ASA 9.Xダイナミックアクセスポリシー(DAP)の 導入

内容
 はじめに
 前提条件
 要件
 使用するコンポーネント
 背景説明
 DAPとAAA属性
 DAPとエンドポイントセキュリティ属性
 デフォルトのダイナミックアクセスポリシー
 ダイナミックアクセスポリシーの設定
 複数のダイナミックアクセスポリシーの集約
 DAP 実務
 編論
 関連情報

はじめに

このドキュメントでは、ASA 9.xダイナミックアクセスポリシー(DAP)の導入、機能、および使用 方法について説明します。

前提条件

要件

次の項目について理解しておくことをお勧めします。

- バーチャルプライベートネットワーク(VPN)ゲートウェイ
- ・ダイナミックアクセスポリシー(DAP)

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの ではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

バーチャル プライベート ネットワーク (VPN) ゲートウェイは、動的な環境で動作します。複数の変数が各VPN接続に影響を与える可能性があります。たとえば、頻繁に変更されるイントラネット構成、組織内の各ユーザーが持つさまざまな役割、リモートアクセスサイトからのログインなど、構成やセキュリティレベルが異なる場合があります。動的 VPN 環境でのユーザ認可のタスクは、静的設定のネットワークでの認可タスクよりもかなり複雑です。

ダイナミックアクセスポリシー(DAP)は、VPN環境のダイナミクスに対応する認可を設定できる 機能です。ダイナミック アクセス ポリシーは、特定のユーザ トンネルまたはユーザ セッション に関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複 数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。

たとえば、セキュリティ アプライアンスは、定義されるポリシーに基づいて、特定のセッション で特定のユーザにアクセス権を付与します。1つ以上のDAPレコードから属性を選択または集約 することにより、ユーザ認証全体を通じてDAPを生成します。DAP レコードは、リモート デバ イスのエンドポイント セキュリティ情報および認証ユーザの AAA 認可情報に基づいて選択され ます。選択された DAP レコードは、ユーザ トンネルまたはセッションに適用されます。



注:DAPポリシー選択属性が含まれているdap.xmlファイルはASAフラッシュに保存されま す。dap.xmlファイルをオフボックスでエクスポートし、編集して(XML構文を理解して いる場合)、再インポートできますが、設定に誤りがあるとASDMでDAPレコードの処理 が停止する可能性があるため、注意が必要です。この設定を操作できる CLI はありませ ん。



注: CLIを使用してdynamic-access-policy-recordアクセスパラメータを設定しようとする と、DAPにより処理が停止されることがあります。ただしASDMではこれは適切に管理さ れます。DAP ポリシーを管理する際には CLI を使用せず、常に ASDM を使用してくださ い。

DAP と AAA 属性

DAP は AAA サービスを補完し、DAP の認可属性により、AAA が提供する属性を上書きできます 。セキュリティ アプライアンスは、ユーザの AAA 認可情報に基づいて DAP レコードを選択でき ます。セキュリティ アプライアンスは、この情報に基づいて複数の DAP レコードを選択し、次 に選択したレコードを集約して DAP 認可属性を割り当てます。

AAA 属性は、Cisco AAA 属性階層から、またはセキュリティ アプライアンスが RADIUS サーバ または LDAP サーバから受信するフル セットの応答属性から指定できます(図 1 を参照)。

図 1.DAP AAA属性GUI

• • •			Add AAA Attribute	
AAA Attribute Type: Cisco				0
Group Policy:	-	٥	DfltGrpPolicy	0
Assigned IPv4 Address:	-	\$		
Assigned IPv6 Address:	-	0		
Connection Profile:	-	0	DefaultRAGroup	٥
Username:	-	0		
✓ Username2:	-	٢		
SCEP Required:	-	0	true	0
	He	lp	Cancel OK	

DAP とエンドポイント セキュリティ属性

セキュリティアプライアンスは、AAA属性に加えて、設定したポスチャ評価方式を使用してエンドポイントセキュリティ属性を取得することもできます。これには、図2に示すように、Basic Host Scan、Secure Desktop、Standard/Advanced Endpoint Assessment、NACが含まれます。 Endpoint Assessment属性が取得され、ユーザ認証の前にセキュリティアプライアンスに送信されます。ただし DAP レコード全体を含む AAA 属性は、ユーザ認証中に検証されます。

図 2:エンドポイント属性 GUI

• • •	Add Endpoint Attribute	
Endpoint Attribute Type:	Application	
	✓ Application	
	AnyConnect	
Client Type: - 🖸	File ess	
	Device	
	NAC	
	Operating System	
	Personal Firewall	
	Multiple Certificate Authentication	
	Help Cancel OK	

デフォルトのダイナミック アクセス ポリシー

DAPの導入と実装の前は、特定のユーザトンネルまたはセッションに関連付けられたアクセスポリシーの属性と値のペアは、ASAでローカルに(つまり、トンネルグループとグループポリシーで)定義されたか、外部のAAAサーバを介してマッピングされていました。

デフォルトでは常に DAP が適用されます。たとえば、DAPを明示的に適用せずに、トンネルグ ループ、グループポリシー、およびAAAを介してアクセスコントロールを適用すると、この動作 が引き続き発生する可能性があります。従来の動作の場合は DAP 機能(デフォルト DAP レコー ド DfltAccessPolicy を含む)の設定変更は不要です(図 3 を参照)。

図 3: デフォルトのダイナミック アクセス ポリシー

•	Edit Dynamic Access Policy
Policy Name: Df	ItAccessPolicy
Description:	
Access/Author	rization Policy Attributes
Configure ac the AAA syst attributes, an	cess/authorization attributes for this policy. Attribute values specified here will override those values obtained fro em and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AA d group-policy hierarchy attributes (those that are not specified in DAP).
Action	Network ACL Filters (client) Webtype ACL Filters (clientless) Functions Port Forwarding Lists
Action:	O Continue O Quarantine O Terminate O
Specify th	he message that will be displayed when this record is selected.
User Mes	sage:
	Help Cancel OK

ただし、DAPレコードのいずれかのデフォルト値(たとえば、DfltAccessPolicyのAction:パラメー タ)がデフォルト値のTerminateから変更され、追加のDAPレコードが設定されていない場合でも 、認証されたユーザはデフォルトでDfltAccessPolicy DAPレコードと照合してVPNアクセスを拒 否できます。

その結果、VPN接続を許可し、認証されたユーザがアクセスを許可されるネットワークリソース を定義するために、1つ以上のDAPレコードを作成して設定する必要があります。したがって、 DAPが設定されている場合は、レガシーポリシーの適用よりも優先されます。

ダイナミックアクセスポリシーの設定

DAPを使用してユーザがアクセスできるネットワークリソースを定義する場合、考慮すべきパラ メータが数多くあります。たとえば、接続エンドポイントが管理対象、管理対象外、非信頼のい ずれの環境からのものかを特定する場合は、接続エンドポイントを特定するために必要な選択基 準を決定し、エンドポイント評価とAAAクレデンシャルに基づいて、接続ユーザがアクセスを許 可されているネットワークリソースを決定します。これを実現するには、まず図4に示すように、 DAPの機能を理解する必要があります。

図 4:ダイナミック アクセス ポリシー

		Add Dynamic A	ccess Policy		
licy Name:					
escription:				ACL Pr	iority: 0
alastian Critaria					
Define the AAA and en below and every endpo the logical expression	dpoint attributes used to select this access bint attribute has been satisfied. These attri text.	policy. A policy i butes can be crea	is used when a user's ted using the tables i	authorization attributes match the below and/or by expanding the Adv	AAA attribute criteria anced option to speci
User has ANY of the	e following AAA Attributes values 😌		and the following	g endpoint attributes are satisfied.	
AAA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
		Edit			Edit
		Delete			Delete
					Logical Op.
Advanced					
Advanced Access/Authorization Po Configure access/auth group-policy hierarchy that are not specified i	olicy Attributes porization attributes for this policy. Attribut y. The resulting VPN authorization policy is in DAP).	e values specified an aggregation o	f here will override th f DAP attributes, AAA	ose values obtained from the AAA s attributes, and group-policy hierar	ystem and the chy attributes (those
Advanced Access/Authorization Pc Configure access/auth group-policy hierarchy that are not specified i Action Networ	olicy Attributes orization attributes for this policy. Attribut y. The resulting VPN authorization policy is in DAP). rk ACL Filters (client) Webtype ACL Filte	e values specified an aggregation o rs (clientless)	I here will override th f DAP attributes, AAA Functions Port I	ose values obtained from the AAA s attributes, and group-policy hierar Forwarding Lists Bookmarks	ystem and the chy attributes (those Access Method

DAP レコードを設定する際には主に次の2つの点について検討する必要があります。

- 選択基準([Advanced] のオプションを含む)
- アクセス ポリシー属性

[Selection Criteria] セクションでは、特定の DAP レコードを選択するために使用される AAA 属 性とエンドポイント属性を管理者が設定します。DAP レコードが使用されるのは、ユーザの認可 属性が AAA 属性基準に一致しており、すべてのエンドポイント属性の基準が満たされている場合 です。

たとえば、AAA属性タイプLDAP(Active Directory)を選択し、属性名にmemberOf、値文字列に Contractorsを指定した場合(図5aを参照)、AAA属性基準を満たすには、認証を行うユーザが Active DirectoryグループContractorsのメンバーである必要があります。

認証ユーザは、AAA属性基準を満たすだけでなく、エンドポイント属性基準も満たす必要があり ます。たとえば、管理者が接続エンドポイントのポスチャを判別するように設定し、そのポスチ ャ評価に基づいて、この評価情報を図5bに示すエンドポイント属性の選択基準として使用できま す。

図 5a. AAA 属性基準

• • •		/	dd AAA Attribu	ute	
AAA Attribute	e Type:	DAP			8
Attribute ID:	memberOf				
Value:	- 3	Contractors			Get AD Groups
		Help	Cancel	ОК	

図 5b. エンドポイント属性基準

• • •	Add Endpoint Attribute
Endpoint Attribute Type:	NAC 3
Posture Status: -	
	Help Cancel OK

図 6.AAA 属性とエンドポイント属性の基準への一致

Policy Name:		
lescription:	ACL Priority: 0	
Define the AAA and endpoint attributes used to select this access policy. A policy is used when below and every endpoint attribute has been satisfied. These attributes can be created using the the logical expression text. User has ANY of the following AAA Attributes values.	a user's authorization attributes match the AAA attrib e tables below and/or by expanding the Advanced opt naion endocint attributes are satisfied.	bute critteria ion to specif
Interest D	Name/Operation/Value	AM
AAA Alterityte Operation/Yalue AAA		
Add American Contractors Add Add Iglap, memb a: Contractors Iddx Iddx	statua - Contractora	6ak
Add American Contractors Add Rec	Insta - Contractors	Edit Delete

AAA 属性とエンドポイント属性を作成するには、図 6 に示されているテーブルを使用するか、または図 7 に示すように [Advanced] オプションを展開して論理式を指定します。現在、論理式は EVAL関数で構成されています。たとえば、AAAやエンドポイント選択論理操作を表すEVAL (endpoint.av.McAfeeAV.exists, "EQ", "true", "string")やEVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string")です。

論理式は、前述のようにAAAおよびエンドポイント属性領域で可能な選択条件とは異なる選択基 準を追加する必要がある場合に便利です。たとえば、指定された基準のいずれか、またはすべて を満たす、あるいはすべてを満たさないAAA属性を使用するようにセキュリティアプライアンス を設定できますが、エンドポイント属性は累積されるため、すべてを満たす必要があります。セ キュリティ アプライアンスが特定のエンドポイント属性を使用するようにするには、DAP レコ ードの [Advanced] セクションで該当する論理式を作成する必要があります。

図 7拡張属性を作成するための論理式 GUI

Advanced AND OR Logical Expressions: ((EVAL (endpoint.av.McAfeeAV.exists, "EQ", "true", "string") and EVAL (endpoint.av.McAfeeAV.description, "EQ", "McAfee VirusScan Enterprise", "string"))) Guide

図 8 に示す [Access Policy Attributes] セクションでは、管理者が特定の DAP レコードの VPN ア クセス属性を設定します。ユーザ認可属性がAAA、エンドポイント、論理式の基準に一致する場 合、このセクションで設定したアクセスポリシー属性値を適用できます。ここで指定する属性値 は、既存のユーザ、グループ、トンネルグループ、およびデフォルトグループレコードの値など 、AAAシステムから取得した値を上書きできます。

DAP レコードには、設定可能な属性値がいくつかあります。これらの値は、図8 ~ 14に示すタブ に分類されます。

図 8.[Action]:特定の接続またはセッションに適用される特別な処理を指定します。

Access/Authoriza Configure acces hierarchy. The r in DAP).	ation Policy Attributes ss/authorization attributes for the esulting VPN authorization polici	nis policy. Attribute values specified he y is an aggregation of DAP attributes,	ere will override thos AAA attributes, and	se values obtained fror I group-policy hierarch	m the AAA system ly attributes (those	and the group-policy that are not specifie
Action	Network ACL Filters (client)	Webtype ACL Filters (clientless)	Functions Po	ort Forwarding Lists	Bookmarks	Access Method
Action: O	Continue Quarantine message that will be displayed t	Terminate o				
User Messa	ge:					

- [Continue]:(デフォルト)クリックするとセッションにアクセスポリシー属性が適用されます。
- [Terminate]: クリックするとセッションが終了します。
- [User Message]: この DAP レコードが選択されるときに、ポータルページに表示するテキ スト メッセージを入力します。最大 128 文字を入力できます。ユーザ メッセージは、黄色 のオーブとして表示されます。ユーザがログインすると、メッセージは 3 回点滅してから 静止します。数件の DAP レコードが選択され、それぞれにユーザ メッセージがある場合は 、ユーザ メッセージがすべて表示されます。このようなメッセージには、URL やその他の 埋め込みテキストを含めることができます。この場合は、正しい HTML タグを使用する必 要があります。

図 9.Network ACL Filtersタブ:このDAPレコードに適用するネットワークACLを選択して設定で きます。DAP の ACL には許可ルールまたは拒否ルールのいずれかを含めることができますが、 両方を含めることはできません。ACL に許可ルールと拒否ルールの両方が含まれる場合は、セキ ュリティ アプライアンスで ACL 設定が拒否されます。

-Access/Authoriza Configure acces hierarchy. The r in DAP).	ation Policy Attributes ss/authorization attributes for tl resulting VPN authorization polic	his policy. Attribute values s cy is an aggregation of DAP	specified here will o attributes, AAA attr	override those values obtained from the AAA system and the group-po tributes, and group-policy hierarchy attributes (those that are not spec	olicy ifie
Action	Network ACL Filters (client)	Webtype ACL Filters (clie	ntless) Functio	ions Port Forwarding Lists Bookmarks Access Method	
				Network ACLs	
any		0	Add>>		
		Manage	Delete		

- Network ACLドロップダウンボックスは、このDAPレコードに追加するためにすでに設定されているネットワークACLです。すべての許可ルールまたは拒否ルールを持つACLのみが適格で、これらがここに表示される唯一のACLです。
- [Manage]: ネットワーク ACL を追加、編集、および削除します。
- ネットワークACL: このDAPレコードのネットワークACLのリスト。
- ・ [Add]:ドロップダウン ボックスから選択したネットワーク ACL を右側の [Network ACLs] リストに追加します。
- ・ [Delete] : [Network ACLs] リストから、選択したネットワーク ACL を削除します。DAP レ

コードまたはその他のレコードに割り当てられている ACL は削除できません。

図 10Web-Type ACL Filtersタブ:このDAPレコードに適用するWeb-type ACLを選択して設定で きます。DAP の ACL には、許可ルールだけまたは拒否ルールだけを含めることができます。 ACL に許可ルールと拒否ルールの両方が含まれる場合は、セキュリティ アプライアンスで ACL 設定が拒否されます。

- Acc C hi	ess/Authorization Policy Attributes onfigure access/authorization attributes for th ierarchy. The resulting VPN authorization polic 1 DAP).	nis policy. Attribute values specified y is an aggregation of DAP attribute	here will override es, AAA attributes	those values obtained fi , and group-policy hierar	rom the AAA syster rchy attributes (tho	n and the group-policy se that are not specifie
	Action Network ACL Filters (client)	Webtype ACL Filters (clientless)	Functions	Port Forwarding Lists	Bookmarks	Access Method
		bbA	Web	otype ACLs		
		Manage Dele	ete			

- [Web-Type ACL] ドロップダウン ボックス:この DAP レコードに追加する、すでに設定済 みの Web-type ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL だけが適格とされ、これらの適格な ACL だけがここに表示されます。
- Manage...:Web-type ACLを追加、編集、および削除します。
- [Web-Type ACL] リスト: この DAP レコードの Web-type ACL を表示します。
- [Add] : ドロップダウン ボックスから選択した Web-type ACL を右側の [Web-Type ACLs] リストに追加します。
- [Delete] : [Web-Type ACLs] リストから Web-type ACL を削除します。DAP レコードまたは その他のレコードに割り当てられている ACL は削除できません。

図 11[Functions]タブ:このタブでは、DAPレコードのファイルサーバエントリとブラウジング、 HTTPプロキシ、およびURLエントリを設定できます。

Acces Cor hier in D	ss/Authorization Polic ifigure access/authori rarchy. The resulting V DAP).	Attributes ation attributes for this policy. Att N authorization policy is an aggre	tribute values specified h gation of DAP attributes,	ere will override AAA attributes,	those values obtained fro and group-policy hierarc	om the AAA system hy attributes (those	and the group-policy that are not specifie
	Action Network	ACL Filters (client) Webtype A	CL Filters (clientless)	Functions	Port Forwarding Lists	Bookmarks	Access Method
	File Server Browsing:	🔾 Unchanged 🔷 Enable 🔷 Di	isable				
	File Server Entry:	🔾 Unchanged 📀 Enable 📀 Di	isable				
	HTTP Proxy:	🔾 Unchanged 📀 Enable 🔿 Di	isable 🔿 Auto-start				
	URL Entry:	🔾 Unchanged 📀 Enable 🔿 Di	isable				

- [File Server Browsing]:ファイル サーバまたは共有機能の CIFS ブラウジングをイネーブル またはディセーブルにします。
- [File Server Entry]: ポータル ページでユーザがファイル サーバのパスおよび名前を入力で きるようにするか、または入力するのを禁止します。イネーブルになっている場合、ポータ ルページにファイル サーバ エントリのドローアが配置されます。ユーザは Windows ファ イルのパス名を直接入力できます。ユーザは、ファイルをダウンロード、編集、削除、名前

変更、および移動できます。また、ファイルとフォルダを追加することもできます。該当す る Windows サーバでユーザ アクセスに対して共有を設定する必要もあります。ネットワー ク要件によっては、ファイルにアクセスする前にユーザの認証が必要になる場合があります 。

- [HTTP Proxy]: クライアントへの HTTP アプレット プロキシの転送に影響します。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー(Java、ActiveX、Flash など)に対して有用です。セキュリティアプライアンスの継続的な使用を保証しながら、マングリング/書き換えプロセスをバイパスします。転送されたプロキシは、自動的にブラウザの古いプロキシ設定を変更して、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Javaなど、ほとんどすべてのクライアント側テクノロジーをサポートしています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
- [URL Entry]:ポータルページでユーザが HTTP/HTTPS URL を入力できるようにするか、 または入力できないようにします。この機能がイネーブルになっている場合、ユーザは URL 入力ボックスに Web アドレスを入力できます。また、クライアントレス SSL VPN を 使用して、これらの Web サイトにアクセスできます。
- ・ [Unchanged] : (デフォルト)このセッションに適用されるグループ ポリシーの値を使用します。
- [Enable]/[Disable]:機能をイネーブルまたはディセーブルにします。
- [Auto-start]: HTTP プロキシをイネーブルにし、DAP レコードにより、これらの機能に関 連付けられたアプレットを自動的に起動させます。

図 12.Port Forwarding Listsタブ:このタブでは、ユーザセッションのポート転送リストを選択お よび設定できます。

Access/Authorization Policy Attributes				
Configure access/authorization attributes for this policy. Attribute values s hierarchy. The resulting VPN authorization policy is an aggregation of DAP	pecified here will overrid attributes, AAA attributes	e those values obtained fro s, and group-policy hierarc	m the AAA system and the group-po hy attributes (those that are not spec	ifie
in DAP).				
Action Network ACL Filters (client) Webtype ACL Filters (clie	ntless) Functions	Port Forwarding Lists	Bookmarks Access Method	
Port Forwarding: 🗿 Unchanged 🔷 Enable 🔷 Disable 🔷 Auto	o-start			
Port Forwarding List:				1
	Add>>			
New	Delete			

- [Port Forwarding]: この DAP レコードに適用されるポート転送リストのオプションを選択 します。このフィールドのその他の属性は、[Port Forwarding] を [Enable] または [Autostart] に設定した場合にだけイネーブルになります。
- [Unchanged]: このセッションに適用されるグループポリシーの値を使用します。
- [Enable]/[Disable]:ポート転送をイネーブルまたはディセーブルにします。
- [Auto-start]:ポート転送をイネーブルにし、DAP レコードに、そのポート転送リストに関連付けられたポート転送アプレットを自動的に起動させます。

- [Port Forwarding List] ドロップダウンボックス:DAP レコードに追加する、すでに設定済みのポート転送リストを選択します。
- [New]:新しいポート転送リストを設定します。
- [Port Forwarding Lists]: DAP レコードのポート転送リストを表示します。
- [Add]:ドロップダウン ボックスから選択したポート転送リストを右側のポート転送リスト に追加します。
- 削除:選択したポートフォワーディングリストをポートフォワーディングリストから削除します。DAP レコードまたはその他のレコードに割り当てられている ACL は削除できません。

図 13.[ブックマーク]タブ:ユーザー・セッションのブックマーク/URLリストを選択および構成で きます。

ccess/Authorization Policy Attributes Configure access/authorization attributes for this policy. Attribute values specif hierarchy. The resulting VPN authorization policy is an aggregation of DAP attrib in DAP).	fied here will overri outes, AAA attribute	de those values obtained fro es, and group-policy hierarcl	m the AAA syster ny attributes (tho:	n and the group-po se that are not spec	licy ified
Action Network ACL Filters (client) Webtype ACL Filters (clientles	s) Functions	Port Forwarding Lists	Bookmarks	Access Method	
Enable bookmarks	Add>>				
Manage	Delete				

- ブックマークを使用可能にする:クリックすると使用可能になります。このボックスが選択 されていない場合、接続のポータル・ページにはブックマーク・リストが表示されません
- [Manage]: ブックマーク リストを追加、インポート、エクスポート、削除します。
- ・ [Bookmarks Lists](ドロップダウン):DAP レコードのブックマーク リストを表示します。
- [Add]:ドロップダウン ボックスから選択したブックマーク リストを右側のブックマーク リスト ボックスに追加します。
- [Delete]: ブックマーク リスト ボックスから選択したブックマークリストを削除します。セキュリティ アプライアンスからブックマーク リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。

図 14.Methodタブ:許可するリモートアクセスのタイプを設定できます。

Access/Authorization	n Policy Attributes authorization attributes for this policy. Attribute values specified here will overr	ide those values of	tained from the AA	A system and the group-policy
hierarchy. The result in DAP).	Iting VPN authorization policy is an aggregation of DAP attributes, AAA attribut	es, and group-poli	cy hierarchy attribu	ites (those that are not specified
◀ Webtype AC	CL Filters (clientless) Functions Port Forwarding Lists Bookmarks	Access Method	AnyConnect	AnyConnect Custom Attributes
Access Method	: 🗿 Unchanged			
	AnyConnect Client			
	🔿 Web-Portal			
	Both-default-Web-Portal			
	Both-default-AnyConnect Client			

- Unchanged:セッションのグループポリシーで設定されている現在のリモートアクセス方式で続行します。
- [AnyConnect Client]: Cisco AnyConnect VPN Client を使用して接続します。
- Webポータル:クライアントレスVPNに接続します。
- ・ [Both-default-Web-Portal] : クライアントレスまたは AnyConnect Client のいずれかによっ て接続します。デフォルトはクライアントレスです。
- ・ [Both-default-AnyConnect Client]: クライアントレスまたは AnyConnect Client のいずれか によって接続します。デフォルトは AnyConnect です。

前述のように、DAPレコードには限られたデフォルト属性値があります。これらの値は、変更さ れている場合にだけ、現在のAAA、ユーザ、グループ、トンネルグループ、およびデフォルトグ ループレコードよりも優先されます。スプリットトンネリングリスト、バナー、スマートトンネ ル、ポータルカスタマイズなど、DAPの範囲外の属性値が追加で必要な場合は、AAA、ユーザ、 グループ、トンネルグループ、およびデフォルトグループレコードを使用して適用する必要があ ります。この場合、これらの特定の属性値はDAPを補完し、上書きすることはできません。した がって、ユーザはすべてのレコードにわたって属性値の累積セットを取得します。

複数のダイナミックアクセスポリシーの集約

管理者は複数の DAP レコードを設定することで複数の変数に対応できます。その結果、認証を 行うユーザは、複数のDAPレコードのAAA属性とエンドポイント属性の基準を満たすことができ ます。その結果、アクセスポリシー属性は、これらのポリシー全体で一貫しているか、または競 合している可能性があります。この場合、認可ユーザは、一致したすべてのDAPレコードの累積 結果を取得できます。

これには、認証、認可、ユーザ、グループ、トンネル グループ、およびデフォルト グループ レ コードによって適用される固有の属性値も含まれます。アクセス ポリシー属性が累積された結果 として、ダイナミック アクセス ポリシーが作成されます。組み合わされたアクセスポリシー属性 の例を次の表に示します。これらの例には、3 つの DAP レコードを組み合わせた結果が示されて います。

表1に示すアクション属性の値は Terminate と Continue です。集約属性値は、選択されている いずれかのDAPレコードでTerminate値が設定されている場合はTerminateとなり、選択されてい るすべてのDAPレコードでContinue値が設定されている場合はContinueとなります。

表 1.アクション属性

属性名	DAP#1	DAP#2	DAP#3	DAP
Action(例 1)	continue	continue	continue	continue
Action(例 2)	終了	continue	continue	terminate

表2に、ストリング値を含むユーザメッセージ属性を示します。集約属性値は、選択された DAPレコードの属性値をリンクして作成された改行(16進数値0x0A)区切りの文字列にすること ができます。連結ストリングでの属性値の順序は特に重要ではありません。

表2ユーザ メッセージ属性

属性名	DAP#1	DAP#2	DAP#3	DAP
user-message	the quick	brown fox	Jumps over	the quick <lf>brown fox<lf>jumps over</lf></lf>

表3に示すクライアントレス機能をイネーブルにする属性(関数)には、Auto-start、Enable、またはDisableの値が含まれています。選択されているいずれかのDAPレコードでAuto-Start値が設定されている場合、集約属性値はAuto-startになる可能性があります。

選択されているどのDAPレコードでもAuto-start値が設定されておらず、少なくとも1つのDAPレ コードでEnable値が設定されている場合は、集約属性値をEnabledにできます。

選択されているどのDAPレコードにもAuto-start値またはEnable 値が設定されておらず、選択さ れているDAPレコードの少なくとも1つに「disable」値が設定されている場合は、集約属性値を 無効にできます。

表3クライアントレス機能イネーブル属性(関数)

属性名	DAP#1	DAP#2	DAP#3	DAP
port-forward	enable	無効化		enable
file-browsing	無効化	enable	無効化	enable
file-entry			無効化	無効化
http-proxy	無効化	auto-start	無効化	auto-start
url-entry	無効化		enable	enable

表4に、URLリスト属性とport-forward属性を示します。これらの属性には、文字列またはカンマ で区切られた文字列のいずれかの値が含まれます。集約属性値は、選択したDAPレコードの属性 値をリンクするときに作成される、カンマで区切られた文字列にすることができます。結合スト リング内の重複する属性値は削除できます。結合ストリング内での属性値の順序は重要ではあり ません。

表4 URL リスト属性とポート転送リスト属性

属性名 DAP#1 DAP#3 DAP#3 DAP

url-list	а	b,c	а	a,b,c
port-forward		d,e	e,f	d,e,f

Access Method属性では、SSL VPN接続に許可されるクライアントアクセス方式を指定します。 クライアントアクセス方式には、AnyConnectクライアントアクセスのみ、Webポータルアクセス のみ、AnyConnectクライアントまたはWebポータルアクセス(デフォルトはWebポータルアクセ ス)、AnyConnectクライアントまたはWebポータルアクセス(デフォルトはAnyConnectクライ アントアクセス)があります。集約属性値の要約を表 5 に示します。

表5アクセス方式属性

AnyConnect Client	Web ポー タル	Both-default- Web- Portal	Both-default- AnyConnect Client	集約結果
			x	Both-default-AnyConnect Client
		x		両方 – デフォルト – Web – ポータル
		x	x	両方 – デフォルト – Web – ポータル
	Х			Web-Portal
	x		x	Both-default-AnyConnect Client
	x	x		両方 – デフォルト – Web – ポータル
	x	x	x	両方 – デフォルト – Web – ポータル
X				AnyConnect Client
x			x	Both-default-AnyConnect Client
x		x		両方 – デフォルト – Web – ポータル
x		x	x	両方 – デフォルト – Web – ポータル
x	x			両方 – デフォルト – Web – ポータル
x	x		x	Both-default-AnyConnect Client
x	x	x		両方 – デフォルト – Web – ポータル
x	x	x	x	両方 – デフォルト – Web – ポータル

ネットワーク(ファイアウォール)属性とWeb-Type(クライアントレス)ACLフィルタ属性を組 み合わせる場合、DAPプライオリティとDAP ACLの2つの主要コンポーネントを考慮する必要が あります。

図15に示すPriorityトリビュートは集約されません。セキュリティ アプライアンスは、複数の DAP レコードからネットワーク ACL と Web-type ACL を集約するときに、この値を使用してア クセス リストを論理的に順序付けします。セキュリティアプライアンスは、プライオリティ番号 の高い順にレコードを並べます。プライオリティ番号の低い順がテーブルの一番下に表示されま す。たとえば、値が4の DAP レコードは、値が2のレコードよりもプライオリティが高くなり ます。プライオリティは、手動での並べ替えはできません。

図 15.[Priority]: DAP レコードのプライオリティを表示します。

• • •	Add Dynamic Access Policy		
Policy Name:			
Description:	ACL Priority: 0		

- [Policy Name]: DAP レコードの名前を表示します。
- [Description]: DAP レコードの目的を説明します。

DAP ACL属性は、厳密なAllow-List ACLモデルまたはBlock-List ACLモデルのいずれかに準拠する アクセスリストのみをサポートします。Allow-List ACLモデルでは、アクセスリストエントリによ って、指定されたネットワークまたはホストへのアクセスを「許可」するルールが指定されます 。ブロックリスト ACLモードでは、アクセスリストエントリによって、指定されたネットワーク またはホストへのアクセスを拒否するルールが指定されます。非準拠アクセスリストには、許可 ルールと拒否ルールが混在したアクセスリストエントリが含まれています。DAPレコードに対し て非準拠アクセスリストが設定されている場合、管理者がレコードを追加しようとすると、設定 エラーとして拒否される可能性があります。準拠するアクセスリストがDAPレコードに割り当て られている場合、準拠の特性を変更するアクセスリストの変更は、設定エラーとして拒否される 可能性があります。

図 16.DAP ACL: このDAPレコードに適用するネットワークACLを選択して設定できます。

Access/Authoriz Configure acce hierarchy. The in DAP).	zation Policy Attributes ess/authorization attributes for resulting VPN authorization pol	this policy. Attribute values icy is an aggregation of DAP	specified here will o attributes, AAA attr	verride those values obtained fro ibutes, and group-policy hierarc	m the AAA system hy attributes (those	and the group-poli that are not specifi
Action	Network ACL Filters (client)	Webtype ACL Filters (clie	entless) Functio	ons Port Forwarding Lists	Bookmarks	Access Method
any		C Manage	Add>> Delete	Network ACLs any		

複数のDAPレコードが選択されると、ネットワーク(ファイアウォール)ACLに指定されている アクセスリスト属性が集約され、DAPファイアウォールACLのダイナミックアクセスリストが作 成されます。同様に、Web-Type(クライアントレス)ACLに指定されているアクセスリスト属性 が集約され、DAPクライアントレスACLのダイナミックアクセスリストが作成されます。次の例 では、ダイナミックDAPファイアウォールアクセスリストがどのように特別に作成されるかにつ いて説明します。ただし、ダイナミックDAPクライアントレスアクセスリスト(ACL)も同じプロ セスを実行できます。

まず、ASAは表6に示すように、DAP Network-ACLの一意の名前を動的に作成します。

表 6 ダイナミック DAP Network-ACL 名

DAP Network-ACL 名
DAP-Network-ACL-X(Xは、一意性を保証するために増分できる整数)

2番目に、ASAは表7に示すように、選択されたDAPレコードからNetwork-ACL属性を取得します 。

表 7 ネットワーク ACL

選択される DAP レコード	Priority	Network-ACL	Network-ACL エントリ
DAP 1	1	101 および 102	ACL 101 には 4 つの拒否ルールがあり、ACL 102 には 4 つの許可ルールがある
DAP 2	2	201 および 202	ACL 201 には 3 つの許可ルールがあり、ACL 202 には 3 つの拒否ルールがある
DAP 3	2	101 および 102	ACL 101 には 4 つの拒否ルールがあり、ACL 102 には 4 つの許可ルールがある

3番目に、ASAはDAPレコードのプライオリティ番号によってNetwork-ACLを並べ替え、次に、選択した2つ以上のDAPレコードのプライオリティ値が同じ場合はBlock-List によって並べ替えます。その後、ASAは表8に示すように、各Network-ACLからNetwork-ACLエントリを取得できます。

表 8 DAP レコードの Priority

Network-ACL	Priority	ホワイト/ブラック アクセス リスト モデル	Network-ACL エントリ
101	2	ブラックリスト	4 つの拒否ルール(DDDD)
202	2	ブラックリスト	3 つの拒否ルール(DDD)
102	2	ホワイトリスト	4 つの許可ルール(PPPP)
202	2	ホワイトリスト	3 つの許可ルール(PPP)
101	1	ブラックリスト	4 つの拒否ルール(DDDD)
102	1	ホワイトリスト	4 つの許可ルール(PPPP)

最後に、ASAはダイナミックに生成されたNetwork-ACLにNetwork-ACLエントリをマージし、ダイナミックNetwork-ACLの名前を、適用する新しいNetwork-ACLとして返します(表9を参照)。

表9ダイナミック DAP Network-ACL

DAP Network-ACL 名 Network-ACL エントリ

DAP 実装

管理者がDAPの実装を検討する必要がある理由は数多くあります。このような理由としては、エ ンドポイントのポスチャ評価を適用する場合や、認可対象ユーザがネットワーク リソースにアク セスするときにより細かな AAA 属性またはポリシー属性を検討する場合などがあります。次の例 では、DAPとそのコンポーネントを設定して、接続エンドポイントを特定し、さまざまなネット ワークリソースへのユーザアクセスを許可できます。

テストケース:クライアントから次のVPNアクセス要件を持つ概念実証が要求されました。

- 従業員のエンドポイントを検出し、管理対象または管理対象外として識別する機能。—エンドポイントが管理対象(ワーク PC)と識別されたが、ポスチャ要件を満たしていない場合、そのエンドポイントのアクセスを拒否する必要があります。一方、従業員のエンドポイントが管理対象外(ホーム PC)と識別された場合、そのエンドポイントに対してクライアントレスアクセスを付与する必要があります。
- クライアントレス接続の終了時にセッションの cookie とキャッシュのクリーンアップを実行できること。
- McAfee AntiVirusなど、管理対象の従業員エンドポイントで実行中のアプリケーションを検 出して適用する機能。アプリケーションが存在しない場合、エンドポイントのアクセスを拒 否する必要があります。
- AAA認証を使用して、認可されたユーザがアクセスする必要があるネットワークリソースを 判別する機能。セキュリティ アプライアンスではネイティブ MS LDAP 認証と複数の LDAP グループ メンバーシップ ロールがサポートされている必要があります。
- クライアント/ネットワークベースの接続を介して接続したときに、ネットワークリソース (ネットワークFAXやプリンタなど)へのローカルLANアクセスを許可する機能。
- 契約作業員にゲスト アクセスを認可できること。契約作業員とそのエンドポイントにはクライアントレスアクセスが必要であり、アプリケーションへのポータルアクセスは従業員アクセスに比べて制限が必要です。

この例では、クライアントのVPNアクセス要件を満たすために、一連の設定手順を実行できます 。必要な設定手順はあっても、DAPに直接関連していない設定がある場合と、DAPに直接関連し ている設定がある場合があります。ASAは非常に動的で、多くのネットワーク環境に適応できま す。このため、VPN ソリューションをさまざまな方法で定義できます。場合によっては、最終的 なソリューションが同一になることがあります。ただし、実行されるアプローチは、クライアン トのニーズと環境によって決まります。

この文書の性質と定義されているクライアント要件に基づいて、Adaptive Security Device Manager(ASDM)を使用し、DAPに関する設定の大部分に焦点を当てることができます。ただし、 ローカルグループポリシーを設定して、DAPがローカルポリシー属性をどのように補完または上 書きできるかを示すこともできます。このテストケースでは、LDAPサーバグループ、スプリッ トトンネリングネットワークリスト、および基本的なIP接続(IPプール、DefaultDNSサーバグル ープなど)が事前に設定されているものとします。

グループ ポリシーの定義:ローカル ポリシー属性の定義に必要な設定です。ここで定義する属性 の一部は、DAP では設定できません(例:Local LAN Access)。(このポリシーは、クライアン トレス属性とクライアントベース属性の定義にも使用できます)。

Configuration > Remote Access VPN > Network (Client) Access > Group Policiesの順に移動し、 次に示すようにInternal Group Policyを追加します。

図 17.[Group Policy]: ローカル VPN 固有の属性を定義します。

: GroupP r: VInhe	Policy1 erit erit	
r: 🔽 Inhe	erit	
orwarding URL: 🗹 Inhe	erit	
ss Pools: 🗹 Inhe	erit	Select
ddress Pools: 🗹 Inhe	erit	Select
Options		
d	dress Pools: 🗹 Inh Options	dress Pools: 💟 Inherit

- a. Generalリンクの下で、グループポリシーのnameSSLVPN_GPを設定します。
- b. また、GeneralリンクでMore Optionsをクリックし、Tunneling Protocol:Clientless SSLVPNのみを設定します(アクセス方式を上書きして管理するようにDAPを設定できます)。
- c. Advanced > Split Tunnelingリンクの下で、次の手順を設定します。

図 18.[Split Tunneling]: クライアント接続時に、指定したトラフィック(ローカル ネット

ワーク)が暗号化されていないトンネルをバイパスできるようにします。

a. ポリシー: UncheckInheritand selectExclude Network List。

- b. ネットワークリスト:継承のチェックを外し、リストnameLocal_Lan_Accessを選択 します。(事前設定されているものと仮定します)。
- d. Advanced > ANYCONNECT Clientリンクの下で、次の手順を設定します。

図 19.[SSL VPN Client Installer]: VPN 終了時に、SSL クライアントをエンドポイントに残

General Keep Installer on Client System:	🗌 Inherit	O Yes	O No		
Servers Advanced Datagram Transport Layer Security (DTLS):	🗹 Inherit	🔘 Enable	 Disable 		
Split Tunneling DTLS Compression:	🗹 Inherit	🔿 Enable	O Disable		
Browser Proxy AnyConnect Cliar SSL Compression:	🗹 Inherit	O Deflate	O LZS	O Disable	
Login Setting Ignore Don't Fragment(DF) Bit:	🗹 Inherit	🔿 Enable	O Disable		
Client Firewal Key Regenerat	🗹 Inherit	🔘 Enable	 Disable 		
Dead Peer Det FQDN of This Device:	🗹 FQDN				
Customizatio Custom Attrit MTU:	🗹 Inherit				
> IPsec(IKEv1) Clier Keepalive Messages:	🗹 Inherit	Disable	Interval:	seconds	
Optional Client Modules to Download:	🗹 Inherit				
Always-On VPN:	🗹 Inherit	O Disable	🔘 Use Anyi	Connect Profile setting	6
Client Profiles to Download:	🗸 Inherit				
	◆ Add 會	Delete			

すか、またはアンインストールすることができます。

e. クライアントシステムにインストーラを保持する: UncheckInheritand then selectYes.

f. OKthenApplyをクリックします。

g. 設定変更を適用します。

接続プロファイルの定義:この設定は、AAA認証方式(LDAPなど)を定義し、以前に設定した グループポリシー(SSLVPN_GP)をこの接続プロファイルに適用するために必要です。この接続プ ロファイルを使用して接続するユーザは、ここで定義する属性と、SSLVPN_GPグループポリシ ーで定義する属性の対象になります。(このプロファイルは、クライアントレス属性とクライア ントベース属性の両方の定義にも使用できます)。

Configuration > Remote Access VPN > Network (Client) Access > IPsec Remote Access Connection Profileの順に移動し、次のように設定します。

<mark>asic</mark> dvanced	Name:	DefaultWEBVPNGroup		
	IKE Peer Authentication	I		
	Pre-shared Key:			
	Identity Certificate:	None	٢	Manage
	User Authentication			
	Server Group:	LOCAL	\bigcirc	Manage
	Fallback:	Use LOCAL if Server Group fails		
	Client Address Assignm	nent		
	DHCP Servers:			
		ONONE ODHCP Link ODHCP	Subnet	
	Client Address Pools	:		Select
	Default Group Policy			
	Group Policy:	DfltGrpPolicy	٥	Manage
	(Following field is an	attribute of the group policy selected ab	ove.)	
	🗹 Enable IPsec p	rotocol		
	C Enable L2TP ov	ver IPsec protocol		
d.		Next Previous		

図 20.接続プロファイル:ローカルVPN固有の属性を定義します。

a. Connection ProfilesセクションでDefaultWEBVPNGroupを編集し、Basicリンクで次の手順

を設定します。

a. 認証:方式:AAA

- b. 認証:AAAサーバグループ:LDAP(事前設定されていると想定)
- c. クライアントアドレスの割り当て:Client Address Pools:IP_Pool(事前に設定されて いると想定)
- d. デフォルトのグループポリシー:グループポリシー: SelectSSLVPN_GP

b. 設定変更を適用します。

SSL VPN接続用のIPインターフェイスの定義:この設定は、指定したインターフェイスでクライ アント/クライアントレスSSL接続を終了するために必要です。

インターフェイスでクライアント/ネットワークアクセスを有効にする前に、SSL VPNクライアン トイメージを定義する必要があります。

- 1. Configuration > Remote Access VPN > Network (Client)Access > Anyconnect Client Softwareの順に選択し、次のイメージである、ASAフラッシュファイルシステムからのSSL VPN Client Image:(このイメージはCCO、<u>https://www.cisco.com</u>からダウンロードできます)を追加します。
 - 図 21.SSL VPNクライアントイメージのインストール:エンドポイントに接続するためにプ

ッシュするAnyConnectクライアントイメージを定義します。

- a. anyconnect-mac-4.x.xxx-k9.pkg(入手可能)
- b. OK、OK、続いてApplyの順にクリックします。
- 2. Configuration > Remote Access VPN > Network (Client)Access > AnyConnect Connection Profilesの順に移動し、次の手順を使用してこれを有効にします。

図 22.SSL VPN アクセス インターフェイス:SSL VPN 接続を終了するためのインターフェ



イスを定義します。

- a. Access Interfaceセクションで、Enable:Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below.
- b. また、「アクセスインターフェイス」セクションで、外部インターフェイスのAllow Accessをチェックします。(この設定により、外部インターフェイスでSSL VPNクラ イアントレスアクセスを有効にすることもできます)。
- c. [適用(Apply)] をクリックします。

クライアントレスアクセスのブックマークリスト(URLリスト)の定義:この設定は、ポータル で公開するWebベースのアプリケーションを定義するために必要です。従業員と契約作業員の 2つのURLリストを定義できます。

1. Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarksの 順に移動し、+ をクリックして、次の手順を設定します。

図 23.ブックマーク リスト: Web ポータルで公開し、アクセスできるようにする URL を定



義します(従業員がアクセスできるようにカスタマイズします)。

a. Bookmark List Name: Employeesと入力し、Addをクリックします。

- b. ブックマークタイトル:企業イントラネット
- c. [URL Value] : <u>https://company.resource.com</u>

OKをクリックし、再度OKをクリックします。

+をクリックして追加し、2番目のブックマークリスト(URLリスト)を次のように設定します。

Bookmark List Name:	Employees	
Bookmark Title	URL	Add
		Edit
		Delete
		Move Up
		Move Down
Find:	🔘 🔘 🛛 Match Case	

図 24.ブックマーク リスト:ゲスト アクセス用にカスタマイズします。

a.

Bookmark List Name: Contractors と入力して、Addをクリックします。

b.

ブックマークタイトル:ゲストアクセス

c.

•

•

[URL Value] : <u>https://company.contractors.com</u>

OKをクリックし、再度OKをクリックします。

[適用(Apply)]をクリックします。

ホストスキャンを設定します。

•

Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Imageの順に移動し、次の手順を設定します。

図 25.HostScanイメージのインストール:エンドポイントを接続するためにプッシュするHostScanイメージを定義します

Use this panel to install HostScan.

HostScan configuration can be performed by going to Secure Desktop Manager/HostScan. If 'HostScan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Location: disk0:/hostscan_4.10.07061-k9.pkg	Browse Flash
✓ Enable HostScan	Upload
	Uninstall

a.

disk0:/hostscan_4.xx.xxxx-k9.pkgimageをASAフラッシュファイルシステムからインストールします。

b.

CheckEnable HostScanを使用します。

c.

[適用(Apply)]をクリックします。

ダイナミック アクセス ポリシー:この設定は、接続ユーザとそのエンドポイントを、定義されている AAA 基準と Endpoint Assessment 基準に照合して検証するために必要です。DAPレコードで定義されている基準を満たす場合、接続ユーザに対して、 そのDAPレコードに関連付けられているネットワークリソースへのアクセス権を付与できます。DAP 認可は認証プロセスで実行 されます。

SSL VPN接続がデフォルトケース(たとえば、エンドポイントが設定済みのダイナミックアクセスポリシー(DAP)に一致しない場合)で確実に終了するようにするには、次の手順で設定します。



注:ダイナミックアクセスポリシー(DAP)を初めて設定するときには、DAPコンフィギュレーションファイル (DAP.XML)が存在しないことを示すDAP.xmlエラーメッセージが表示されます。初期DAP設定を変更して保存すると、 このメッセージは表示されなくなります。

Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policiesの順に移動し、次の手順を設定 します。

.

図 30.デフォルトのダイナミックアクセスポリシー(DAP):事前に定義されたDAPレコードが一致しない場合、このDAPレコードを適用できます。したがって、SSL VPNアクセスを拒否できます。

	Add Dynamic A	ccess Policy		
Case				
			ACL Pri	ority: 0
endpoint attributes used to select this acces dpoint attribute has been satisfied. These attr on text.	ss policy. A policy i ributes can be crea	is used when a user's ted using the tables b	authorization attributes match the A elow and/or by expanding the Adva	AA attribute criteria nced option to speci
the following AAA Attributes values 😑)	and the following	endpoint attributes are satisfied.	
Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
	Edit			Edit
	Delete			Delete
				Logical Op.
i roisey Attributes uthorization attributes for this policy. Attribu chy. The resulting VPN authorization policy in ed in DAP).	ute values specified s an aggregation of	here will override the DAP attributes, AAA	ose values obtained from the AAA sy attributes, and group-policy hierarc	stem and the hy attributes (those
work ACL Filters (client) Webtype ACL Filt	ters (clientless)	Functions Port F	orwarding Lists Bookmarks	Access Method
ntinue Quarantine O Terminate O				
sage that will be displayed when this record	is selected.			
	Case I endpoint attributes used to select this access dpoint attribute has been satisfied. These att ion text. the following AAA Attributes values Operation/Value Operation/Value n Policy Attributes uthorization attributes for this policy. Attributes trehy. The resulting VPN authorization policy i ed in DAP). work ACL Filters (client) Webtype ACL Filter	Case I endpoint attributes used to select this access policy. A policy is dopint attribute has been satisfied. These attributes can be creation text. the following AAA Attributes values Operation/Value Add Edit Delete n Policy Attributes uthorization attributes for this policy. Attribute values specified rchy. The resulting VPN authorization policy is an aggregation of ed in DAP). work ACL Filters (client) Webtype ACL Filters (clientless)	Case I endpoint attributes used to select this access policy. A policy is used when a user's i dpoint attribute has been satisfied. These attributes can be created using the tables b ion text. the following AAA Attributes values Operation/Value Add Edit Delete In Policy Attributes uthorization attributes for this policy. Attribute values specified here will override the rchy. The resulting VPN authorization policy is an apgregation of DAP attributes, AAA ed in DAP). Work ACL Filters (client) Webtype ACL Filters (clientless) Functions Port Fo	Case ACL Private A

a.

DfltAccessPolicyを編集し、ActionをTerminateに設定します。

b.

[OK] をクリックします。

Managed_Endpointsという名前の新しいダイナミックアクセスポリシーを次のように追加します。

a.

٠

説明:従業員のクライアントアクセス

図31に示すように、エンドポイント属性タイプ(アンチウイルス)を追加します。完了したら、「OK」をクリッ クします。

図 31.DAPエンドポイント属性:Advanced Endpoint Assessment AntiVirusは、クライアント/ネットワークアクセ

	• • •	Add Endpoint Attribute		
	Endpoint Attribute Type:	Anti-Virus	Θ	
	Product Installation: 0	Installed Not Installed		
	(Hostscan extension need:	nabled Uisabled sto be enabled in Hostscan Image to get a list of Anti-Virus items.)		
	Vendor:	McAfeeAV		
	Product Description: Version:	=	• • • • • • • • • • • • • • • • • • •	
		Please replace character $\mathbf{'x'}$ in Version field with the specific value you want.		
	Last Update:	<	0	days
準として使用できます。		Help Cancel OK		

スのDAP基

c.

前の図に示すように、ドロップダウンリストのAAA Attributeセクションで、User has ALL of the following AAA Attributes Valuesを選択します。

٠

図33および34に示すように、AAA属性タイプ(LDAP)を追加します(AAA属性ボックスの右側)。完了したら、「 OK」をクリックします。

図 33.DAP AAA属性:AAAグループメンバーシップを、従業員を識別するDAP基準として使用できます。 図 34.DAP AAA属性: AAAグループメンバーシップを、リモートアクセス機能を許可するDAP基準として使用で

LDAP
Df
Remote Access Get AD Group
iber(

図35に示すように、Actionタブで、ActionがContinueに設定されていることを確認します。

図 35.[Action] タブ:この設定は、特定の接続またはセッションの特殊処理を定義するために必要です。DAPレコードが一致し、ActionがTerminateに設定されている場合は、VPNアクセスを拒否できます。

図36に示すように、Access MethodタブでAccess MethodAnyConnect Clientを選択します。 図 36.[Access Method] タブ:この設定は、SSL VPN クライアント接続タイプを定義するために必要です。

OK、Applyの順にクリックします。

「Unmanaged_Endpoints」という名前の2番目のダイナミックアクセスポリシーを次のように追加します。

a.

•

٠

説明:従業員のクライアントレスアクセス。

b.

AAA属性セクションの上記の図に示されているドロップダウンリストから、User has ALL of the following AAA Attributes Valuesを選択します。

•

図38および39に示すように、AAA属性タイプ(LDAP)の右側に配置されたAAA属性タイプを追加します。完了したら、「OK」をクリックします。

図 38.DAP AAA属性: AAAグループメンバーシップを、従業員を識別するDAP基準として使用できます。 図 39.DAP AAA属性: AAAグループメンバーシップを、リモートアクセス機能を許可するDAP基準として使用でき ます。

• • •			Add AAA A	ttribute		
AAA Attribute	Type:	u	IAP			0
Attribute ID:	memb	erOf				
Value:	-	0	Remote Access			Get AD Groups
			Citata Conse		_	
			Help Cano			

Actionタブで、ActionがContinueに設定されていることを確認します。(図 35)。

[ブックマーク]タブで、ドロップダウンからリストnameEmployeesを選択し、[追加]をクリックします。また、図 40に示すように、Enable bookmarksにチェックマークが付いていることも確認します。

図 40.[ブックマーク]タブ:このタブでは、ユーザセッションのURLリストを選択および設定できます。

Access/Authorization Policy Attributes Configure access/authorization attributes fo group-policy hierarchy. The resulting VPN as that are not specified in DAP).	r this policy. Attribute values sper athorization policy is an aggregation	ified here will o on of DAP attrib	verride those values obtain utes, AAA attributes, and gr	ed from the AAA roup-policy hier	system and the archy attributes (the	ose
Action Network ACL Filters (client)	Webtype ACL Filters (clientless	Functions	Port Forwarding Lists	Bookmarks	Access Method	
Enable bookmarks Employees		Add>>	Employees			
compress (compress)	Manage	Delete				

•

Access Method タブで、Access Method Web Portalを選択します。(図 36)。

• OK、Applyの順にクリックします。

1. 契約作業員は、DAP AAA属性でのみ識別できます。その結果、エンドポイント属性タイプ:(ポリシー)は手順 4で設定できません。これは、DAP 内の多様性を示すことだけを目的としています。

3.3番目のダイナミックアクセスポリシーGuest_Accessを追加し、以下の項目を設定します。

説明:ゲストクライアントレスアクセス。

•

•

図 37 に示すように、エンドポイント属性タイプ(Policy)を追加します([Endpoint Attribute Type] ボックスの右側)。完 了したら、「OK」をクリックします。

図40では、AAA Attributeセクションのドロップダウンリストから、User has ALL of the following AAA Attributes Valuesを選択します。

図41および図42に示すように、AAA属性タイプ(LDAP)を追加します(AAA属性ボックスの右側)。完了したら、「OK」 をクリックします。

図 41.DAP AAA属性: AAAグループメンバーシップをDAP基準として使用して契約作業員を識別できます

• • •				Add	AAA Attrib	ute			
AAA Attribute	e Type:	LC	AP						3
Attribute ID:	membe	rOf							
Value:	- (0	GuestAccess					Get AD Groups	
			Help		Cancel		ОК		
		_		_		_			_

図 42.DAP AAA属性: AAAグループメンバーシップをDAP基準として使用し、リモートアクセス機能を許可できます

• • •		Add AAA Attribute	
AAA Attribute	Type:	DAP	8
Attribute ID:	memberOf		
Value:	- 0	Remote Access	Get AD Groups
		Help Cancel OK	

•

a.

[Action] タブで、[Action] に [Continue] が設定されていることを確認します(図 35)。

b.

[Bookmarks] タブで、ドロップダウンから「Contractors」というリスト名を選択し、[Add] をクリックします。また 、Enable bookmarksにチェックマークが付いていることも確認します。(図 40 を参照)。

c.

「アクセス方法」タブで、「アクセス方法Webポータル」を選択します。 (図 36)。

d.

[OK] をクリックし、次に [Apply] をクリックします。

結論

この例に記載されているクライアントのリモートアクセスSSL VPN要件に基づき、このソリューションはクライアントのリモート アクセスVPN要件を満たします。

この統合によって進化するダイナミックVPN環境により、ダイナミックアクセスポリシーは、頻繁なインターネット設定の変更、 組織内の各ユーザが持つさまざまなロール、および設定とセキュリティレベルが異なるマネージド/アンマネージドリモートアク セスサイトからのログインに適応し、拡張することができます。

ダイナミックアクセスポリシーは、Advanced Endpoint Assessment、ホストスキャン、Secure Desktop、AAA、ローカルアクセスポ リシーなどの新しい実績あるレガシーテクノロジーによって補完されます。その結果、組織はあらゆるロケーションからあらゆる ネットワーク リソースへのセキュア VPN アクセスを確実に実現できます。

関連情報

シスコのテクニカルサポートとダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。