

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。

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 (5 ページ)
- ・ダイヤルイン許可または拒否アクセスの適用 (7ページ)
- ログオン時間と Time-of-Day ルールの適用 (9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.]

330370

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。

			User1 Properties		-		?
Active Directory Users and Compo Die Action View Window He →	uters p } 🔁 😰 👻 Users 31 objects	1 🛐 🎘 🖉	Terminal Services E-mail Addresses Member Of Dial General Address	Profile Exchan in Envin Account	COM+ ge Features onment \$ Profile	Excha Excha Sessions Telephones	ange General nge Advanced Remote control Organization
Saved Queries demo.cisco.com Bultin Computers Somain Controllers ForeignSecurityPrincipals Users	Name DonsUpdatePr Domain Admins Domain Com Domain Cont Domain Cont Domain Guests Domain Users Enterprise A Exchange Do Exchange Do Guest HelpServices His_WPG USR_PDC WM_PDC Marketing RA5 and IA5 Sales Support_38 Todate(Tiente	Type Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou User Security Grou User Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou	User User Erst name: Last name: Display name: Description: Office: Ielephone number: E-mail: Web page: OK	User1	to LDAP"	Initials:	Qther Other
·	S User1	User Security Group	Members who hav	re view		1	<u>.</u>

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。

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。

330373

🛃 aaatme	User Web1 Properties
Administrator	User
Cert Publishers	Secul Terminal Services Profile COM+ Exchange General
DHCP Administrators	Secul E-mail Addresses Exchange Features Exchange Advanced
DHCP Users	Secul General Address Account Profile Telephones Organization
22 DnsAdmins	Secul Member Of Dial-in Environment Sessions Remote control
2 DnsUpdateProxy	Secul Bemote Access Permission (Dial-in or VPN)
Domain Admins	Secul
Domain Computers	Secul C Allow access
Domain Controllers	Secul C. Denu access
Domain Guests	Secul
Domain Users	Secure Control access through Remote Access Policy
Enterprise Admins	Security Sec
Exchange Domain Servers	Secul
Exchange Enterprise Servers	Secur Callback Options
Group Policy Creator Owners	Secul G No Callback
Group1	Secul Could off the state of the state
Group2	Securio
🙍 Guest	User C Always Callback to:
HelpServicesGroup	Secu
WIIS_WPG	Secul 🔽 Assign a Static IP Address
IUSR_PDC	User
IWAM_PDC	User Apply Static Boutes
Marketing	Securi Define routes to enable for this Dial-in Course Provider
RAS and IAS Servers	Secul connection.
11 Sales	Secul
Schema Admins	Secur
SUPPORT_388945a0	User OK Canaal Labora Labora
TelnetClients	Secul
🔮 User1	User
VPN_User_Group	User Welcome LDAP VPN_User
2 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	: webl	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 2	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。

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クライアントまたは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 (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。

			_	
Terminal Services Profile COM+ Exchange Ger		nge General		
E-mail Addresses	Exchange Feat	ures	Exchan	ge Advanced
General Address	Account Profi	ile Telep	hones	Organization
Member Of Dial-in	Environment	Session	ns I	Remote control
Allow access Allow access Deny access C Deny access C Control access thre Verify Caller-ID: Callback Options	ough Remote Acc	ess <u>Policy</u>		
No <u>C</u> allback				
 No <u>C</u>allback <u>S</u>et by Caller (Rou 	ting and Remote A	locess Serv	ice only)
No <u>C</u> allback <u>S</u> et by Caller (Rou Always Callback to	ting and Remote A o:	Access Serv	ice only)
No <u>C</u> allback <u>S</u> et by Caller (Rou Always Callback to Always Callback to Assign a Static IP /	ting and Remote A o: Address	Access Serv	ice only)
No <u>C</u> allback <u>S</u> et by Caller (Rou Always Callback to Always Callback to Assign a Static IP of Apply Static <u>R</u> oute	ting and Remote A o: Address		ice 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。

Gile Action View Window Help ← →	User1 Properties ? X Member Of Dialin Environment Sessions Remote control	X
Active Directory Users and Computer Saved Queries Users 33 objects Users 30 objects Domain Admins Domain Controllers Domain Controllers Domain Users Domain Users Enterprise Admins Exchange Domain Servers Exchange Enterprise Servers Group Polic Creator Owners Guest HelpServicesGroup IISR_PDC IWSR_PDC RAS and IAS Servers	Terminal Services Profile CDM+ Exchange General E-mail Addresses Exchange Features Exchange Advanced General Address Account Profile Einst name: User1 Initials: Imitials: Last name: User1 Imitials: Imitials: Display name: User1 Imitials: Imitials: Offige: Partner Imitials: Imitials: Jelephone number: Imitials: Imitials: Imitials:	-
SUPPORT 385945a0 TehetClents User1 VPN_User_Group Web1 WVINS Users	E-mait User1@demo.cisco.com Web page: Other 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。