

VPNの外部 AAA サーバの設定

- 外部 AAA サーバについて (1ページ)
- 外部 AAA サーバを使用する際のガイドライン (2ページ)
- Active Directory/LDAP VPN リモートアクセス許可の例 (2ページ)

外部 AAA サーバについて

このASAは、外部のLDAP、RADIUS、TACACS+サーバを使用して、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、ユーザ認可属性(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。ASAを設定して、次のいずれかの組み合わせ からユーザ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 (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 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。

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。

- AAAサーバ上のユーザ属性:ユーザ認証や認可が成功すると、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 データベースで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 サーバからユーザに対して 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、 サーバから返されるユーザ属性、ユーザ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。

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。

- ユーザベースの属性のポリシー適用 (3ページ)
- 特定のグループ ポリシーへの LDAP ユーザの配置 (5 ページ)
- AnyConnect トンネルのスタティック IP アドレス割り当ての適用 (6ページ)
- ダイヤルイン許可または拒否アクセスの適用(8ページ)
- ログオン時間と Time-of-Day ルールの適用 (10 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.]

ユーザベースの属性のポリシー適用

この例では、ユーザ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。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。

AD LDAP サーバ上で設定されたユーザ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。

手順

ステップ1 ユーザ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。

330370

Active Directory Users and Computers Terminal Services Profile COM+ Exchange General End Action Werk Window Help Email Addresses Exchange Features Exchange Advanced Member Of Dial-in Environment Sessions Remote control Active Directory Users Soved Queries Image Type Image Image Active Directory Users Users 31 objects Image Image Image Image Computers Domain Contru- Security Grou Domain Contru- Security Grou Image Image Image Domain Contru- Security Grou Domain Contru- Security Grou Image Image Image Image Domain Contru- Security Grou Exchange Do			User1 Properties		?
Endpoint definitions Image: Computers Image: Domain Controllers Image: Computers Image: Domain Controllers Image: Domain Controllers Image: Domain Controllers Security Group Image: Domain Controllers Security Group	Active Directory Users and Comp Ge Action View Window He → C Im & Max He Active Directory Users and Computer Go Saved Queries Saved Queries	uters p P E 2 2 10 m Users 31 objects Name Type	Terminal Services P E-mail Addresses Member Of Diakin General Address Status User1	rofile CDM+ Exchange Features Environment Account Profile	Exchange General Exchange Advanced Sessions Remote control Telephones Organization
A Members who have view-	demo.dsco.com demo.ds	DnsUpdatePr Security Gro Domain Admins Security Gro Domain Com Security Gro Domain Cont Security Gro Domain Cont Security Gro Domain Guests Security Gro Domain Guests Security Gro Domain Users Security Gro Enterprise A Security Gro Exchange Do Security Gro Group Policy Security Gro Guest User HelpServices Security Gro IUSR_PDC User IWAM_PDC User Marketing Security Gro SupPoRT_38 User SUPPORT_38 User User1 User	U Eirst name: U Eirst name: U Last name: U Display name: U Description: U Office: U Ielephone number: E-mail: Web page: U OK	User1 User1 ''Welcome to LDAP'1 Cancel	Initials: Qther Otheg

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 サーバに関連付けます。

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、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 ユーザの配置

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、Userl 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。

⊨ → 🗈 🗉 🐰 💼 🗡 🖆	T 🕅 🖪 😢 📆 🖥
Active Directory Users and Computer Saved Queries Bultin Computers Domain Controllers ForeignSecurityPrincipals Users	I Users 33 objects Member Of Dial-in Environment Sessions Remote control Name Typ Domain Com Sec Domain Comt Sec Domain Guests Sec Domain Guests Sec Domain Guests Sec Domain Guests Sec Denterprise A Sec Department Group-Policy-1 Exchange En Sec Opmany: Company: Group Policy Sec Disgrammet: Company: Group Policy Sec Disgrammet: Company: Group Policy Sec Disgrammet: Manager Marketing Sec RAS and IAS, Sec Digot reports: Sales Sec Schema Admins Sec Schema Admins Sec

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 サーバに関連付けます。

AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 に対して 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、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 とサーバの間の通信 をモニタします。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 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 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 サーバの [Dialin] タブの [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。

🔮 aaatme	User Web1 Properties
aaatme Administrator Cert Publishers DHCP Administrators DHCP Users DnsUpdateProxy Domain Admins Domain Computers Domain Controllers Domain Guests Domain Users Enterprise Admins Exchange Domain Servers Exchange Enterprise Servers Group Policy Creator Owners Group 1 Group1	User Web1 Properties ? ? ? User Terminal Services Profile CDM+ Exchange General Secu E-mail Addresses Exchange Features Exchange Advanced General Address Account Profile Telephones Organization Member Of Dial-in Environment Sessions Remote control Secu Remote Access Permission (Dial-in or VPN) Secu Callow access Secu Control access through Remote Access Policy Secu Callback Options Secu Callback Secu Secu Callback Secu Secu Callback Secu Secu Callback Secu Secu Secu Callback
Guest HelpServicesGroup IIS_WPG IUSR_PDC IWAM_PDC Marketing RAS and IAS Servers Sales Sales Science Admins	User Callback to: Secure Sec
SUPPORT_388945a0	User OK Cancel Apply Help
a reinetClients	
V User1	User
VPN_User_Group	User Welcome LDAP VPN_User
Web1	User
WINS Users	Security Group Members who have view

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 サーバに関連付けます。

AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 に対して 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、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。サーバで設定され、ASA にマッピン グされた IP アドレスをユーザ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。

Session Type: SVC Index : 31 Username : webl Assigned IP : 10.1.1.2 Public IP : 10.86.181.70 : Clientless SSL-Tunnel DTLS-Tunnel Protocol : SHA1 Encryption : RC4 AES128 Hashing 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 : 0h:01m:48s Duration 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

hostname# show vpn-sessiondb svc

この例では、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。

值	トンネリング プロトコル
1	РРТР
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 または SSL VPN クライアン ト

値	トンネリング プロトコル
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。

	Exchange General
E-mail Addresses Exchange Feature	s Exchange Advanced
aeneral Address Account Profile	Telephones Organization
Member Of Dial-in Environment	Sessions Remote control
Allow access Deny access C Deny access C Control access through Remote Access	Policy
 No Laliback C Sat by Caller (Pauling and Parata Ass 	aas Convige oplu)
C Always Callback to:	
Assign a Static IP Address	
Assign a Static IP Address Apply Static <u>R</u> outes	

- (注) [Control access through the Remote Access Policy] オプションを選択した場合は、サーバから値が返されず、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 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。
 - 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 サーバに関連付けます。
 - a) AAA サーバグループ MS_LDAP でホスト 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(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 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 ユーザを選択して、[Properties] を右クリックし、[General] タブを開きます。

Active Directory Users and Computers	User1 Properties	
	Member Of Dial-in Environment Sessions Remote control Terminal Services Profile CDM+ Exchange General	£×
Contain Collid Uter's Contain Guests Contain Guest Contain Guests Contain Guests Contain Guests Co	Eist name: User1 Initials: Digplay name: User1 Office: Patner	
VIWAM_PDC VIRAS and IAS Servers VISchema Admins SupPort.388945a0 VITehetClents VIDERI VIDERI	Ielephone number:	
VPN_User_Group Web1 WINS Users	OK Cancel Apply Help	-

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 サーバに関連付けます。

AAA サーバ グループ MS_LDAP のホスト 10.1.1.2 に対して 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、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

30379

I