許可および認証用の外部サーバの設定

この付録では、ASA で AAA をサポートするための外部 LDAP、RADIUS、または TACACS+ サーバの設定方法について説明します。外部サーバを使用するように ASA を設定する前に、正しい ASA 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。

この付録では、次の項目について説明します。

権限および属性のポリシー実施の概要

ASA は、ユーザ許可属性（ユーザ権利またはユーザ権限とも呼ばれる）を VPN 接続に適用するためのいくつかの方法をサポートしています。ユーザ属性を、ASA のダイナミック アクセス ポリシー（DAP）を通じて、外部認証サーバや許可 AAA サーバ（RADIUS または LDAP）から、ASA のグループ ポリシーから、またはこれら 3 つのすべてから取得できるように ASA を設定できます。

ASA がすべてのソースから属性を受信すると、その属性が評価され、集約されてユーザ ポリシーに適用されます。DAP、AAA サーバ、またはグループ ポリシーから取得した属性の間で衝突がある場合、DAP から取得した属性が常に優先されます。

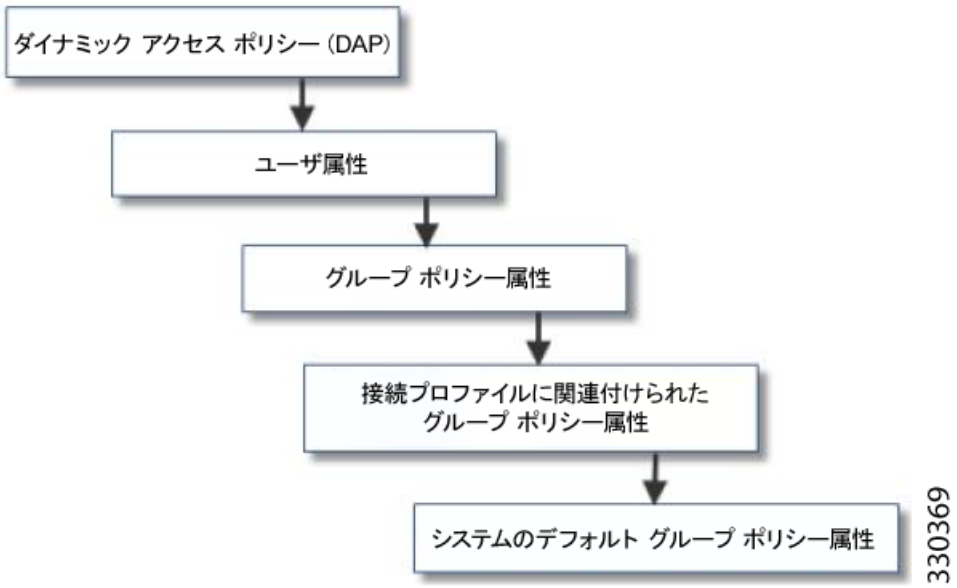
ASA によって属性が適用される順序は次のとおりです（図 14-1 を参照）。

1. ASA 上の DAP 属性：バージョン 8.0(2) で導入されたこの属性は、他のすべての属性よりも優先されます。DAP 内でブックマークまたは URL リストを設定した場合は、グループ ポリシーで設定されているブックマークや URL リストよりも優先されます。
2. AAA サーバ上のユーザ属性：ユーザ認証や許可が成功すると、サーバからこの属性が返されます。これらの属性を、ASA のローカル AAA データベースの個々のユーザに設定されている属性（ASDM のユーザ アカウント）と混同しないでください。
3. ASA 上で設定されているグループ ポリシー：RADIUS サーバからユーザの RADIUS CLASS 属性 IETF-Class-25（OU=*group-policy*）の値が返された場合は、ASA はそのユーザを同じ名前のグループ ポリシーに入れて、そのグループ ポリシーの属性のうち、サーバから返されないものを適用します。

   LDAP サーバでは、任意の属性名を使用してセッションのグループ ポリシーを設定できます。ASA 上で設定されている LDAP 属性マップによって、LDAP 属性が Cisco 属性 IETF-Radius-Class にマッピングされます。

4. 接続プロファイル（CLI では「トンネル グループ」と呼ばれます）によって割り当てられたグループ ポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザに適用されるデフォルトのグループ ポリシーが含まれています。ASA に接続するすべてのユーザは、最初にこのグループに所属します。このグループでは、DAP、サーバから返されるユーザ属性、またはユーザに割り当てられたグループ ポリシーにはない属性が定義されています。
5. ASA で割り当てられたデフォルトのグループ ポリシー（DfltGrpPolicy）：システムのデフォルト属性は、DAP、ユーザ属性、グループ ポリシー、または接続プロファイルで不足している値を提供します。

図 14-1　　ポリシー実施フロー



外部 LDAP サーバの設定

VPN 3000 コンセントレータと ASA/PIX 7.0 ソフトウェアでは、認証作業に Cisco LDAP スキーマが必要でした。バージョン 7.1.x 以降では、ASA は、ネイティブ LDAP スキーマを使用して認証および許可を行うため、Cisco スキーマは必要なくなりました。

許可（権限ポリシー）の設定は、LDAP 属性マップを使用して行います。例については、「Active Directory/LDAP VPN リモート アクセス許可の例」（P.14-16）を参照してください。

ここでは、LDAP サーバの構造、スキーマ、および属性について説明します。次の項目を取り上げます。

- 「ASA での LDAP の設定」（P.14-3）
- 「ASA LDAP コンフィギュレーションの定義」（P.14-5）
- 「Active Directory/LDAP VPN リモート アクセス許可の例」（P.14-16）

これらのプロセスの実際のステップは、使用する LDAP サーバのタイプによって異なります。

（注）　LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

ASA での LDAP の設定

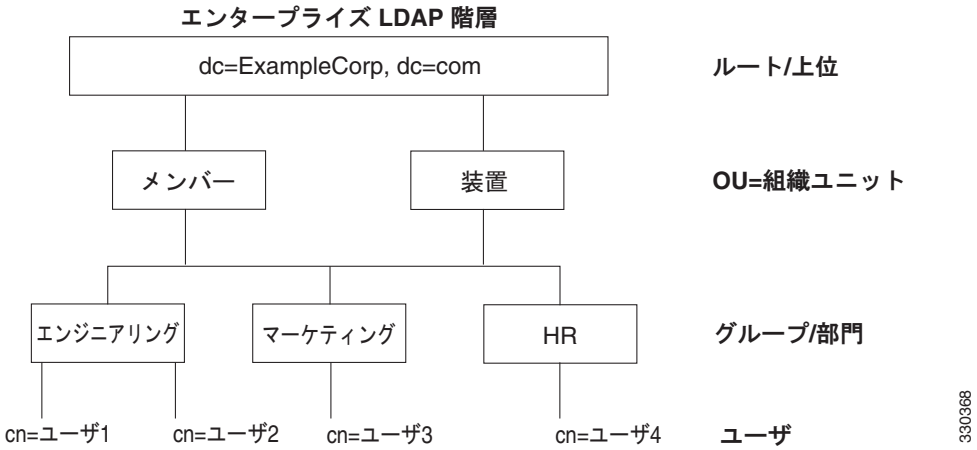
この項では、LDAP 階層内で検索し、LDAP サーバに対する認証済みバインディングを実行する方法について説明します。説明する項目は次のとおりです。

- 「LDAP 階層の検索」（P.14-3）
- 「LDAP への ASA のバインド」（P.14-4）

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Employee1 を例に考えてみます。Employee1 は Engineering グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。たとえば、シングルレベル階層をセットアップします。この中で、Employee1 は Example Corporation のメンバーであると見なされます。あるいは、マルチレベル階層をセットアップします。この中で、Employee1 は Engineering 部門のメンバーであると見なされ、この部門は People という名称の組織ユニットのメンバーであり、この組織ユニットは Example Corporation のメンバーです。マルチレベル階層の例については、図 14-2 を参照してください。

マルチレベル階層の方が詳細ですが、検索結果が速く返されるのはシングルレベル階層の方です。

図 14-2　マルチレベルの LDAP 階層



LDAP 階層の検索

ASA では、LDAP 階層内での検索を調整できます。ASA に次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドは、ユーザの権限が含まれている部分だけを検索するように階層の検索を限定します。

- LDAP Base DN では、サーバが ASA から許可要求を受信したときに LDAP 階層内のどの場所からユーザ情報の検索を開始するかを定義します。
- Search Scope では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバによる検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute では、LDAP サーバのエントリを一意に識別する RDN を定義します。一般的な名前属性には、cn（一般名）、sAMAccountName、および userPrincipalName を含めることができます。

図 14-2 に、Example Corporation の LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。表 14-1 に、2 つの検索コンフィギュレーションの例を示します。

最初のコンフィギュレーションの例では、Employee1 が IPSec トンネルを確立するときに LDAP 許可が必要であるため、ASA から LDAP サーバに検索要求が送信され、この中で Employee1 を Engineering グループの中で検索することが指定されます。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、ASA から送信される検索要求の中で、Employee1 を Example Corporation 全体の中で検索することが指定されています。この検索には時間がかかります。

表 14-1　検索コンフィギュレーションの例

No.	LDAP Base DN	検索範囲	名前属性	結果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	1 レベル	cn=Employee1	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Employee1	検索に時間がかかる

LDAP への ASA のバインド

一部の LDAP サーバ（Microsoft Active Directory サーバなど）では、他の LDAP 動作の要求を受け入れる前に、認証済みバインディングを介したハンドシェイクが必要です。ASA は、ログイン認定者名（DN）とログイン パスワードを使用して、LDAP サーバとの信頼関係（認証済みバインド）を築きます。Login DN は、管理者がバインディングに使用する LDAP サーバのユーザ レコードを表します。

Microsoft Active Directory の読み取り専用操作（認証、許可、グループ検索など）を行うときは、ASA は特権の低い Login DN でバインドできます。たとえば、Login DN には、AD の「Member Of」の指定が Domain Users の一部であるユーザを指定することができます。VPN のパスワード管理書き込み操作では、Login DN に昇格特権が付与されていることと、AD の Account Operators グループのメンバーの一部であることが必要です。Microsoft Active Directory グループの検索（「MemberOf retrieval」とも呼ばれる）ASA バージョン 8.0.4 に追加されました。

Login DN に含まれるエントリの例を次に示します。

cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com

読み取りおよび書き込みの操作に関する Login DN の具体的な要件については、使用する LDAP の管理者ガイドを参照してください。

ASA でサポートされる機能は次のとおりです。

- パスワードを暗号化しない簡易 LDAP 認証（デフォルト ポート 389 を使用）。デフォルトのポートの代わりに他のポートも使用できます。
- セキュア LDAP（LDAP-S）（デフォルト ポート 636 を使用）。デフォルトのポートの代わりに他のポートも使用できます。
- Simple Authentication and Security Layer（SASL）MD5
- SASL Kerberos

ASA は匿名認証をサポートしていません。

（注） LDAP クライアントとしての ASA は、匿名のバインドや要求の送信をサポートしていません。

ASA LDAP コンフィギュレーションの定義

許可では、権限または属性を使用するプロセスを参照します。認証または許可サーバとして定義されている LDAP サーバは、権限または属性（設定されている場合）を適用します。

この項では、LDAP AV-pair 属性の構文の定義方法について説明します。内容は次のとおりです。

- 「LDAP 許可でサポートされている Cisco 属性」（P.14-5）
- 「Cisco-AV-Pair 属性の構文」（P.14-13）
- 「Cisco-AV-Pair の ACL 例」（P.14-14）

ガイドライン

ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を使用します。RADIUS 属性は、名前ではなく数値 ID によって適用されます。

ASDM バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。ASDM バージョン 7.1 以降では、このプレフィックスは削除されています。

LDAP 許可でサポートされている Cisco 属性

この項では、ASA 5500、VPN 3000 コンセントレータ、および PIX 500 シリーズ ASA で使用される全属性のリスト（表 14-2 を参照）を示します。この表には、VPN 3000 コンセントレータおよび PIX 500 シリーズ ASA での属性サポート情報も含まれていますが、これは、このようなデバイスの組み合わせを使用するネットワークの設定を支援するためです。

表 14-2　ASA で LDAP 許可に対してサポートされる Cisco 属性

属性名	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Access-Hours	Y	Y	Y	String	シングル	time-range の名前（Business-Hours など）
Allow-Network-Extension- Mode	Y	Y	Y	Boolean	シングル	0 = ディセーブル 1 = イネーブル
Authenticated-User-Idle- Timeout	Y	Y	Y	Integer	シングル	1 ～ 35791394 分
Authorization-Required	Y			Integer	シングル	0 = しない 1 = する
Authorization-Type	Y			Integer	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	Y	Y	String	シングル	クライアントレス SSL VPN、クライアント SSL VPN、および IPSec クライアントのバナー文字列。
Banner2	Y	Y	Y	String	シングル	クライアントレス SSL VPN、クライアント SSL VPN、および IPSec クライアントのバナー文字列。

表 14-2　ASA で LDAP 許可に対してサポートされる Cisco 属性 （続き）

属性名	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Cisco-AV-Pair	Y	Y	Y	String	マルチ	次の形式のオクテット文字列： [Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port] 詳細については「Cisco-AV-Pair 属性の構文」（P.14-13）を参照してください。
Cisco-IP-Phone-Bypass	Y	Y	Y	Integer	シングル	0 = ディセーブル 1 = イネーブル
Cisco-LEAP-Bypass	Y	Y	Y	Integer	シングル	0 = ディセーブル 1 = イネーブル
Client-Intercept-DHCP-Configure-Msg	Y	Y	Y	Boolean	シングル	0 = ディセーブル 1 = イネーブル
Client-Type-Version-Limiting	Y	Y	Y	String	シングル	IPsec VPN クライアントのバージョン番号を示す文字列
Confidence-Interval	Y	Y	Y	Integer	シングル	10 ～ 300 秒
DHCP-Network-Scope	Y	Y	Y	String	シングル	IP アドレス
DN-Field	Y	Y	Y	String	シングル	有効な値：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name。
Firewall-ACL-In		Y	Y	String	シングル	ACL ID
Firewall-ACL-Out		Y	Y	String	シングル	ACL ID
Group-Policy		Y	Y	String	シングル	リモート アクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の 3 つの形式のいずれかを使用できます。 • *グループ ポリシー名* • OU= *グループ ポリシー名* • OU= *グループ ポリシー名*:
IE-Proxy-Bypass-Local				Boolean	シングル	0=ディセーブル 1=イネーブル
IE-Proxy-Exception-List				String	シングル	DNS ドメインのリスト。エントリは改行文字シーケンス（\n）で区切る必要があります。
IE-Proxy-Method	Y	Y	Y	Integer	シングル	1 = プロキシ設定を変更しない 2 = プロキシを使用しない 3 = 自動検出 4 = ASA 設定を使用する

表 14-2　ASA で LDAP 許可に対してサポートされる Cisco 属性 （続き）

属性名	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
IE-Proxy-Server	Y	Y	Y	Integer	シングル	IP アドレス
IETF-Radius-Class	Y	Y	Y		シングル	リモート アクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2 以降では、Group-Policy 属性の使用を推奨します。次の 3 つの形式のいずれかを使用できます。 • *グループ ポリシー名* • OU= *グループ ポリシー名* • OU= *グループ ポリシー名:*
IETF-Radius-Filter-Id	Y	Y	Y	String	シングル	ASA で定義された ACL 名。これらの設定は、VPN リモート アクセス クライアント、IPSec クライアント、および SSL クライアントの設定に適用されます。
IETF-Radius-Framed-IP-Address	Y	Y	Y	String	シングル	IP アドレス。これらの設定は、VPN リモート アクセス クライアント、IPSec クライアント、および SSL クライアントの設定に適用されます。
IETF-Radius-Framed-IP-Netmask	Y	Y	Y	String	シングル	IP アドレス マスク。これらの設定は、VPN リモート アクセス クライアント、IPSec クライアント、および SSL クライアントの設定に適用されます。
IETF-Radius-Idle-Timeout	Y	Y	Y	Integer	シングル	秒
IETF-Radius-Service-Type	Y	Y	Y	Integer	シングル	1 = Login 2 = Framed 5 = リモート アクセス 6 = Administrative 7 = NAS プロンプト
IETF-Radius-Session-Timeout	Y	Y	Y	Integer	シングル	秒
IKE-Keep-Alives	Y	Y	Y	Boolean	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Allow-Passwd-Store	Y	Y	Y	Boolean	シングル	0 = ディセーブル 1 = イネーブル

表 14-2　ASA で LDAP 許可に対してサポートされる Cisco 属性 （続き）

属性名	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
IPsec-Authentication	Y	Y	Y	Integer	シングル	0 = なし 1 = RADIUS 2 = LDAP（許可のみ） 3 = NT ドメイン 4 = SDI（RSA） 5 = 内部 6 = RADIUS での Expiry 7 = Kerberos または Active Directory
IPsec-Auth-On-Rekey	Y	Y	Y	Boolean	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Backup-Server-List	Y	Y	Y	String	シングル	サーバ アドレス（スペース区切り）
IPsec-Backup-Servers	Y	Y	Y	String	シングル	1 = クライアントが設定したリストを使用する 2 = クライアント リストをディセーブルにして消去する 3 = バックアップ サーバ リストを使用する
IPsec-Client-Firewall-Filter- Name	Y			String	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	Y	Y	Integer	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	Y	Y	String	シングル	クライアントに送信する 1 つのデフォルト ドメイン名を指定します（1 ～ 255 文字）。
IPsec-Extended-Auth-On-Rekey		Y	Y	String	シングル	String
IPsec-IKE-Peer-ID-Check	Y	Y	Y	Integer	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	Y	Y	Integer	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Mode-Config	Y	Y	Y	Boolean	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP	Y	Y	Y	Boolean	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP-Port	Y	Y	Y	Integer	シングル	4001 ～ 49151、デフォルトは 10000。
IPsec-Required-Client-Firewall-Capability	Y	Y	Y	Integer	シングル	0 = なし 1 = リモート FW Are-You-There（AYT）で定義されているポリシー 2 = Policy pushed CPP 4 = サーバからのポリシー

表 14-2　ASA で LDAP 許可に対してサポートされる Cisco 属性 （続き）

属性名	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
IPsec-Sec-Association	Y			String	シングル	セキュリティ アソシエーションの名前
IPsec-Split-DNS-Names	Y	Y	Y	String	シングル	クライアントに送信するセカンダリドメイン名のリストを指定します（1 ～ 255 文字）。
IPsec-Split-Tunneling-Policy	Y	Y	Y	Integer	シングル	0 = すべてをトンネリング 1 = スプリット トンネリング 2 = ローカル LAN を許可
IPsec-Split-Tunnel-List	Y	Y	Y	String	シングル	スプリット トンネルの包含リストを記述したネットワークまたは ACL の名前を指定します。
IPsec-Tunnel-Type	Y	Y	Y	Integer	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock	Y			Boolean	シングル	0 = ディセーブル 1 = イネーブル
L2TP-Encryption	Y			Integer	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 =128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化 / ステートレスが必要
L2TP-MPPC-Compression	Y			Integer	シングル	0 = ディセーブル 1 = イネーブル
MS-Client-Subnet-Mask	Y	Y	Y	String	シングル	IP アドレス
PFS-Required	Y	Y	Y	Boolean	シングル	0 = しない 1 = する
Port-Forwarding-Name	Y	Y		String	シングル	名前の文字列（「Corporate-Apps」など）
PPTP-Encryption	Y			Integer	シングル	ビットマップ： 1 = 暗号化が必要 2 =40 ビット 4 =128 ビット 8 = ステートレスが必要 例： 15 = 40/128 ビットで暗号化 / ステートレスが必要
PPTP-MPPC-Compression	Y			Integer	シングル	0 = ディセーブル 1 = イネーブル
Primary-DNS	Y	Y	Y	String	シングル	IP アドレス
Primary-WINS	Y	Y	Y	String	シングル	IP アドレス
Privilege-Level				Integer	シングル	ユーザ名の場合、0 ～ 15

表 14-2　ASA で LDAP 許可に対してサポートされる Cisco 属性 （続き）

属性名	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Required-Client-Firewall-Vendor-Code	Y	Y	Y	Integer	シングル	1 = シスコ（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコ（Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Description	Y	Y	Y	String	シングル	—
Required-Client-Firewall-Product-Code	Y	Y	Y	Integer	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Require-HW-Client-Auth	Y	Y	Y	Boolean	シングル	0 = ディセーブル 1 = イネーブル
Require-Individual-User-Auth	Y	Y	Y	Integer	シングル	0 = ディセーブル 1 = イネーブル
Secondary-DNS	Y	Y	Y	String	シングル	IP アドレス
Secondary-WINS	Y	Y	Y	String	シングル	IP アドレス
SEP-Card-Assignment				Integer	シングル	未使用
Simultaneous-Logins	Y	Y	Y	Integer	シングル	0 ～ 2147483647
Strip-Realm	Y	Y	Y	Boolean	シングル	0 = ディセーブル 1 = イネーブル
TACACS-Authtype	Y	Y	Y	Integer	シングル	—
TACACS-Privilege-Level	Y	Y	Y	Integer	シングル	—
Tunnel-Group-Lock		Y	Y	String	シングル	トンネル グループの名前または「none」

表 14-2　ASA で LDAP 許可に対してサポートされる Cisco 属性 （続き）

属性名	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Tunneling-Protocols	Y	Y	Y	Integer	シングル	1 = PPTP 2 = L2TP 4 = IPSec（IKEv1） 8 = L2TP/IPSec 16 = WebVPN. 32 = SVC 64 = IPsec（IKEv2） 8 および 4 は相互排他値（0 ～ 11、16 ～ 27、32 ～ 43、48 ～ 59 は有効値）。
Use-Client-Address	Y			Boolean	シングル	0 = ディセーブル 1 = イネーブル
User-Auth-Server-Name	Y			String	シングル	IP アドレスまたはホスト名
User-Auth-Server-Port	Y			Integer	シングル	サーバ プロトコルのポート番号
User-Auth-Server-Secret	Y			String	シングル	サーバのパスワード
WebVPN-ACL-Filters		Y		String	シングル	Webtype ACL 名
WebVPN-Apply-ACL-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル バージョン 8.0 以降では、この属性は必須ではありません。
WebVPN-Citrix-Support-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル バージョン 8.0 以降では、この属性は必須ではありません。
WebVPN-Enable-functions				Integer	シングル	使用しない（廃止）
WebVPN-Exchange-Server-Address				String	シングル	使用しない（廃止）
WebVPN-Exchange-Server-NETBIOS-Name				String	シングル	使用しない（廃止）
WebVPN-File-Access-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Browsing-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Entry- Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Forwarded-Ports		Y		String	シングル	ポート転送リスト名
WebVPN-Homepage	Y	Y		String	シングル	URL（たとえば http://www.example.com）

表 14-2　ASA で LDAP 許可に対してサポートされる Cisco 属性 （続き）

属性名	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
WebVPN-Macro-Substitution-Value1	Y	Y		String	シングル	例については、次の URL にある『*SSL VPN Deployment Guide*』を参照してください。 http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x
WebVPN-Macro-Substitution-Value2	Y	Y		String	シングル	例については、次の URL にある『*SSL VPN Deployment Guide*』を参照してください。 http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x
WebVPN-Port-Forwarding-Auto-Download-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding- Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-HTTP-Proxy-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Single-Sign-On-Server-Name		Y		String	シングル	SSO サーバの名前（1 ～ 31 文字）
WebVPN-SVC-Client-DPD	Y	Y		Integer	シングル	0 = ディセーブル n = デッドピア検出値（30 ～ 3600 秒）
WebVPN-SVC-Compression	Y	Y		Integer	シングル	0 = なし 1 = デフレート圧縮
WebVPN-SVC-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Gateway-DPD	Y	Y		Integer	シングル	0 = ディセーブル n = デッドピア検出値（30 ～ 3600 秒）
WebVPN-SVC-Keepalive	Y	Y		Integer	シングル	0 = ディセーブル n = キープアライブ値（15 ～ 600 秒）
WebVPN-SVC-Keep-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Rekey-Method	Y	Y		Integer	シングル	0 = なし 1 = SSL 2 = 新規トンネル 3 = 任意（SSL に設定）

表 14-2　ASA で LDAP 許可に対してサポートされる Cisco 属性 （続き）

属性名	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
WebVPN-SVC-Rekey-Period	Y	Y		Integer	シングル	0 = ディセーブル n = 分単位の再試行間隔（4 ～ 10080 分）
WebVPN-SVC-Required-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-Entry-Enable	Y	Y		Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-List		Y		String	シングル	URL リスト名

Cisco-AV-Pair 属性の構文

Cisco Attribute Value（AV）ペア（ID 番号 26/9/1）を使用して、（Cisco ACS のような）RADIUS サーバから、または LDAP 属性マップ経由で LDAP サーバから、ACL を適用できます。

Cisco-AV-Pair ルールの構文は次のとおりです。

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]

表 14-3 で構文のルールについて説明します。

表 14-3　AV-Pair 属性の構文ルール

フィールド	説明
Action	ルールに一致する場合に実行するアクション（deny または permit）。
Destination	パケットを受信するネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード **any** で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。
Destination Wildcard Mask	宛先アドレスに適用されるワイルドカード マスク。
Log	FILTER ログ メッセージを生成します。重大度レベル 9 のイベントを生成するには、このキーワードを使用する必要があります。
Operator	論理演算子：greater than、less than、equal to、not equal to。
Port	TCP または UDP ポートの番号（0 ～ 65535）。
Prefix	AV ペアの固有識別子。（例：ip:inacl#1=（標準 ACL 用）または webvpn:inacl#（クライアントレス SSL VPN ACL 用））。このフィールドは、フィルタが AV ペアとして送信された場合にだけ表示されます。
Protocol	IP プロトコルの番号または名前。0 ～ 255 の整数値、または **icmp**、**igmp**、**ip**、**tcp**、**udp** のいずれかのキーワード。

表 14-3　AV-Pair 属性の構文ルール （続き）

フィールド	説明
Source	パケットを送信するネットワークまたはホスト。P アドレス、ホスト名、またはキーワード **any** で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。ASA がソースまたはプロキシの役割を果たすため、このフィールドはクライアントレス SSL VPN には適用されません。
Source Wildcard Mask	送信元アドレスに適用されるワイルドカード マスク。ASA がソースまたはプロキシの役割を果たすため、このフィールドはクライアントレス SSL VPN には適用されません。

Cisco-AV-Pair の ACL 例

表 14-4 に Cisco AV ペアの例を示し、その結果の許可または拒否のアクションについて説明します。

（注）　inacl# の各 ACL # は固有である必要があります。ただし、これらは連続している（たとえば 1、2、3、4）必要はありません。たとえば、5、45、135 でもかまいません。

表 14-4　Cisco AV ペアとそのアクション許可 / 拒否の例

Cisco-AV-Pair の例	アクションの許可または拒否
`ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log`	フルトンネル IPsec または SSL VPN クライアントを使用した、2 つのホスト間の IP トラフィックを許可します。
`ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log`	フルトンネル IPsec または SSL VPN クライアントのみを使用した、すべてのホストから特定のホストのポート 80 への TCP トラフィックを許可します。

`webvpn:inacl#1=permit url http://www.example.com`
`webvpn:inacl#2=deny url smtp://server`
`webvpn:inacl#3=permit url cifs://server/share`
	指定 URL へのクライアントレス SSL VPN トラフィックを許可し、特定サーバへの SMTP トラフィックを拒否し、指定サーバへのファイル共有アクセス（CIFS）を許可します。

`webvpn:inacl#1=permit tcp 10.86.1.2 eq 2222 log` `webvpn:inacl#2=deny tcp 10.86.1.2 eq 2323 log`	クライアントレス SSL VPN について、非デフォルト ポート 2323 および 2222 で Telnet アクセスを拒否し、SSH アクセスを許可します。これらのポートを使用して通過する他のアプリケーション トラフィックも同様に許可または拒否します。

`webvpn:inacl#1=permit url ssh://10.86.1.2`
`webvpn:inacl#35=permit tcp 10.86.1.5 eq 22 log`
`webvpn:inacl#48=deny url telnet://10.86.1.2`
`webvpn:inacl#100=deny tcp 10.86.1.6 eq 23`
	クライアントレス SSL VPN でのデフォルト ポート 22 への SSH アクセスを許可し、ポート 23 への Telnet アクセスを拒否します。この例は、これらの ACL で適用される Telnet または SSH Java プラグインを使用していることを前提とします。

ACL でサポートされる URL タイプ

URL は部分的な URL でもかまいません。また、サーバを表すワイルドカードや、ポートが含まれていてもかまいません。

次の URL タイプがサポートされています。

すべての URL	https://	post://	ssh://
cifs://	ica://	rdp://	telnet://
citrix://	imap4://	rdp2://	vnc://
citrixs://	ftp://	smart-tunnel://	
http://	pop3://	smtp://	

（注）　この表に示した URL が CLI または ASDM のメニューに表示されるかどうかは、関連付けられたプラグインがイネーブルかどうかによって決まります。

Cisco-AV-Pair（ACL）使用のガイドライン

- リモート IPSec トンネルおよび SSL VPN Client（SVC）トンネルに ACL を適用するには、Cisco-AV-Pair エントリにプレフィックス ip:inacl# を追加して使用してください。
- SSL VPN クライアントレス（ブラウザモード）トンネルに ACL を適用するには、Cisco-AV-Pair エントリにプレフィックス webvpn:inacl# を追加して使用してください。
- Webtype ACL では ASA がソースとなるため、ソースを指定しないでください。

表 14-5 に、Cisco-AV-Pair 属性のトークンの一覧を示します。

表 14-5　ASA でサポートされるトークン

トークン	構文のフィールド	説明
ip:inacl#*Num*=	該当なし（識別子）	（*Num* は固有の整数）。AV ペアのアクセス コントロール リストをすべて開始します。リモート IPSec トンネルと SSL VPN（SVC）トンネルに ACL を適用します。
webvpn:inacl#*Num*=	該当なし（識別子）	（*Num* は固有の整数）。クライアントレス SSL AV ペアのアクセス コントロール リストをすべて開始します。クライアントレス（ブラウザモード）トンネルに ACL を適用します。
deny	Action	アクションを拒否します。（デフォルト）
permit	Action	アクションを許可します。
icmp	Protocol	インターネット制御メッセージ プロトコル（ICMP）
1	Protocol	インターネット制御メッセージ プロトコル（ICMP）
IP	Protocol	インターネット プロトコル（IP）
0	Protocol	インターネット プロトコル（IP）
TCP	Protocol	伝送制御プロトコル（TCP）
6	Protocol	伝送制御プロトコル（TCP）
UDP	Protocol	ユーザ データグラム プロトコル（UDP）
17	Protocol	ユーザ データグラム プロトコル（UDP）
any	Hostname	すべてのホストにルールを適用します。
host	Hostname	ホスト名を示す任意の英数字文字列。
log	Log	イベントが発生すると、フィルタ ログ メッセージが表示されます。（permit and log または deny and log の場合と同様）。

表 14-5　ASA でサポートされるトークン （続き）

トークン	構文のフィールド	説明
lt	Operator	値より小さい
gt	Operator	値より大きい
eq	Operator	値と等しい
neq	Operator	値と等しくない
range	Operator	この範囲に含まれる。range の後に 2 つの値を続けます。

Active Directory/LDAP VPN リモート アクセス許可の例

この項では、Microsoft Active Directory サーバを使用している ASA で認証および許可を設定するための手順の例を示します。説明する項目は次のとおりです。

- 「ユーザベースの属性ポリシーの適用」（P.14-16）
- 「特定のグループ ポリシーへの LDAP ユーザの配置」（P.14-18）
- 「AnyConnect トンネルへのスタティック IP アドレスの割り当て」（P.14-20）
- 「ダイヤルインの許可または拒否アクセスの適用」（P.14-22）
- 「ログイン時間と Time-of-Day ルールの適用」（P.14-25）

その他の設定例については、Cisco.com にある次のテクニカル ノートを参照してください。

- 『*ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example*』
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml
- 『*PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login*』
  http://www.cisco.com/en/US/partner/products/ps6120/products_configuration_example09186a00808d1a7c.shtml

ユーザベースの属性ポリシーの適用

すべての標準 LDAP 属性は、予約済みのベンダー固有属性（VSA）にマッピングできます。また、1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングできます。

次の例では、AD の LDAP サーバで設定されたユーザに対し、簡単なバナーを適用するように ASA を設定します。サーバ上で [General] タブの [Office] フィールドを使用してバナー テキストを入力します。このフィールドでは、physicalDeliveryOfficeName という名前の属性を使用します。ASA で、physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングする属性マップを作成します。認証の間に、ASA はサーバから physicalDeliveryOfficeName の値を取得し、その値を Cisco 属性 Banner1 にマッピングしてユーザにバナーを表示します。

この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続を使用して接続します。

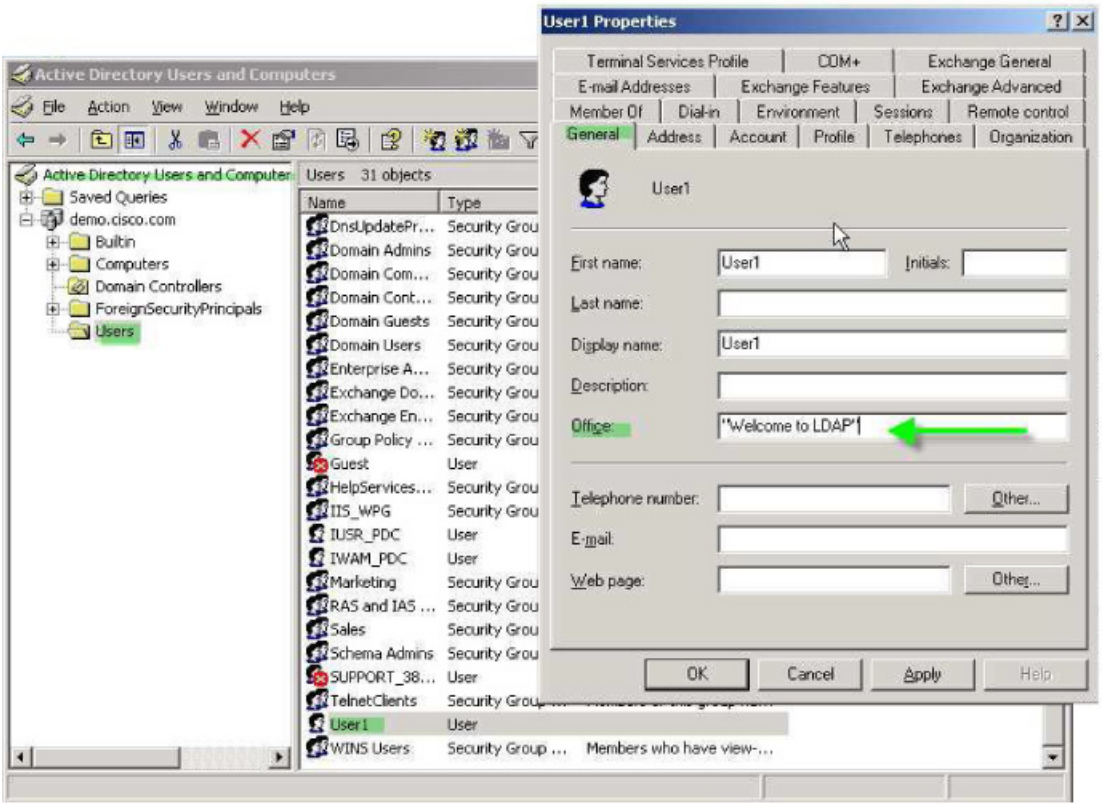
ユーザの属性を AD または LDAP サーバ上で設定するには、次の手順を実行します。

ステップ 1　ユーザを右クリックします。

[Properties] ダイアログボックスが表示されます（図 14-3 を参照）。

ステップ 2　[General] タブをクリックし、バナー テキストを [Office] フィールドに入力します。このフィールドでは、AD/LDAP 属性 physicalDeliveryOfficeName が使用されます。

図 14-3　LDAP ユーザの設定



ステップ 3　ASA 上で LDAP 属性マップを作成します。

次の例では、Banner というマップを作成し、AD/LDAP 属性 physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングします。

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ Banner を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

ステップ 5　バナーの適用をテストします。

クライアントレス SSL 接続の例を次に示します。このバナーは、ユーザ認証後に属性マップ経由で適用されたものです（図 14-4 を参照）。

図 14-4　表示されたバナー

特定のグループ ポリシーへの LDAP ユーザの配置

次に示す例では、AD LDAP サーバ上の User1 を ASA 上の特定のグループ ポリシーに対して認証する方法について説明します。サーバで、[Organization] タブの [Department] フィールドを使用して、グループ ポリシーの名前を入力します。次に、属性マップを作成し、[Department] を Cisco 属性である IETF-Radius-Class にマッピングします。認証の間に、ASA はサーバから [Department] の値を取得し、その値を IETF-Radius-Class にマッピングして User1 をグループ ポリシーに配置します。

この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続経由で接続します。

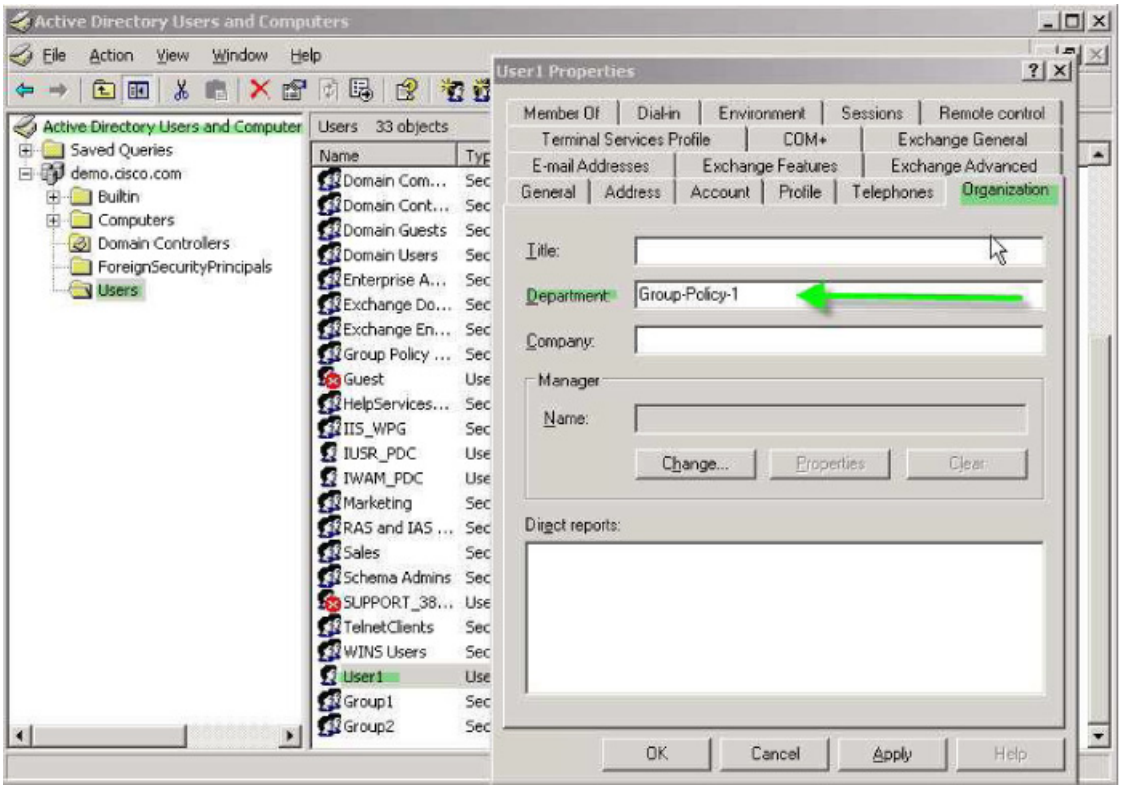
AD LDAP サーバ上のユーザの属性を設定するには、次の手順を実行します。

ステップ 1　ユーザを右クリックします。

[Properties] ダイアログボックスが表示されます（図 14-5 を参照）。

ステップ 2　[Organization] タブをクリックして、[Department] フィールドに **Group-Policy-1** と入力します。

図 14-5　AD/LDAP の [Department] 属性



ステップ 3　ステップ 1 に示した LDAP コンフィギュレーションの属性マップを定義します。

次の例では、AD 属性 Department を Cisco 属性 IETF-Radius-Class にマッピングする方法について説明します。

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ group_policy を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map group_policy
```

ステップ 5　ASA で新しい group-policy を追加し、ユーザに割り当てるために必要なポリシー属性を設定します。次の例では、Group-policy-1 を作成します。この名前は、サーバで [Department] フィールドに入力したものです。

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

ステップ 6　このユーザとして VPN 接続を確立し、Group-Policy1 からの属性（およびその他に適用可能な、デフォルトのグループ ポリシーからの属性）がセッションに継承されていることを確認します。

ステップ 7　ASA とサーバの間の通信をモニタするには、特権 EXEC モードで **debug ldap 255** コマンドをイネーブルにします。このコマンドからの出力の例を次に示します。これは、主要なメッセージがわかるように編集済みです。

```
[29] Authentication successful for user1 to 10.1.1.2
[29] Retrieving user attributes from server 10.1.1.2
```

```
[29] Retrieved Attributes:
[29] department: value = Group-Policy-1
[29] mapped to IETF-Radius-Class: value = Group-Policy-1
```

AnyConnect トンネルへのスタティック IP アドレスの割り当て

この例では、AnyConnect クライアント ユーザ Web1 を、特定のスタティック IP アドレスを受信するように設定します。そのアドレスを、AD LDAP サーバで [Dialin] タブの [Assign Static IP Address] フィールドに入力します。このフィールドでは、msRADIUSFramedIPAddress 属性を使用します。この属性を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングする属性マップを作成します。

認証時に、ASA は msRADIUSFramedIPAddress の値をサーバから取得し、その値を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングし、スタティック アドレスを User1 に渡します。

次の例が当てはまるのは、フルトンネル クライアント、つまり IPsec クライアントや SSL VPN クライアント（AnyConnect クライアント 2.x および SSL VPN クライアント）などです。

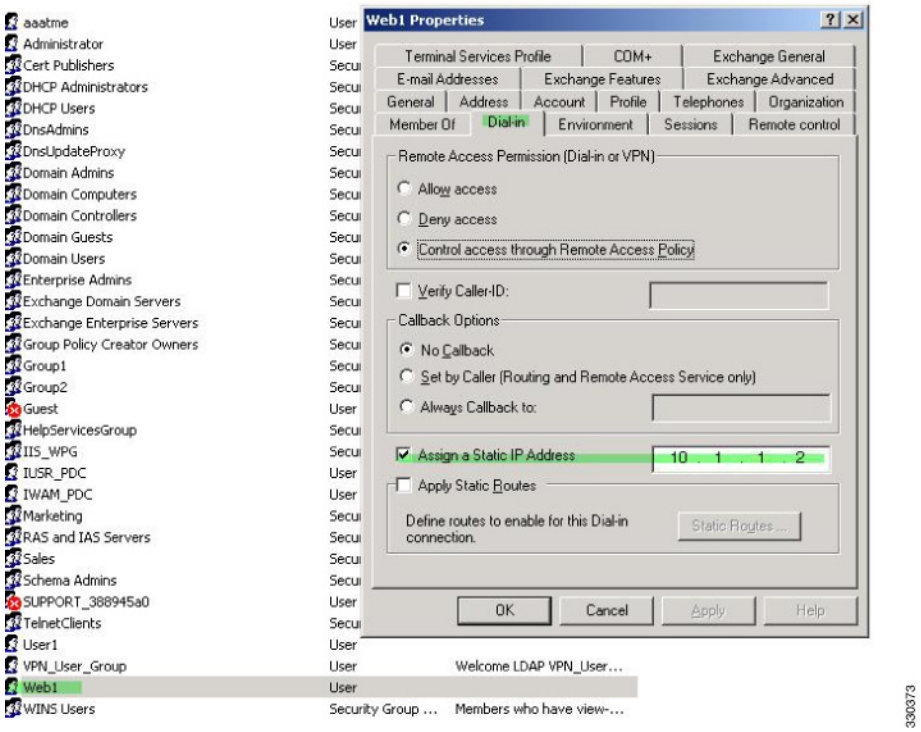
AD/LDAP サーバ上でユーザ属性を設定するには、次の手順を実行します。

ステップ 1　ユーザ名を右クリックします。

[Properties] ダイアログボックスが表示されます（図 14-6 を参照）。

ステップ 2　[Dialin] タブをクリックし、[Assign Static IP Address] チェックボックスをオンにして、IP アドレス 10.1.1.2 を入力します。

図 14-6　スタティック IP アドレスの割り当て



ステップ 3　ステップ 1 に示した LDAP コンフィギュレーションの属性マップを作成します。

次の例では、スタティック アドレス フィールドで使用されている AD 属性 msRADIUSFramedIPAddress を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングする方法を示します。

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ static_address を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

ステップ 5　**vpn-address-assignment** コマンドが AAA を指定するように設定されているかどうかを確認するために、コンフィギュレーションのこの部分を **show run all vpn-addr-assign** コマンドで表示します。

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa    << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

ステップ 6　ASA と AnyConnect クライアントとの接続を確立します。次のことを確認します。

- バナーがクライアントレス接続と同じシーケンスで受信されている（図 14-7 を参照）。
- サーバ上で設定されて ASA にマッピングされた IP アドレスをユーザが受信している（図 14-8 を参照）。

図 14-7　AnyConnect セッションのバナーの確認

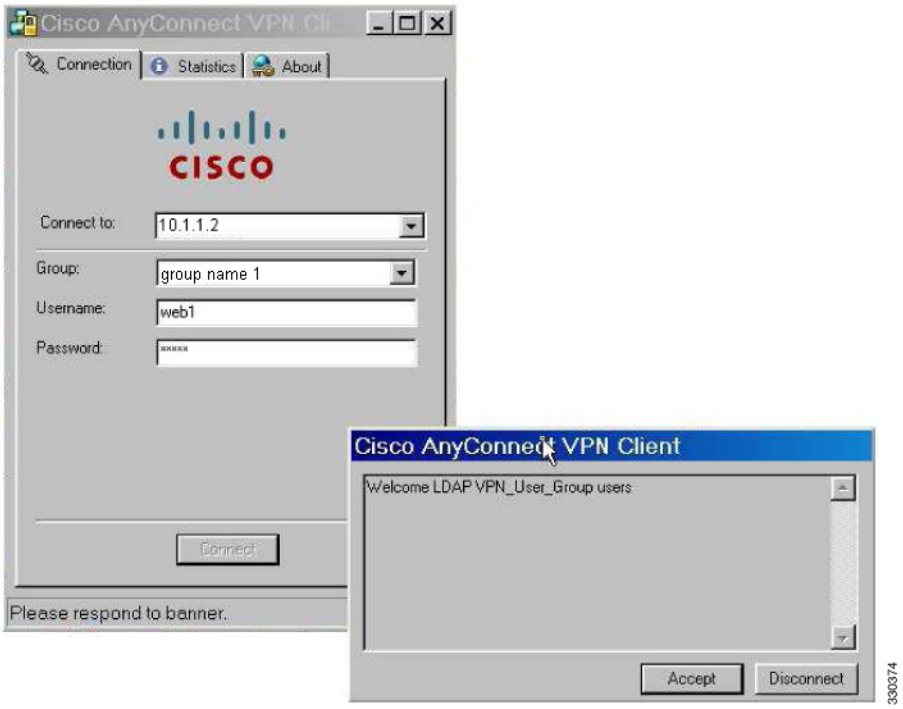
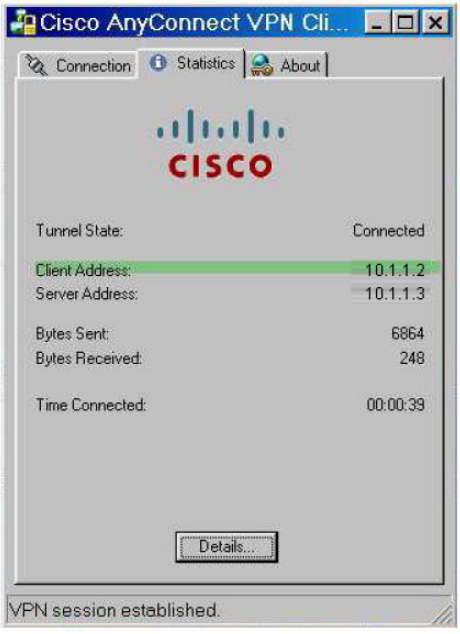


図 14-8　確立された AnyConnect セッション



ステップ 7　**show vpn-sessiondb svc** コマンドを使用してセッションの詳細を表示し、割り当てられたアドレスを確認します。

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

ダイヤルインの許可または拒否アクセスの適用

次の例では LDAP 属性マップを作成し、ユーザによって許可されるトンネリング プロトコルを指定します。[Dialin] タブでの許可アクセスと拒否アクセスの設定を、Cisco 属性 Tunneling-Protocol にマッピングします。この属性では、表 14-6 に示すビットマップ値がサポートされます。

表 14-6　Cisco Tunneling-Protocol 属性のビットマップ値

値	トンネリング プロトコル
1	PPTP
2	L2TP
4[1]	IPsec（IKEv1）

表 14-6　Cisco Tunneling-Protocol 属性のビットマップ値 （続き）

値	トンネリング プロトコル
8[2]	L2TP/IPsec
16	クライアントレス SSL
32	SSL クライアント：AnyConnect または SSL VPN クライアント
64	IPsec（IKEv2）

1. IPsec と L2TP over IPsec は同時にはサポートされません。そのため、値 4 と 8 は相互排他値となります。
2. 注 1 を参照してください。

この属性を使用して、プロトコルの [Allow Access]（TRUE）または [Deny Access]（FALSE）の条件を作成し、ユーザがアクセスを許可される方法を適用します。

この単純化した例では、トンネル プロトコル IPsec/IKEv1（4）をマッピングすることによって、Cisco VPN クライアントの許可（true）条件を作成できます。また、WebVPN（16）と SVC/AC（32）を値 48（16+32）としてマッピングし、拒否（false）条件を作成します。これで、ユーザは ASA に IPsec を使用して接続できるようになりますが、クライアントレス SSL または AnyConnect クライアントを使用して接続しようとすると拒否されます。

ダイヤルイン許可アクセスまたは拒否アクセスを適用する別の例については、次の URL にあるテクニカル ノート『*ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example*』を参照してください。

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml

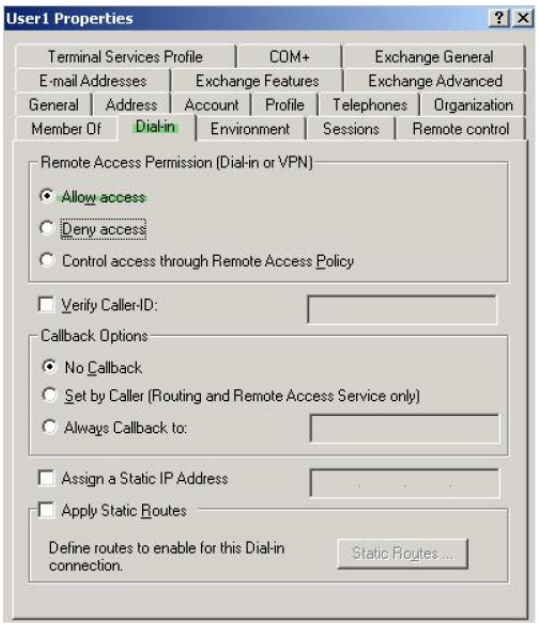
AD/LDAP サーバ上のユーザに属性を設定するには、次の手順を実行します。

ステップ 1　ユーザを右クリックします。

[Properties] ダイアログボックスが表示されます。

ステップ 2　[Dial-in] タブをクリックしてから、[Allow Access] オプション ボタンをクリックします（図 14-9）。

図 14-9　AD/LDAP User1 - 許可アクセス



（注）　[Control access through the Remote Access Policy] オプションを選択した場合は、値はサーバから返されず、適用される権限は ASA の内部グループ ポリシー設定に基づいて決定されます。

ステップ 3　IPsec と AnyConnect の両方の接続を許可するがクライアントレス SSL 接続を拒否する属性マップを作成します。

この例では、初めに tunneling_protocols というマップを作成します。次に、[Allow Access] 設定で使用される AD 属性 msNPAllowDialin を、**map-name** コマンドを使用して Cisco 属性 Tunneling-Protocols にマッピングします。次に、マップ値を **map-value** コマンドで追加します。

```
hostname(config)# ldap attribute-map tunneling_protocols
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 2 で作成した属性マップ tunneling_protocols を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

ステップ 5　属性マップが設定したとおりに機能することを確認します。

ステップ 6　クライアントレス SSL、AnyConnect クライアント、および IPsec クライアントを使用して接続を試みます。クライアントレス SSL と AnyConnect では接続に失敗し、その原因が許可されていない接続メカニズムにあることを示すメッセージが表示されます。IPsec クライアントの接続は成功します。IPsec は、属性マップに従って許可されるトンネリング プロトコルであるためです（図 14-10 および 図 14-11 を参照）。

図 14-10　クライアントレス ユーザへのログイン拒否メッセージ

図 14-11　AnyConnect クライアント ユーザへのログイン拒否メッセージ

ログイン時間と Time-of-Day ルールの適用

次の例では、クライアントレス SSL ユーザ（たとえばビジネス パートナー）にネットワークへのアクセスを許可する時間帯を設定して適用する方法を示します。

AD サーバ上で、[Office] フィールドを使用してパートナーの名前を入力します。このフィールドでは、physicalDeliveryOfficeName 属性が使用されます。次に、ASA で属性マップを作成し、その属性を Cisco 属性 Access-Hours にマッピングします。認証時に、ASA はサーバから physicalDeliveryOfficeName の値を取得して Access-Hours にマッピングします。

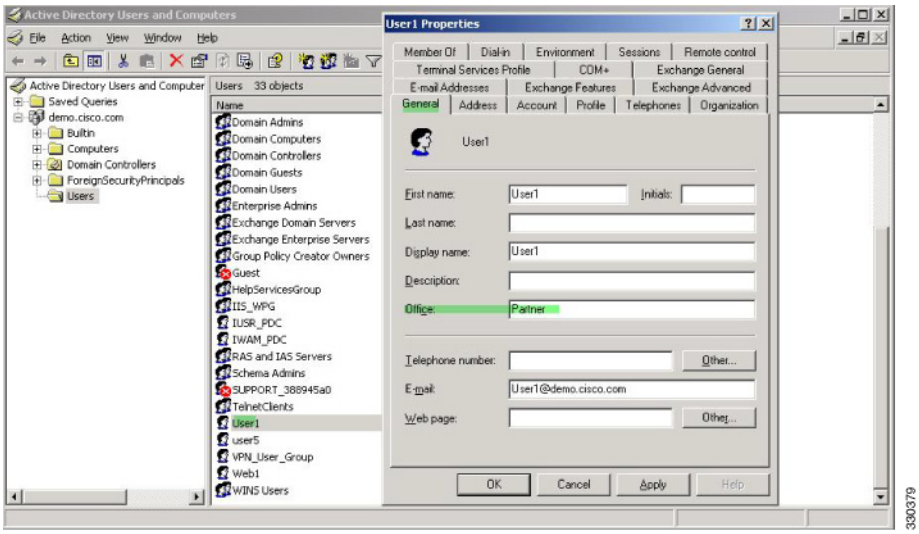
AD/LDAP サーバ上でユーザ属性を設定するには、次の手順を実行します。

ステップ 1　ユーザを選択して [Properties] を右クリックします。

[Properties] ダイアログボックスが表示されます（図 14-12 を参照）。

ステップ 2　[General] タブをクリックします。

図 14-12　Active Directory [Properties] ダイアログボックス



ステップ 3　属性マップを作成します。

次の例では、属性マップ access_hours を作成して AD 属性 physicalDeliveryOfficeName（[Office] フィールドで使用）を Cisco 属性 Access-Hours にマッピングする方法を示します。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

ステップ 4　LDAP 属性マップを AAA サーバに関連付けます。

次の例では、AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバ ホスト コンフィギュレーション モードを開始し、ステップ 3 で作成した属性マップ access_hours を関連付けます。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

ステップ 5　各値にサーバで許可された時間範囲を設定します。

次の例では、Partner のアクセス時間が月曜日から金曜日の午前 9 時から午後 5 時に設定されています。

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

VPN のための LDAP での許可の設定

VPN アクセスのための LDAP 認証が成功すると、ASA は、LDAP 属性を返す LDAP サーバのクエリーを実行します。通常これらの属性には、VPN セッションに適用される許可データが含まれます。

この許可メカニズムとは別の異なる許可を LDAP ディレクトリ サーバから取得することが必要な場合があります。たとえば、認証に SDI または証明書サーバを使用している場合、許可情報は返されません。この場合、ユーザ許可では、認証の成功後に LDAP ディレクトリのクエリーを実行するため、認証と許可は 2 つのステップで行われます。

LDAP を使用した VPN ユーザ許可を設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的

ステップ 1	**aaa-server** *server_group* **protocol** {**kerberos** | **ldap** | **nt** | **radius** | **sdi** | **tacacs+**}
	
	例：
	`hostname(config)# aaa-server servergroup1 protocol ldap`
	`hostname(config-aaa-server-group)`
		AAA サーバ グループを作成します。

ステップ 2	**tunnel-group** *groupname* **例：** `hostname(config)# tunnel-group remotegrp`	「remotegrp」という名前の IPsec リモート アクセス トンネル グループを作成します。
ステップ 3	**tunnel-group** *groupname* **general-attributes** **例：** `hostname(config)# tunnel-group remotegrp general-attributes`	サーバ グループとトンネル グループを関連付けます。
ステップ 4	**authorization-server-group** *group-tag* **例：** `hostname(config-general)# authorization-server-group ldap_dir_1`	以前作成した認証のための AAA サーバ グループに新しいトンネル グループを割り当てます。

例

特定の要件で使用できる許可関連のコマンドとオプションは他にもありますが、次の例では、LDAP でのユーザ許可をイネーブルにするコマンドを示します。この例では、remote-1 という名前の IPsec リモートアクセス トンネルグループを作成し、すでに作成してある許可用の ldap_dir_1 AAA サーバ グループにその新しいトンネルグループを割り当てています。

```
hostname(config)# tunnel-group remote-1 type ipsec-ra
hostname(config)# tunnel-group remote-1 general-attributes
hostname(config-general)# authorization-server-group ldap_dir_1
hostname(config-general)#
```

この設定が完了したら、次のコマンドを入力して、ディレクトリ パスワード、ディレクトリ検索の開始点、ディレクトリ検索の範囲など、追加の LDAP 許可パラメータを設定できます。

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# ldap-login-dn obscurepassword
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

外部 RADIUS サーバの設定

この項では、RADIUS の設定手順の概要を示し、Cisco RADIUS 属性を定義します。説明する項目は次のとおりです。

RADIUS 設定手順の確認

この項では、ASA ユーザの認証および許可をサポートするために必要な RADIUS 設定手順について説明します。

RADIUS サーバを ASA と相互運用するように設定するには、次の手順を実行します。

ステップ 1　ASA の属性を RADIUS サーバにロードします。属性をロードするために使用する方法は、使用する RADIUS サーバのタイプによって異なります。

- Cisco ACS を使用している場合：サーバには、これらの属性がすでに統合されています。したがって、この手順をスキップできます。
- 他のベンダーの RADIUS サーバ（たとえば Microsoft Internet Authentication Service）の場合：ASA の各属性を手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダー コード（3076）を使用します。ASA の RADIUS 許可属性および値のリストについては、表 14-7 を参照してください。

ステップ 2　ユーザまたはグループの権限および属性をセットアップします。これらは、IPsec または SSL トンネルの確立時に送信されます。

ASA の RADIUS 許可属性

許可では、権限または属性を使用するプロセスを参照します。認証サーバとして定義されている RADIUS サーバは、権限または属性が設定されている場合はこれらを使用します。これらの属性のベンダー ID は 3076 です。

表 14-7 に、ユーザ許可に使用でき、ASA がサポートしている使用可能な RADIUS 属性の一覧を示します。

（注）　RADIUS 属性名には、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS の属性名にはまだ cVPN3000 プレフィックスが含まれています。ASA によって RADIUS 属性が適用されるときは、属性名ではなく数値の属性 ID に基づいて適用されます。LDAP 属性は、ID ではなく属性名で使用します。

表 14-7 に示した属性はすべてダウンストリーム属性であり、RADIUS サーバから ASA に送信されます。ただし、属性番号 146、150、151、および 152 を除きます。これらの属性番号はアップストリーム属性であり、ASA から RADIUS サーバに送信されます。RADIUS 属性 146 および 150 は、認証および許可の要求の場合に ASA から RADIUS サーバに送信されます。前述の 4 つの属性はすべて、ア

カウンティング開始、中間アップデート、および終了の要求の場合に ASA から RADIUS サーバに送信されます。アップストリーム RADIUS 属性 146、150、151、および 152 は ASA バージョン 8.4.3 で導入されました。
Cisco ACS 5x および Cisco ISE は、ASA バージョン 9.0 の RADIUS 認証を使用する IP アドレスの割り当ての IPv6 Framed IP アドレスはサポートされません。

表 14-7　ASA でサポートされる RADIUS 属性と値

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	String	シングル	時間範囲の名前（Business-hours など）
Access-List-Inbound	Y	86	String	シングル	ACL ID
Access-List-Outbound	Y	87	String	シングル	ACL ID
Address-Pools	Y	217	String	シングル	IP ローカル プールの名前
Allow-Network-Extension-Mode	Y	64	Boolean	シングル	0 = ディセーブル 1 = イネーブル
Authenticated-User-Idle-Timeout	Y	50	Integer	シングル	1 ～ 35791394 分
Authorization-DN-Field	Y	67	String	シングル	有効な値 : UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
Authorization-Required		66	Integer	シングル	0 = しない 1 = する
Authorization-Type	Y	65	Integer	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	15	String	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列
Banner2	Y	36	String	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列。Banner2 文字列は Banner1 文字列に連結されます（設定されている場合）。
Cisco-IP-Phone-Bypass	Y	51	Integer	シングル	0 = ディセーブル 1 = イネーブル
Cisco-LEAP-Bypass	Y	75	Integer	シングル	0 = ディセーブル 1 = イネーブル

表 14-7　ASA でサポートされる RADIUS 属性と値 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
Client Type	Y	150	Integer	シングル	1 = Cisco VPN クライアント（IKEv1） 2 = AnyConnect クライアント SSL VPN 3 = クライアントレス SSL VPN 4 = カットスルー プロキシ 5 = L2TP/IPsec SSL VPN 6 = AnyConnect クライアント IPsec VPN（IKEv2）
Client-Type-Version-Limiting	Y	77	String	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	String	シングル	IP アドレス
Extended-Authentication-On-Rekey	Y	122	Integer	シングル	0 = ディセーブル 1 = イネーブル
Group-Policy	Y	25	String	シングル	リモート アクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の 3 つの形式のいずれかを使用できます。 • *グループ ポリシー名* • OU= *グループ ポリシー名* • OU= *グループ ポリシー名*;
IE-Proxy-Bypass-Local		83	Integer	シングル	0 = なし 1 = ローカル
IE-Proxy-Exception-List		82	String	シングル	改行（\n）区切りの DNS ドメインのリスト
IE-Proxy-PAC-URL	Y	133	String	シングル	PAC アドレス文字列
IE-Proxy-Server		80	String	シングル	IP アドレス
IE-Proxy-Server-Policy		81	Integer	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検出 4 = コンセントレータ設定を使用する
IKE-KeepAlive-Confidence-Interval	Y	68	Integer	シングル	10 ～ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	Integer	シングル	2 ～ 10 秒
IKE-Keep-Alives	Y	41	Boolean	シングル	0 = ディセーブル 1 = イネーブル
Intercept-DHCP-Configure-Msg	Y	62	Boolean	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Allow-Passwd-Store	Y	16	Boolean	シングル	0 = ディセーブル 1 = イネーブル

表 14-7　ASA でサポートされる RADIUS 属性と値 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
IPsec-Authentication		13	Integer	シングル	0 = なし 1 = RADIUS 2 = LDAP（許可のみ） 3 = NT ドメイン 4 = SDI 5 = 内部 6 = RADIUS での Expiry 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	Boolean	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Backup-Server-List	Y	60	String	シングル	サーバ アドレス（スペース区切り）
IPsec-Backup-Servers	Y	59	String	シングル	1 = クライアントが設定したリストを使用する 2 = クライアント リストをディセーブルにして消去する 3 = バックアップ サーバ リストを使用する
IPsec-Client-Firewall-Filter-Name		57	String	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	58	Integer	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	28	String	シングル	クライアントに送信するデフォルト ドメイン名を 1 つだけ指定します（1 ～ 255 文字）。
IPsec-IKE-Peer-ID-Check	Y	40	Integer	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	39	Integer	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Mode-Config	Y	31	Boolean	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP	Y	34	Boolean	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP-Port	Y	35	Integer	シングル	4001 ～ 49151。デフォルトは 10000 です。
IPsec-Required-Client-Firewall-Capability	Y	56	Integer	シングル	0 = なし 1 = リモート FW Are-You-There（AYT）で定義されているポリシー 2 = Policy pushed CPP 4 = サーバからのポリシー
IPsec-Sec-Association		12	String	シングル	セキュリティ アソシエーションの名前

表 14-7　ASA でサポートされる RADIUS 属性と値 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
IPsec-Split-DNS-Names	Y	29	String	シングル	クライアントに送信するセカンダリ ドメイン名のリストを指定します（1 ～ 255 文字）。
IPsec-Split-Tunneling-Policy	Y	55	Integer	シングル	0 = スプリット トンネリングなし 1 = スプリット トンネリング 2 = ローカル LAN を許可
IPsec-Split-Tunnel-List	Y	27	String	シングル	スプリット トンネルの包含リストを記述したネットワークまたは ACL の名前を指定します。
IPsec-Tunnel-Type	Y	30	Integer	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	Boolean	シングル	0 = ディセーブル 1 = イネーブル
IPv6-Address-Pools	Y	218	String	シングル	IP ローカル プール IPv6 の名前
IPv6-VPN-Filter	Y	219	String	シングル	ACL 値
L2TP-Encryption		21	Integer	シングル	ビットマップ： 1 = 暗号化が必要 2 =40 ビット 4 =128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化 / ステートレスが必要
L2TP-MPPC-Compression		38	Integer	シングル	0 = ディセーブル 1 = イネーブル
Member-Of	Y	145	String	シングル	カンマ区切りの文字列。例： `Engineering, Sales` ダイナミック アクセス ポリシーで使用できる管理属性。グループ ポリシーは設定されません。
MS-Client-Subnet-Mask	Y	63	Boolean	シングル	IP アドレス
NAC-Default-ACL		92	String		ACL
NAC-Enable		89	Integer	シングル	0 = しない 1 = する
NAC-Revalidation-Timer		91	Integer	シングル	300 ～ 86400 秒
NAC-Settings	Y	141	String	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	Integer	シングル	30 ～ 1800 秒
Perfect-Forward-Secrecy-Enable	Y	88	Boolean	シングル	0 = しない 1 = する

表 14-7　ASA でサポートされる RADIUS 属性と値 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
PPTP-Encryption		20	Integer	シングル	ビットマップ： 1 = 暗号化が必要 2 =40 ビット 4 =128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化 / ステートレスが必要
PPTP-MPPC-Compression		37	Integer	シングル	0 = ディセーブル 1 = イネーブル
Primary-DNS	Y	5	String	シングル	IP アドレス
Primary-WINS	Y	7	String	シングル	IP アドレス
Privilege-Level	Y	220	Integer	シングル	0 ～ 15 の整数。
Required-Client- Firewall-Vendor-Code	Y	45	Integer	シングル	1 = シスコ（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコ（Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Description	Y	47	String	シングル	文字列
Required-Client-Firewall-Product-Code	Y	46	Integer	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	Integer	シングル	0 = ディセーブル 1 = イネーブル
Require-HW-Client-Auth	Y	48	Boolean	シングル	0 = ディセーブル 1 = イネーブル
Secondary-DNS	Y	6	String	シングル	IP アドレス
Secondary-WINS	Y	8	String	シングル	IP アドレス
SEP-Card-Assignment		9	Integer	シングル	未使用

表 14-7　ASA でサポートされる RADIUS 属性と値 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
Session Subtype	Y	152	Integer	シングル	0 = なし 1 = クライアントレス 2 = クライアント 3 = クライアントのみ Session Subtype が適用されるのは、Session Type（151）属性の値が 1、2、3、または 4 の場合のみです。
Session Type	Y	151	Integer	シングル	0 = なし 1 = AnyConnect クライアント SSL VPN 2 = AnyConnect クライアント IPSec VPN（IKEv2） 3 = クライアントレス SSL VPN 4 = クライアントレス電子メール プロキシ 5 = Cisco VPN クライアント（IKEv1） 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロード バランシング
Simultaneous-Logins	Y	2	Integer	シングル	0 ～ 2147483647
Smart-Tunnel	Y	136	String	シングル	スマート トンネルの名前
Smart-Tunnel-Auto	Y	138	Integer	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動スタート
Smart-Tunnel-Auto-Signon-Enable	Y	139	String	シングル	ドメイン名が付加された Smart Tunnel Auto Signon リストの名前
Strip-Realm	Y	135	Boolean	シングル	0 = ディセーブル 1 = イネーブル
SVC-Ask	Y	131	String	シングル	0 = ディセーブル 1 = イネーブル 3 = デフォルト サービスをイネーブルにする 5 = デフォルト クライアントレスをイネーブルにする （2 と 4 は使用しない）
SVC-Ask-Timeout	Y	132	Integer	シングル	5 ～ 120 秒
SVC-DPD-Interval-Client	Y	108	Integer	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	Integer	シングル	0 = オフ 5 ～ 3600 秒
SVC-DTLS	Y	123	Integer	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	Integer	シングル	0 = オフ 15 ～ 600 秒

表 14-7　ASA でサポートされる RADIUS 属性と値 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
SVC-Modules	Y	127	String	シングル	文字列（モジュールの名前）
SVC-MTU	Y	125	Integer	シングル	MTU 値 256 ～ 1406 バイト
SVC-Profiles	Y	128	String	シングル	文字列（プロファイルの名前）
SVC-Rekey-Time	Y	110	Integer	シングル	0 = ディセーブル 1 ～ 10080 分
Tunnel Group Name	Y	146	String	シングル	1 ～ 253 文字
Tunnel-Group-Lock	Y	85	String	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	Y	11	Integer	シングル	1 = PPTP 2 = L2TP 4 = IPSec（IKEv1） 8 = L2TP/IPSec 16 = WebVPN. 32 = SVC 64 = IPsec（IKEv2） 8 および 4 は相互排他値 （0 ～ 11、16 ～ 27、32 ～ 43、48 ～ 59 は有効値）。
Use-Client-Address		17	Boolean	シングル	0 = ディセーブル 1 = イネーブル
VLAN	Y	140	Integer	シングル	0 ～ 4094
WebVPN-Access-List	Y	73	String	シングル	アクセス リスト名
WebVPN ACL	Y	73	String	シングル	デバイスの WebVPN ACL 名
WebVPN-ActiveX-Relay	Y	137	Integer	シングル	0 = ディセーブル Otherwise = イネーブル
WebVPN-Apply-ACL	Y	102	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Auto-HTTP-Signon	Y	124	String	シングル	予約済み
WebVPN-Citrix-Metaframe-Enable	Y	101	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Content-Filter-Parameters	Y	69	Integer	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメージ 8 = イメージに含まれるクッキー
WebVPN-Customization	Y	113	String	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	String	シングル	URL（たとえば http://example-example.com）
WebVPN-Deny-Message	Y	116	String	シングル	有効な文字列（500 文字以内）
WebVPN-Download_Max-Size	Y	157	Integer	シングル	0x7fffffff

表 14-7　ASA でサポートされる RADIUS 属性と値 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
WebVPN-File-Access-Enable	Y	94	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Browsing-Enable	Y	96	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Entry-Enable	Y	95	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	Y	78	String	シングル	オプションのワイルドカード（*）を使用したカンマ区切りの DNS/IP（たとえば、*.cisco.com、192.168.1.*、wwwin.cisco.com）
WebVPN-Hidden-Shares	Y	126	Integer	シングル	0 = なし 1 = 表示
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	Boolean	シングル	クライアントレス ホーム ページをスマート トンネル経由で表示する場合にイネーブルにします。
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ 8 = クッキー
WebVPN-HTTP-Compression	Y	120	Integer	シングル	0 = オフ 1 = デフレート圧縮
WebVPN-HTTP-Proxy-IP-Address	Y	74	String	シングル	http= または https= プレフィックス付きの、カンマ区切りの DNS/IP: ポート（例：http=10.10.10.10:80、https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	Y	148	Integer	シングル	0（ディセーブル）～ 30
WebVPN-Keepalive-Ignore	Y	121	Integer	シングル	0 ～ 900
WebVPN-Macro-Substitution	Y	223	String	シングル	無制限。例については、次の URL にある『*SSL VPN Deployment Guide*』を参照してください。 http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x
WebVPN-Macro-Substitution	Y	224	String	シングル	無制限。例については、次の URL にある『*SSL VPN Deployment Guide*』を参照してください。 http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x
WebVPN-Port-Forwarding-Enable	Y	97	Integer	シングル	0 = ディセーブル 1 = イネーブル

表 14-7　ASA でサポートされる RADIUS 属性と値 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-List	Y	72	String	シングル	ポート転送リスト名
WebVPN-Port-Forwarding-Name	Y	79	String	シングル	文字列の名前（「Corporate-Apps」など） このテキストでクライアントレス ポータル ホームページのデフォルト文字列「Application Access」が置き換えられます。
WebVPN-Post-Max-Size	Y	159	Integer	シングル	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	Integer	シングル	0（ディセーブル）～ 30
WebVPN Smart-Card-Removal-Disconnect	Y	225	Boolean	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Smart-Tunnel	Y	136	String	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	String	シングル	ドメイン名が付加されたスマート トンネル自動サインオン リストの名前
WebVPN-Smart-Tunnel-Auto-Start	Y	138	Integer	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動開始
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	String	シングル	「e ネットワーク名」、「i ネットワーク名」、「a」のいずれか。ここで、ネットワーク名は、スマート トンネル ネットワークのリストの名前です。e はトンネルが除外されることを示し、i はトンネルが指定されることを示し、a はすべてのトンネルを示します。
WebVPN-SSL-VPN-Client-Enable	Y	103	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Keep- Installation	Y	105	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Required	Y	104	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSO-Server-Name	Y	114	String	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	String	シングル	
WebVPN-Storage-Objects	Y	161	String	シングル	
WebVPN-SVC-Keepalive-Frequency	Y	107	Integer	シングル	15 ～ 600 秒、0=オフ
WebVPN-SVC-Client-DPD-Frequency	Y	108	Integer	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-DTLS-Enable	Y	123	Integer	シングル	0 = ディセーブル 1 = イネーブル

表 14-7　ASA でサポートされる RADIUS 属性と値 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
WebVPN-SVC-DTLS-MTU	Y	125	Integer	シングル	MTU 値は 256 ～ 1406 バイトです。
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	Integer	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-Rekey-Time	Y	110	Integer	シングル	4 ～ 10080 分、0=オフ
WebVPN-SVC-Rekey-Method	Y	111	Integer	シングル	0（オフ）、1（SSL）、2（新しいトンネル）
WebVPN-SVC-Compression	Y	112	Integer	シングル	0（オフ）、1（デフォルトの圧縮）
WebVPN-UNIX-Group-ID (GID)	Y	222	Integer	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	Integer	シングル	UNIX での有効なユーザ ID
WebVPN-Upload-Max-Size	Y	158	Integer	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-List	Y	71	String	シングル	URL リスト名
WebVPN-User-Storage	Y	160	String	シングル	
WebVPN-VDI	Y	163	String	シングル	設定のリスト

ASA IETF RADIUS 許可属性

表 14-8 に、サポートされている IETF RADIUS 属性を示します。

表 14-8　ASA でサポートされる IETF RADIUS 属性と値

属性名	VPN 3000	ASA	PIX	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Class	Y	Y	Y	25		シングル	バージョン 8.2.x 以降の場合は、表 14-7 で説明している Group-Policy 属性（VSA 3076、#25）を使用することを推奨します。 • *グループ ポリシー名* • OU= *グループ ポリシー名* • OU= *グループ ポリシー名*
IETF-Radius-Filter-Id	Y	Y	Y	11	String	シングル	フルトンネルの IPsec クライアントと SSL VPN クライアントのみに適用される、ASA で定義された ACL 名
IETF-Radius-Framed-IP-Address	Y	Y	Y	n/a	String	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	Y	Y	n/a	String	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	Y	Y	28	Integer	シングル	秒

表 14-8　ASA でサポートされる IETF RADIUS 属性と値 （続き）

IETF-Radius-Service-Type	Y	Y	Y	6	Integer	シングル	秒。使用可能なサービス タイプの値： .Administrative：ユーザは configure プロンプトへのアクセスを許可されています。 .NAS-Prompt：ユーザは exec プロンプトへのアクセスを許可されています。 .remote-access：ユーザはネットワーク アクセスを許可されています。
IETF-Radius-Session-Timeout	Y	Y	Y	27	Integer	シングル	秒

RADIUS アカウンティング切断の理由コード

これらのコードは、パケットを送信するときに ASA が切断された場合に返されます。

表 14-9

切断の理由コード
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

外部 TACACS+ サーバの設定

ASA は、TACACS+ 属性をサポートします。TACACS+ は、認証、許可、アカウンティングの機能を分離します。プロトコルでは、必須とオプションの 2 種類の属性をサポートします。サーバとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。

（注）　TACACS+ 属性を使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認してください。

表 14-10 に、カットスルー プロキシ接続に対してサポートされている TACACS+ 許可応答属性の一覧を示します。表 14-11 に、サポートされている TACACS+ アカウンティング属性の一覧を示します。

表 14-10　サポートされる TACACS+ 許可応答属性

属性	説明
acl	接続に適用する、ローカルで設定済みの ACL を識別します。
idletime	認証済みユーザ セッションが終了する前に許可される非アクティブ時間（分）を示します。
timeout	認証済みユーザ セッションが終了する前に認証クレデンシャルがアクティブな状態でいる絶対時間（分）を指定します。

表 14-11　サポートされる TACACS+ アカウンティング属性

属性	説明
bytes_in	この接続中に転送される入力バイト数を指定します（ストップ レコードのみ）。
bytes_out	この接続中に転送される出力バイト数を指定します（ストップ レコードのみ）。
cmd	実行するコマンドを定義します（コマンド アカウンティングのみ）。
disc-cause	切断理由を特定する数字コードを示します（ストップ レコードのみ）。
elapsed_time	接続の経過時間（秒）を定義します（ストップ レコードのみ）。
foreign_ip	トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
local_ip	トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
NAS port	接続のセッション ID が含まれます。
packs_in	この接続中に転送される入力パケット数を指定します。
packs_out	この接続中に転送される出力パケット数を指定します。
priv-level	コマンド アカウンティング要求の場合はユーザの権限レベル、それ以外の場合は 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。
service	使用するサービスを指定します。コマンド アカウンティングだけは、常に「シェル」に設定されます。
task_id	アカウンティング トランザクションに固有のタスク ID を指定します。
username	ユーザの名前を示します。

ユーザに対する VPN ポリシー属性の設定

前提条件

この手順では、既存のユーザを編集する方法について説明します。詳細については、“Adding a User Account to the Local Database” section on page 32-22 を参照してください。

手順の詳細