

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)
- 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。

複数証明書認証の設定

AnyConnect 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。 ユーザ名の事前入力フィールドでは、2つ目の(ユーザ)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名は、常にクライアントから受信した2つ目の(ユーザ) 証明書から取得されます。

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)証明書は、事前入力および証明書由来のユーザ名のプライマリおよびセカンダリユーザ名 による解析対象です。

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 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 (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CiscoLDAP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、

330370

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。

			ser1 Properties				?
Active Directory Users and Compo File Action Yiew Window He ← →	iters p 1 🛱 🗟 😫 🌌 💆	2 章 4	Terminal Services F E-mail Addresses Member Of Dial-i General Address	Profile Exchar in Envir Account	CDM+ ige Features onment S Profile	Excha Exchar Sessions Telephones	ange General age Advanced Remote control Organization
Active Directory Users and Computer Saved Queries demo.cisco.com Demo.cisco	Users 31 objects Name Typ DinsUpdatePr Sec Domain Admins Sec Domain Com Sec Domain Cont Sec Domain Guests Sec Domain Users	pe curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou er er curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou curity Grou	User1 Eirst name: Last name: Display name: Description: Offige Lelephone number: E-mail: Web page: OK	User1	to LDAP*	Initials: [Qther Otheg
• <u> </u>	User 1 Use	er curity Group .	Members who have	e view		-	•

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。

Active Directory Users and Computer Saved Queries Computers Dultin Computers Domain Controllers ForeignSecurityPrincipals Users	Isers 33 objects Member Of Isers 33 objects Terminal See Name Type Domain Com See Domain Comt See Domain Comt See Domain Comt See Domain Guests See Group Policy See Group Policy See Group Policy See TIS_WPG See Marketing See Stales See Schema Admins See SupPoRT_38 User Wins Users See User1 User	Dial-in Environment Sessio rvices Profile COM+ isses Exchange Features Idress Account Profile Telep 	ns Remote control Exchange General Exchange Advanced hones Organization
--	---	--	---

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。

- $\left[29\right]$ 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。

330373

aaatme	User Web1 Properties
Administrator	
Cert Publishers	Secul Ferminal Services Profile UM+ Exchange General
DHCP Administrators	Secul E-mail Addresses Exchange Features Exchange Advanced
2 DHCP Users	Secul General Address Account Profile Telephones Organization
DnsAdmins	Secul Member Of Dial-in Environment Sessions Remote control
DnsUpdateProxy	Secul Bemote Access Permission (Dial-in or VPN)
Domain Admins	Secui
Domain Computers	Secul C Allow access
Domain Controllers	Secul C Denv access
Domain Guests	Secul
Domain Users	Secul
Enterprise Admins	Secul Example
Exchange Domain Servers	Secul
Exchange Enterprise Servers	Secur Callback Options
Group Policy Creator Owners	Secul C No Callback
Group1	Secul Control Date In the second second
Group2	Security Sec
Guest	User C Always Callback to:
HelpServicesGroup	Secu
IIS_WPG	Secul 🔽 Assign a Static IP Address
IUSR_PDC	User
IWAM_PDC	User Apply Static Houtes
Marketing	Secur Define routes to enable for this Dial-in
RAS and IAS Servers	Secul connection.
a Sales	Secur
Schema Admins	Secur
SUPPORT_388945a0	User OK Canaal Acat I I I I I
TelnetClients	Secul UK Cancel Eppy Help
User1	User
VPN_User_Group	User Welcome LDAP VPN_User
Web1	User
2 WINS Lisers	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。

hostname# show vpn-sessiondb svc

Session Type:	: SVC			
Username	: webl	Index	:	31
Assigned IP	: 10.1.1.2	Public IP	: 1	0.86.181.70
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 2	8 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	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
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。

			Ŀ	
Terminal Services Profile COM+		Exchange G		
E-mail Addresses Exchange Fe	atures	Exchan	ige Advanced	
Seneral Address Account Pro	ofile Tel	ephones	Organization	
MemberOf Dial-in Environmer	nt Sess	ions I	Remote control	
Remote Access Permission (Dial-in or \	/PN)			
Ueny access				
C Control access through Remote Ac	cess <u>P</u> olicy			
I Verity Caller-ID:				
Callback Options			1	
No Callback				
 No <u>Callback</u> <u>Set</u> by Caller (Routing and Remote 	Access Se	rvice only)	
 No <u>C</u>allback <u>S</u>et by Caller (Routing and Remote <u>Always Callback to:</u> 	Access Se	rvice only)	
 No Callback Set by Caller (Routing and Remote Always Callback to: 	Access Se	rvice only)	
 No Callback Set by Caller (Routing and Remote Always Callback to: Assign a Static IP Address 	Access Se	rvice only]	
 No Callback Set by Caller (Routing and Remote Always Callback to: Assign a Static IP Address Apply Static Routes 	Access Se	rvice only)	
 No Callback Set by Caller (Routing and Remote Always Callback to: Assign a Static IP Address Apply Static Routes 	Access Se	rvice only) 	

- (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。

يَ Elle Action Yiew Window Help ← → È 配 & ⊫ × ۲۲ ۲۹ ⊑ 12 12 12 12 12 12 12 12 12 12 12 12 12	Member Of Diałin Environment Sessions Remote control Terminal Services Profile CDM+ Exchange General	<u>_8×</u>
Active Directory Users and Computer Saved Queries Saved Queries Gomain Concest Saved Queries Gomain Concest Domain Computers Gomain Controllers Gomain Controllers Gomain Controllers Gomain Guests Domain Users Exchange Domain Servers Group Policy Creator Owners Guest HelpServicesGroup	E-mail Addresses Exchange Features Exchange Advanced General Address Account Profile Telephones Organization User1 Erst name: User1 Initials: Last name: User1 Display name: User1 Description: Office: Partner	
IUSR_POC WAM_PDC RAS and IAS Servers Schema Admins SupPoRT_388945a0 TeinetClents User1 User1 User5 VPN_User_Group Web1 WINS Users	Ielephone number:	·

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
```