されている場合）。これはデフォルトです。

server1 server 2....server10 パラメータ リストは、プライマリの ASA 1000V が使用不可の場合に VPN クライアントが使用するサーバをプライオリティ順にスペースで区切ったリストです。このリストには、サーバを IP アドレスまたはホスト名で指定します。このリストの長さは 500 文字までで、格納できるエントリは最大 10 個までです。

次の例は、FirstGroup という名前のグループ ポリシーに、IP アドレスが 10.10.10.1 と 192.168.10.14 であるバックアップ サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```