VPN の外部 AAA サーバーの設定

- 外部 AAA サーバーについて （1 ページ）
- 外部 AAA サーバーを使用する際のガイドライン （2 ページ）
- 複数証明書認証の設定 （2 ページ）
- Active Directory/LDAP VPN リモート アクセス許可の例 （3 ページ）

外部 AAA サーバーについて

この ASA は、外部の LDAP、RADIUS、TACACS+ サーバーを使用して、ASA の認証、認可、アカウンティング（AAA）をサポートするように設定できます。外部 AAA サーバーは、設定されたアクセス許可と属性を適用します。外部サーバーを使用するように ASA を設定する前に、適切な ASA 許可属性を指定して外部 AAA サーバーを設定し、それらの属性のサブセットから特定のアクセス許可を個々のユーザーに割り当てる必要があります。

許可属性のポリシー適用の概要

ASA は、ユーザー認可属性（ユーザー権利またはユーザー権限とも呼ばれる）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。ASA を設定して、次のいずれかの組み合わせからユーザー属性を取得できます。

- ASA のダイナミック アクセス ポリシー（DAP）
- 外部 RADIUS または LDAP 認証および許可サーバー（およびその両方）
- ASA のグループ ポリシー

ASA がすべてのソースから属性を受信すると、それらの属性は評価されて集約され、ユーザー ポリシーに適用されます。属性の間で衝突がある場合、DAP 属性が優先されます。

ASA は次の順序で属性を適用します。

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、他のど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 サーバー上のユーザー属性：ユーザー認証や認可が成功すると、サーバー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 データベースで個々のユーザーに設定されている属性（ASDM のユーザー アカウント）と混同しないようにしてください。

3. ASA で設定されているグループ ポリシー：RADIUS サーバーからユーザーに対して RADIUS CLASS 属性 IETF-Class-25 （OU=*group-policy*）の値が返された場合、ASA はそのユーザーを同じ名前のグループ ポリシーに配置し、そのグループ ポリシーの属性のうち、サーバーから返されないものを適用します。

   LDAP サーバーでは、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 上に設定された 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、認証前にユーザー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 に接続しているすべてのユーザーは、最初にこのグループに所属します。このグループで、DAP、サーバーから返されるユーザー属性、ユーザーに割り当てられているグループ ポリシーにはない属性が提供されます。

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、ユーザー属性、グループ ポリシー、接続プロファイルで不足している値を提供します。

外部 AAA サーバーを使用する際のガイドライン

ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を適用します。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 属性は、RADIUS の章に記載されている RADIUS 属性のサブセットです。

複数証明書認証の設定

AnyConnect クライアント SSL クライアントプロトコルと IKEv2 クライアントプロトコルを使用して、セッションごとに複数の認証を検証できるようになりました。たとえば、マシン証明書の発行元が特定の CA と一致することでデバイスが企業から支給されたデバイスであることを確認できます。

複数証明書オプションを使用すると、証明書を通じたマシンとユーザー両方の証明書認証が可能になります。このオプションがなければ、両方ではなく一方のみの証明書認証しか行うことができません。

（注） 複数の証明書認証にはマシン証明書とユーザー証明書（または2つのユーザー証明書）が必要であるため、この機能では AnyConnect クライアント Start Before Logon（SBL）を使用できません。

ユーザー名の事前入力フィールドでは、2 つ目の（ユーザー）証明書のフィールドを解析し、AAA および証明書認証済みの接続で以降の AAA 認証に使用することができます。プライマリとセカンダリの両方の事前入力のユーザー名は、常にクライアントから受信した2つ目の（ユーザー）証明書から取得されます。

9.14(1) 以降、ASA では、複数証明書認証を設定し、認証または許可にユーザー名の事前入力オプションを使用する場合に、プライマリユーザー名およびセカンダリユーザー名を取得する証明書を指定できます。詳細については、AnyConnect クライアント接続プロファイル、認証属性を参照してください。

複数証明書認証では、2つの証明書が認証されます。クライアントから受信した2つ目の（ユーザー）証明書は、事前入力および証明書由来のユーザー名のプライマリおよびセカンダリ ユーザー名による解析対象です。

SAML による複数証明書認証も設定できます。

複数証明書認証では、その接続試行を認証するために使用された証明書のフィールドに基づいてポリシー決定を行うことができます。複数証明書認証中にクライアントから受信したユーザーおよびマシンの証明書は DAP にロードされ、証明書のフィールドに基づいてポリシーを設定することができます。接続試行を許可または拒否するルールを設定できるようにダイナミック アクセス ポリシー（DAP）を使用して複数証明書認証を追加するには、『ASA VPN ASDM Configuration Guide』の適切なリリースの「*Add Multiple Certificate Authentication to DAP*」を参照してください。

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

この項では、Microsoft Active Directory サーバーを使用している ASA で認証および認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。

- ユーザー ベースの属性のポリシー適用 （4 ページ）
- AnyConnect クライアント トンネルのスタティック IP アドレス割り当ての適用 （7 ページ）
- ダイヤルイン許可または拒否アクセスの適用 （9 ページ）
- ログオン時間と Time-of-Day ルールの適用 （11 ページ）

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』
- 『PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login』

ユーザー ベースの属性のポリシー適用

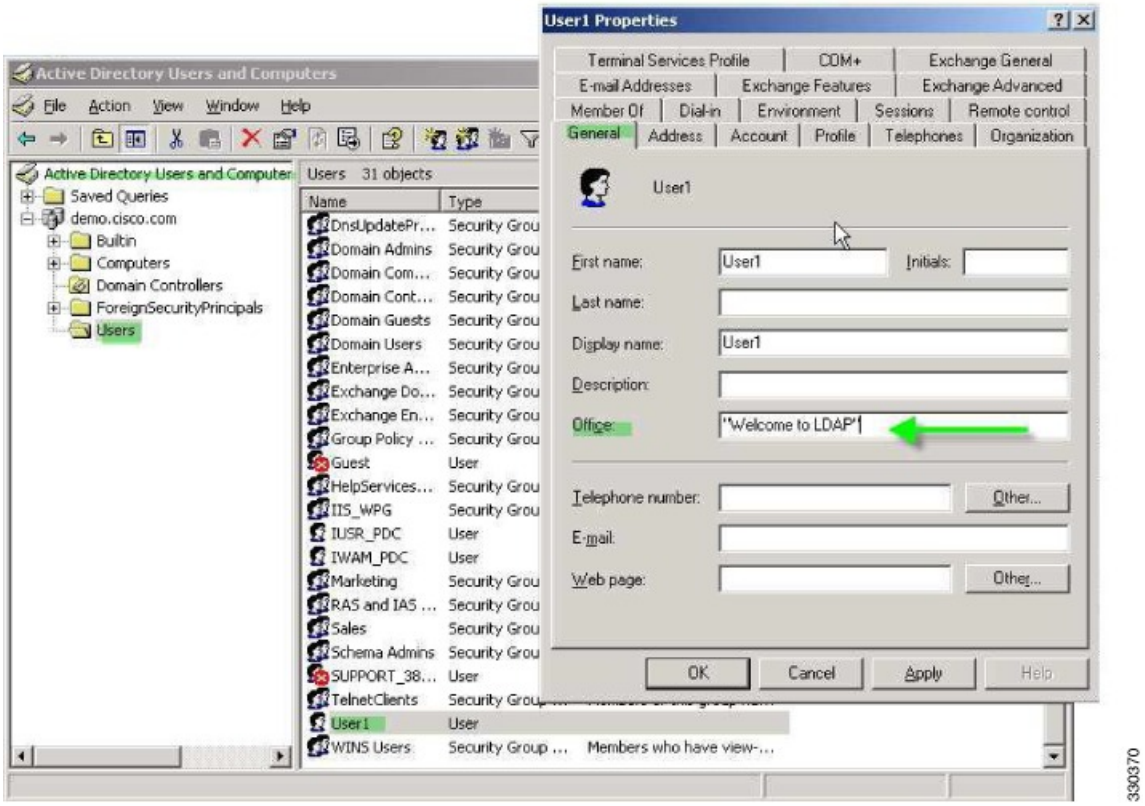
この例では、ユーザー向けの簡易バナーを表示して、標準の LDAP 属性を既知のベンダー固有属性（VSA）にマッピングする方法と 1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングする方法を示します。IPsec VPN クライアントやAnyConnect クライアントなど、どの接続タイプにも適用されます。

AD LDAP サーバー上で設定されたユーザーに簡易バナーを適用するには、[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。

認証時、ASA はサーバーから 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ーにバナーを表示します。

手順

ステップ 1 ユーザー名を右クリックして、[Properties] ダイアログボックスの [General] タブを開き、AD/LDAP 属性 physicalDeliveryOfficeName を使用する [Office] フィールドにバナー テキストを入力します。



ステップ 2 ASA で LDAP 属性マップを作成します。

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 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ MS_LDAP のホスト 10.1.1.2 の AAA サーバー ホスト コンフィギュレーション モードを開始し、以前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 4 バナーの適用をテストします。

特定のグループ ポリシーへの LDAP ユーザーの配置

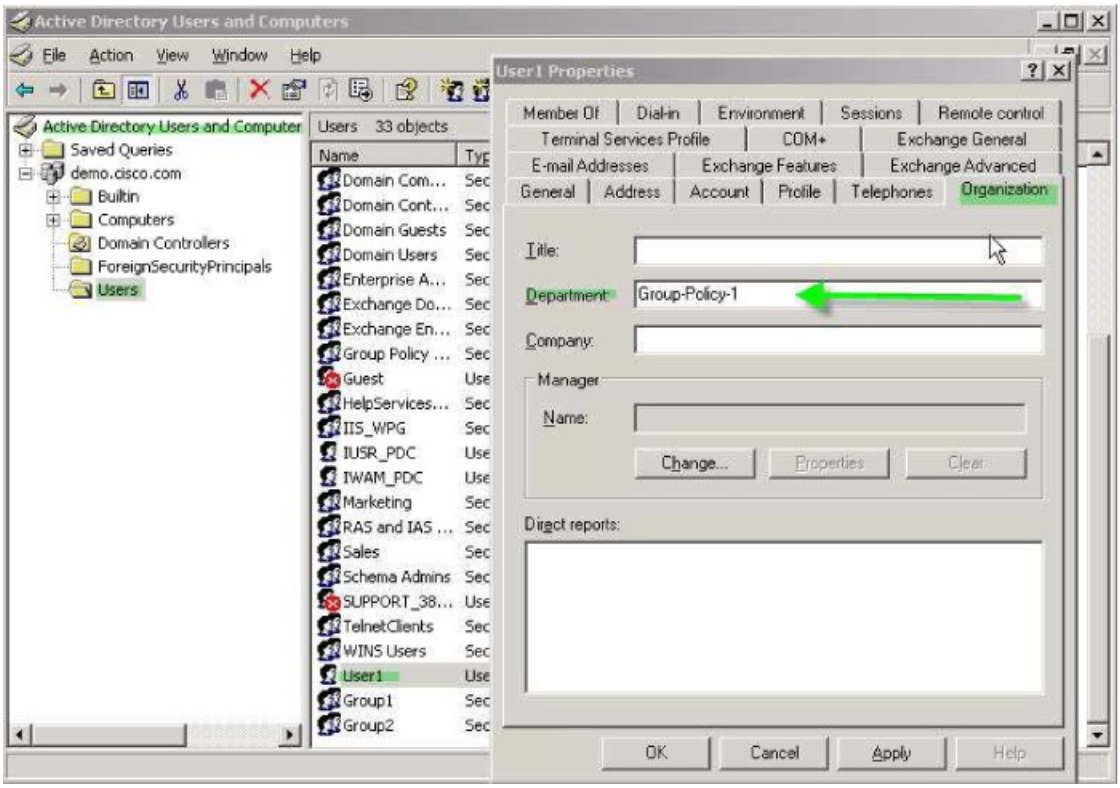
この例は、IPsec VPN クライアントやAnyConnect クライアントなど、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続経由で接続します。

LDAP ユーザーを特定のグループ ポリシーに配置するには、[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。

認証時、ASA はサーバーから [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。

手順

ステップ 1 ユーザー名を右クリックして、[Properties] ダイアログボックスの [Organization] タブを開き、[Department] フィールドに「**Group-Policy-1**」と入力します。



ステップ 2 LDAP コンフィギュレーションの属性マップを定義します。

AD 属性 Department を Cisco 属性 IETF-Radius-Class にマッピングします。

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

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ MS_LDAP のホスト 10.1.1.2 に対して AAA サーバー ホスト コンフィギュレーション モードを開始し、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 4 サーバーの [Department] フィールドに入力されているグループ ポリシー *Group-policy-1* を ASA に追加し、ユーザーに割り当てる必須ポリシー属性を設定します。

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

ステップ 5 このユーザーとして 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 6 特権 EXEC モードで **debug ldap 255** コマンドをイネーブルにして、ASA とサーバーの間の通信をモニターします。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 クライアント トンネルのスタティック IP アドレス割り当ての適用

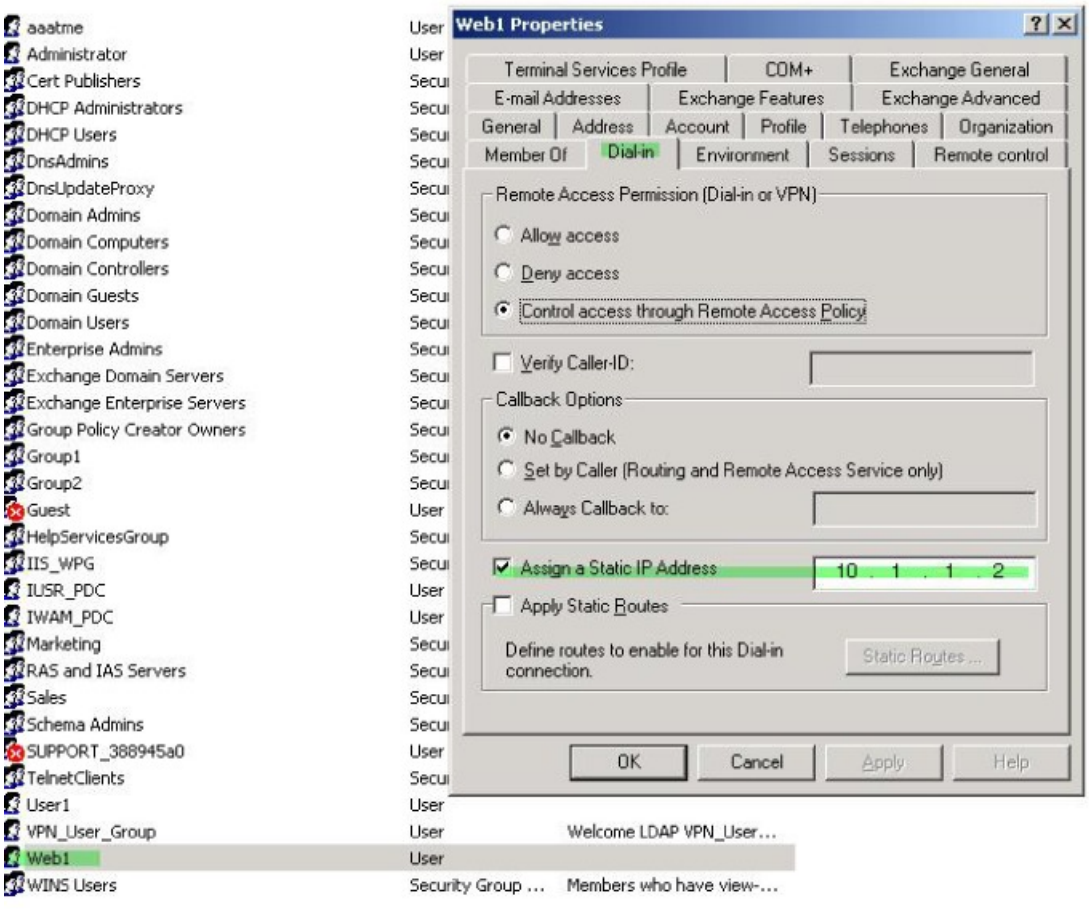
この例は、IPsec クライアントや SSL VPN クライアントなどのフルトンネル クライアントに適用されます。

スタティック AnyConnect クライアント スタティック IP 割り当てを適用するには、AnyConnect クライアントユーザー Web1 をスタティック IP アドレスを受信するように設定して、そのアドレスを AD LDAP サーバーの [ダイヤルイン（Dialin）] タブの [スタティック IP アドレスの割り当て（Assign Static IP Address）] フィールド（このフィールドで msRADIUSFramedIPAddress 属性が使用される）に入力し、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 はサーバーから msRADIUSFramedIPAddress の値を取得し、その値を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングして、User1 にスタティック アドレスを渡します。

手順

ステップ 1 ユーザー名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Assign Static IP Address] チェックボックスをオンにして、10.1.1.2 という IP アドレスを入力します。



ステップ 2 図に示す LDAP コンフィギュレーションの属性マップを作成します。

[Static Address] フィールドで使用される AD 属性 msRADIUSFramedIPAddress を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングします。

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

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ MS_LDAP のホスト 10.1.1.2 に対して AAA サーバー ホスト コンフィギュレーション モードを開始し、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 4 **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 5 ASA と AnyConnect クライアント との接続を確立します。サーバーで設定され、ASA にマッピングされた IP アドレスをユーザーが受信することを確認します。

ステップ 6 **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
```

ダイヤルイン許可または拒否アクセスの適用

この例では、ユーザーによって許可されるトンネリング プロトコルを指定する LDAP 属性マップを作成します。[Dialin] タブ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。この属性は次のビットマップ値をサポートします。

値	トンネリング プロトコル
1	PPTP
2	L2TP
4	IPsec（IKEv1）
8	L2TP/IPsec
16	クライアントレス SSL
32	SSL クライアント：AnyConnect クライアント または SSL VPN クライアント
64	IPsec（IKEv2）

[1] （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] （2）注 1 を参照。

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、ユーザーがアクセスを許可される方法を適用します。

ダイヤルイン許可アクセスまたは拒否アクセスの適用に関するその他の例については、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。

手順

ステップ 1 ユーザー名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Allow Access] オプション ボタンをクリックします。

（注）
[Control access through the Remote Access Policy] オプションを選択した場合は、サーバーから値が返されず、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 2 IPsec と AnyConnect クライアント の両方の接続を許可する一方で、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。

a) マップ tunneling_protocols を作成します。

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) [Allow Access] 設定で使用される AD 属性 msNPAllowDialin を Cisco 属性 Tunneling-Protocols にマッピングします。

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) マップ値を追加します。

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

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

a) AAA サーバー グループ MS_LDAP でホスト 10.1.1.2 の AAA サーバー ホスト コンフィギュレーション モードを開始します。

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) 作成した属性マップ tunneling_protocols を関連付けます。

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

ステップ 4 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。

クライアントレス SSL を使用して接続を試みます。ユーザーには、許可されていない接続メカニズムが接続の失敗の原因であることが通知されます。IPsec クライアントの接続は成功します。これは、属性マップに従って IPsec にトンネリング プロトコルが許可されるためです。

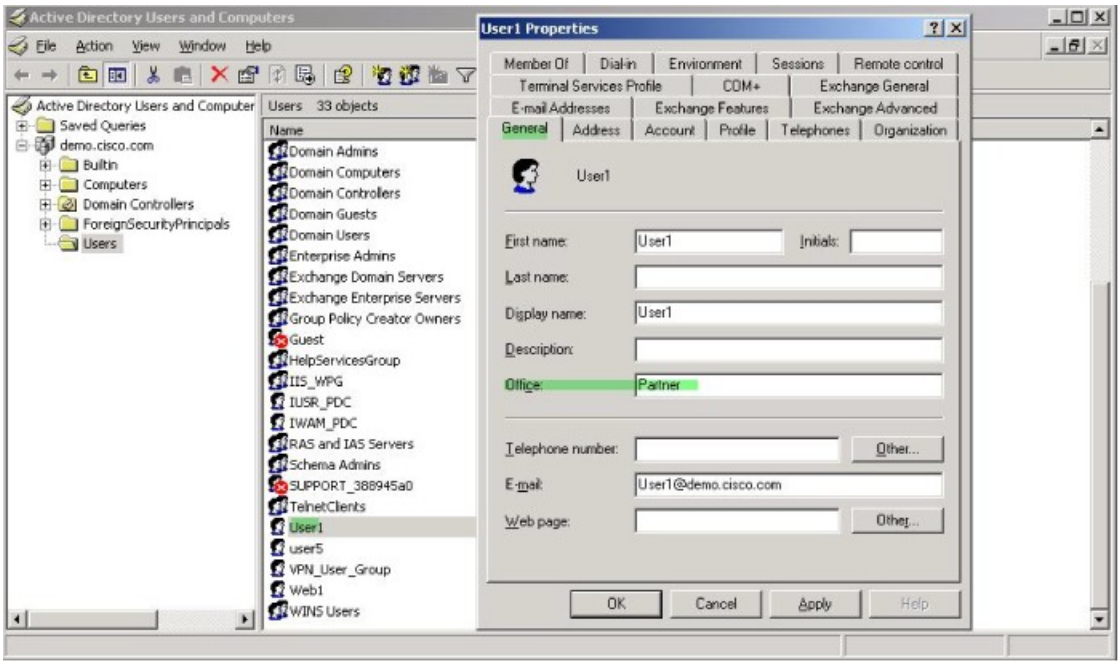
ログオン時間と Time-of-Day ルールの適用

次の例では、クライアントレス SSL ユーザー（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 サーバー上で、[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 physicalDeliveryOfficeName の値を取得して Access-Hours にマッピングします。

手順

ステップ 1 ユーザーを選択して、[Properties] を右クリックし、[General] タブを開きます。



ステップ 2 属性マップを作成します。

属性マップ access_hours を作成し、[Office] フィールドで使用される AD 属性 physicalDeliveryOfficeName を Cisco 属性 Access-Hours にマッピングします。

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

ステップ 3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ MS_LDAP のホスト 10.1.1.2 に対して AAA サーバー ホスト コンフィギュレーション モードを開始し、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 4 各値にサーバーで許可された時間範囲を設定します。

パートナー アクセス時間を月曜日から金曜日の午前 9 時から午後 5 時に設定します。

```
hostname(config)# time-range Partner
```

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。