Cisco Secure Firewall Threat Defense ダイナミック アクセス ポリシーの使用例

初版：2021 年 7 月 8 日

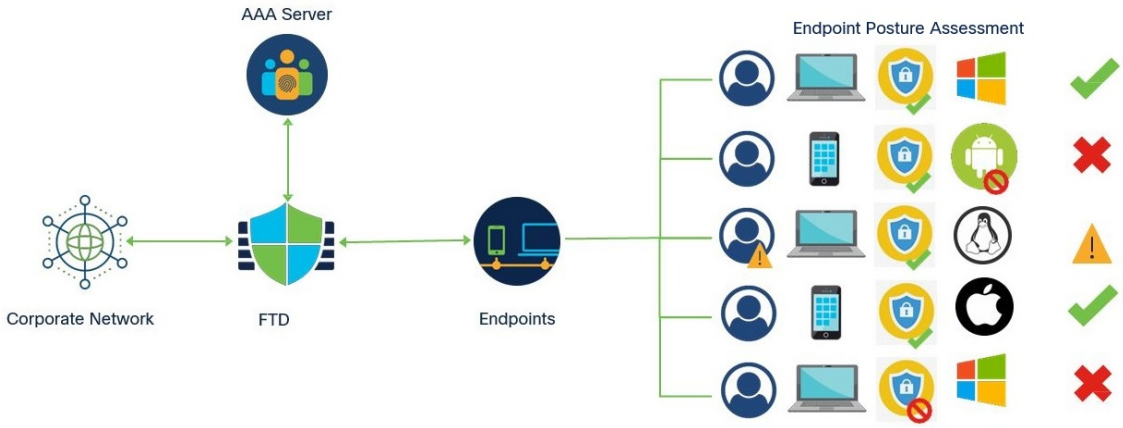
最終更新：2024 年 4 月 18 日

Cisco Secure Firewall Threat Defense ダイナミック アクセス ポリシー

Secure Firewall Threat Defense （旧 Firepower Threat Defense）のダイナミック アクセス ポリシー（DAP）を使用すると、VPN環境のダイナミクスに対処するように承認を設定できます。Secure Firewall Management Center （旧 Firepower Management Center）Web インターフェイスを使用してアクセス制御属性のコレクションを設定し、DAPを作成できます。属性を特定のユーザートンネルまたはセッションに関連付けることができます。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。

脅威に対する防御 は、DAP設定に基づいて特定のユーザーセッションへのVPNアクセスを許可します。 脅威に対する防御 は、1 つ以上の DAP レコードから属性を選択して集約し、ユーザー認証中に DAP を生成します。脅威に対する防御 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とAAA情報に基づいてDAPレコードを選択します。脅威に対する防御は、選択された DAP レコードをユーザートンネルまたはセッションに適用します。

図 *1:* ダイナミック アクセス ポリシーの例



DAP 設定のコンポーネント

新しい DAP 設定では、次の DAP ポリシー、DAP レコード、および DAP 基準属性を作成する必要があります。

- **ダイナミック アクセス ポリシー**：DAP 設定はレコードで構成されます。

- **DAP レコード**：DAP レコードは、基準エンドポイント評価とユーザ認証（AAA）属性で構成されます。レコードが一致する場合、DAP は VPN セッションに適用されるアクションを定義します。
- **DAP 基準と属性**：[AAA基準（AAA Criteria）]、[エンドポイント基準（Endpoint Criteria）]、および[詳細設定（Advanced）] 基準には、ネットワークアクセスの詳細な設定属性が含まれています。

詳細な設定手順については、ダイナミック アクセス ポリシーを設定する （4 ページ）を参照してください。

Threat Defense リモートアクセス VPN と DAP の連携

1. リモートユーザーが、エンドポイントデバイスから Secure Client を使用して VPN 接続を試みます。
2. Threat Defense がエンドポイントでポスチャ評価を実行します。
3. Threat Defense がユーザーを認証、認可、およびアカウンティング（AAA）サーバー経由で認証します。AAA サーバーは、ユーザーの認可属性も返します。
4. Threat Defense が、AAA 認可属性をそのセッションに適用し、VPN トンネルを確立します。
5. 脅威に対する防御 が、AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。
6. Threat Defense が、選択した DAP レコードから DAP 属性を集約し、DAP ポリシーを作成します。
7. Threat Defense が、DAP ポリシーをリモートアクセス VPN セッションに適用します。

DAP を導入する理由

接続しているエンドポイントを特定して、さまざまなネットワークリソースへのユーザーアクセスを許可する DAP 属性を設定できます。次のシナリオ用の DAP を作成できます。さらに DAP 属性を使用してエンドポイントとネットワークリソースの保護を強化できます。

- VPNに接続するエンドポイントが、エンドポイントデバイスまたはプラットフォームに関係なく、組織のセキュリティポリシーに準拠していることを確認します。
- オペレーティングシステム、エンドポイントで実行されているさまざまなセキュリティソフトウェア、レジストリ設定、ファイルバージョン、およびエンドポイントで実行されている潜在的なキーストロークロガーを特定します。
- 企業が管理するエンドポイントでのアプリケーションの可用性と更新を検出して適用します。例：ウイルス対策ソフトウェア。

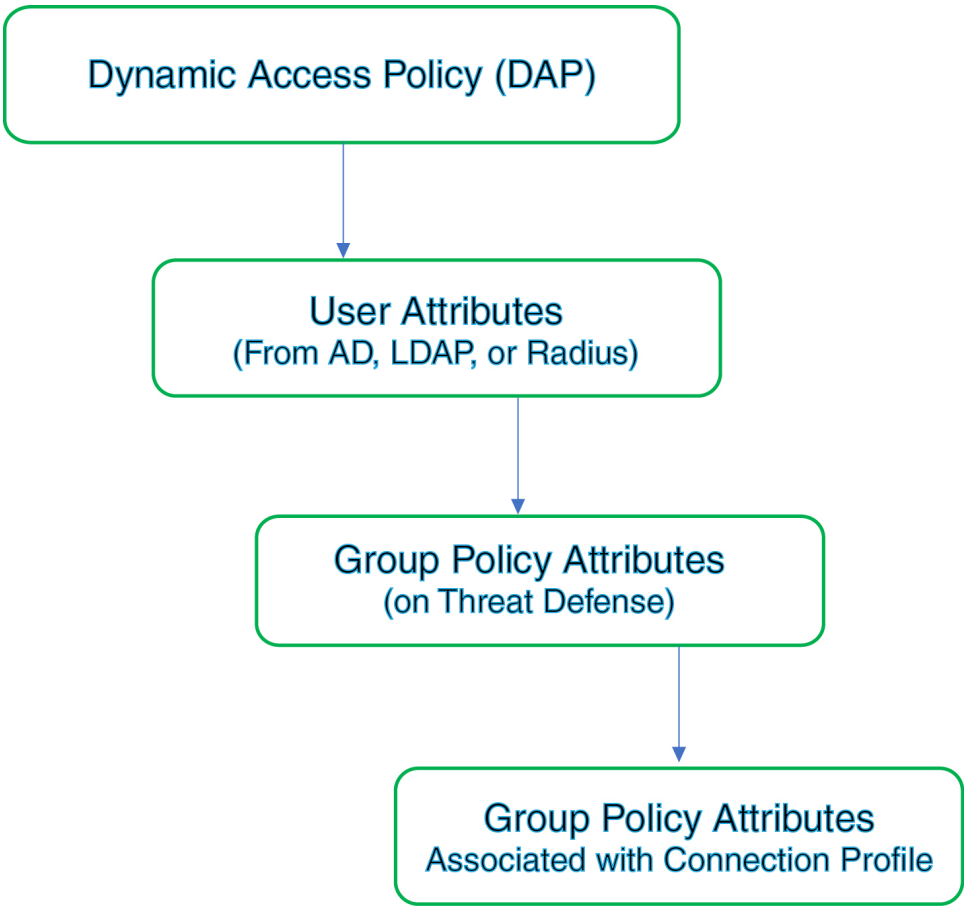
- 許可されたユーザーがアクセスできるネットワークリソースを判別します。

Threat Defense での権限および属性のポリシーの適用

脅威に対する防御デバイスは、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）のVPN接続への適用をサポートしています。属性は、457903脅威に対する防御のDAP、外部認証サーバー、または承認 AAA サーバー（RADIUS）（あるいはこれらのすべて）、または 脅威に対する防御 デバイスのグループポリシーから適用されます。

脅威に対する防御 デバイスがすべてのソースから属性を受信すると、脅威に対する防御 はその属性を評価し、集約してユーザーポリシーに適用します。DAP、AAA サーバー、またはグループポリシーから取得した属性の間で衝突がある場合、DAPから取得した属性が常に優先されます。

図 *2*：ポリシー実施フロー



1. Threat Defense **上の DAP 属性**：DAP 属性は、他のすべての属性よりも優先されます。
2. **外部 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。

3. Threat Defense 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の RADIUS Class 属性 IETF-Class-25（OU=group-policy）の値が返された場合、脅威に対する防御 デバイスはそのユーザーを同じ名前のグループポリシーに入れて、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。
4. 接続プロファイル（トンネル グループと呼ばれる）で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、接続の事前設定と、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。

（注） 脅威に対する防御 デバイスは、デフォルトのグループ ポリシー *DfltGrpPolicy* から継承したシステム デフォルト属性をサポートしていません。ユーザー属性または AAA サーバーのグループポリシーによって上書きされない場合、接続プロファイルから割り当てられたグループポリシーの属性がユーザーセッションに使用されます。

ダイナミック アクセス ポリシーのライセンス

脅威に対する防御 には、リモートアクセス VPN をサポートする次のいずれかの AnyConnect ライセンスが必要です。

- Secure Client Premier
- Secure Client Advantage
- Secure Client VPN Only

Management Center ではエクスポート制御機能を有効にする必要があります。

脅威に対する防御 のライセンスに関する詳細については、『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Licensing the Firepower System*」の章を参照してください。

ダイナミック アクセス ポリシーを設定する

ダイナミック アクセス ポリシー（DAP）には、ユーザーとエンドポイントの属性を構成する複数の DAP レコードを含めることができます。ユーザーが VPN 接続を試みるときに必要な基準が適用されるように、DAP レコードに優先順位を付けることができます。

始める前に

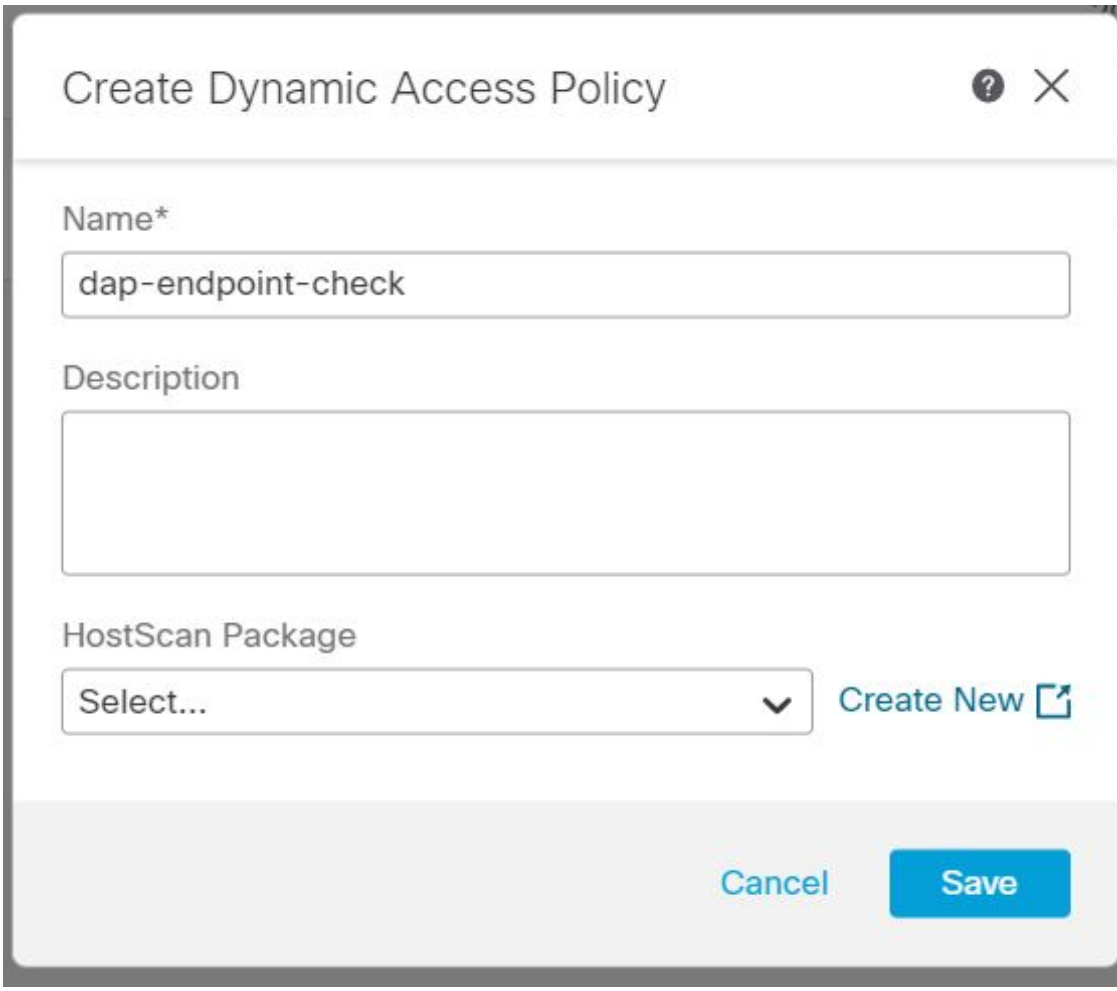
ダイナミック アクセス ポリシー（DAP）を作成する前に、以下の必要なアプリケーションと設定を構成しているか確認します。

- **HostScan パッケージ**：HostScan パッケージバージョン 4.6 以降をダウンロードします。
- **AAA サーバー** ：VPN セッションを認証または認可するときに正しい属性を返すように必要な AAA サーバを設定します。

- **Secure Client パッケージ**：Cisco Secure Clientの最新バージョンをダウンロードし、リモートアクセス VPN 設定に追加します。
- **リモートアクセス VPN**：**[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]** で Remote Access VPN Configuration ウィザードを使用して、リモートアクセス VPN の設定を構成します。
- **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [AnyConnectファイル（AnyConnect File）]**で HostScan パッケージをアップロードします。

1. まだ行っていない場合は、新しいダイナミックポリシーを設定します。
   a) **[デバイス（Devices）] > [ダイナミックアクセスポリシー（Dynamic Access Policy）] > [ダイナミックアクセスポリシーの作成（Create Dynamic Access Policy）]**を選択します。

   図 *3:* ダイナミック アクセス ポリシーの作成



   b) DAP ポリシーの [名前（Name）] を指定し、必要に応じて [説明（Description）] を指定します。

c) ドロップダウンから [HostScanパッケージ（HostScan Package）] を選択します。または、[新規作成（Create New）] をクリックして HostScan パッケージファイルを追加します。
ダイナミック アクセス ポリシーには、デフォルトの DAP レコードが含まれています。Lua スクリプトを使用して、[AAA基準（AAA Criteria）]、[エンドポイント基準（Endpoint Criteria）]、および [詳細設定（Advanced）] 基準の必須属性を持つ DAP レコードの追加を開始できます。

d) [保存（Save）] をクリックします。

2. DAP レコードを作成し、優先順位の数値を割り当てます。

DAP レコードには、VPN ユーザーが 脅威に対する防御 VPN ゲートウェイへの VPN 接続を試みるときに照合する属性が含まれます。DAP レコードの設定を使用して、選択した基準属性に基づいて VPN アクセスを許可、拒否、または制限できます。

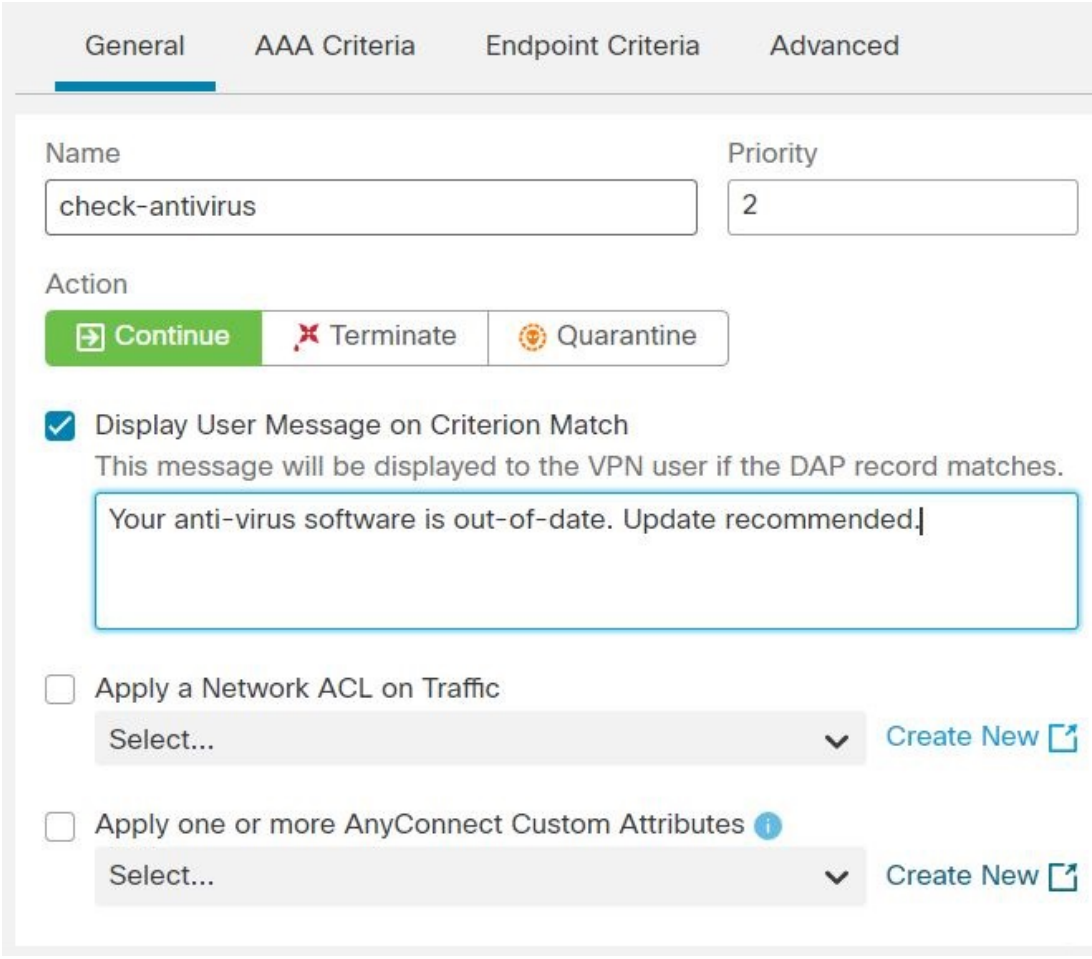
[優先順位（Priority）] の数値は、レコードの照合順序を示します。脅威に対する防御 は DAP レコードの優先順位の数値を使用して、レコードの順序付けと選択を行います。値が小さいほど、優先順位が高くなります。

（注） DAP の DAP レコードを設定しない場合、**デフォルトの DAP** レコードが適用されます。デフォルトの DAP レコードには優先順位がありません。

a) [デバイス（Devices）]>[ダイナミック アクセス ポリシー（Dynamic Access Policy）] を選択します。 >

b) 既存の DAP を編集するか、新しい DAP を作成します。

c) [DAPレコードの作成（Create DAP Record）] をクリックします。



d) DAP レコードの [名前（Name）] を指定します。

e) DAP レコードの [優先順位（Priority）] の数値を入力します。

f) DAP レコードが一致した場合に実行する [アクション（Action）] を選択します。

- [続行（Continue）]：セッションにアクセスポリシー属性を適用し、ユーザーを許可する場合にクリックします。
- [終了（Terminate）]：セッションを終了する場合に選択します。
- [検疫（Quarantine）]：接続を隔離する場合に選択します。

g) [基準に一致したときユーザーメッセージを表示（Display User Message on Criterion Match）] を選択し、ボックスにメッセージを追加します。

（注） VPN ユーザーは、DAP レコードが一致するとメッセージを受け取ります。

h) [トラフィックにネットワークACLを適用する（Apply a Network ACL on Traffic）] チェックボックスをオンにして、リストから ACL を選択します。新しい ACL を作成して選択することもできます。

この DAP レコードが一致すると、ネットワーク ACL が VPN セッションに適用されます。

i) [1つまたは複数のAnyConnectカスタム属性を適用する（Apply one or more AnyConnect Custom Attributes）] を選択し、ドロップダウンからカスタム属性オブジェクトを選択します。

j) [保存（Save）] をクリックします。

ネットワーク ACL および AnyConnect カスタム属性の詳細については、最新の『Secure Firewall Management Center Configuration Guide』を参照してください [英語]。

k) ユーザーとエンドポイントが VPN に接続したときにチェックする DAP 属性を設定します。

- DAP の AAA 基準設定を構成する （9 ページ）
- DAP のエンドポイント属性選択基準の設定 （11 ページ）
- DAP の詳細設定を構成する （12 ページ）

3. DAP をリモートアクセス VPN の設定とリンクします。

VPN セッションの認証または認可中に DAP 属性が照合されるように、DAP をリモートアクセス VPN ポリシーに関連付ける必要があります。

a) Secure Firewall Management Center の Web インターフェイスで、**[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]**を選択します。

b) DAP を追加するリモートアクセスポリシーを選択して編集します。

a) ダイナミック アクセス ポリシーの関連付けリンクをクリックします。

b) リストから [ダイナミックアクセスポリシー（Dynamic Access Policy）] を選択します。

c) [OK] をクリックします。

DAP をリモートアクセス VPN に関連付けると、 脅威に対する防御 はユーザーが VPN 接続を試みたときに、設定された DAP レコードと属性をチェックします。脅威に対する防御 は、一致に基づいて DAP を作成し、VPN セッションで適切なアクションを実行します。

4. 脅威に対する防御 デバイスでリモートアクセス VPN を展開します。

a) Management Center メニューバーで、[展開（Deploy）] をクリックし、[展開（Deployment）] を選択します。

脅威に対する防御 デバイスへの展開が保留されているすべての古い設定のリストを表示できます。

b) リモートアクセス VPN およびその他の設定変更を展開するデバイスを特定して選択します。

c) [展開（Deploy）] をクリックします。

（注） 設定を展開する前に問題を修正してください。

DAP の AAA 基準設定を構成する

Threat Defense は、AAA サーバーによって VPN セッションに付加された AAA 属性を使用して、ユーザーまたはユーザーグループを照合します。

DAP は AAA サービスを補完します。用意されている認可属性のセットはかぎられていますが、それらの属性によって AAA で提供される認可属性を無効にできます。Threat Defense は、AAA 認可情報と VPN セッションのポスチャ評価情報に基づいて DAP レコードを選択します。脅威に対する防御 は、アセスメントに基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 認可属性を作成します。

始める前に

VPN ユーザーの認証、許可、アカウンティングに必要な AAA サーバーが設定されていることを確認します。AAA サーバーは、リモートアクセス VPN を展開する 脅威に対する防御 デバイスから到達可能であることが必要です。

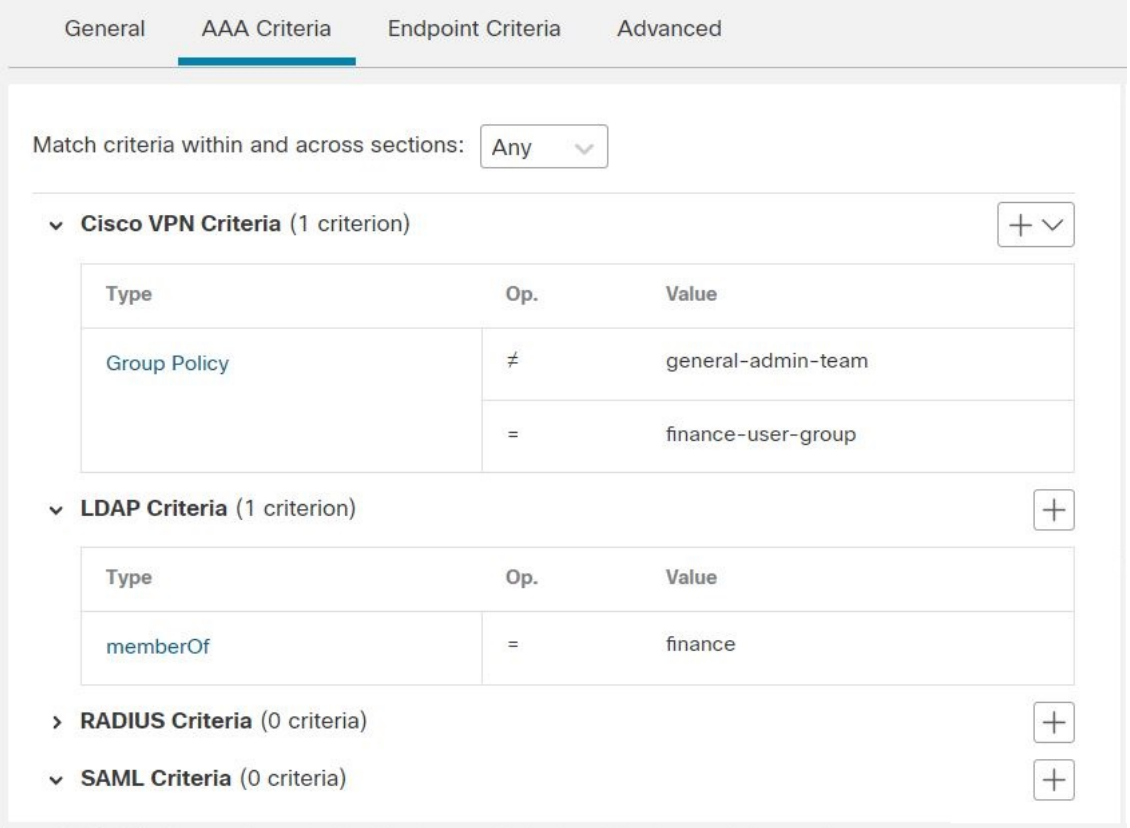
手順

ステップ 1 [デバイス（Devices）] > [ダイナミック アクセス ポリシー（Dynamic Access Policy）] を選択します。 >

ステップ 2 既存の DAP ポリシーを編集するか、新しい DAP ポリシーを作成してからポリシーを編集します。

ステップ 3 DAP レコードを選択するか新しいレコードを作成して、DAP レコードを編集します。

ステップ 4 [AAA基準（AAA Criteria）] をクリックします。



ステップ 5 次の [セクション間の一致基準（Match criteria between sections）] のいずれかを選択します。

- [任意（Any）]：いずれかの基準に一致。
- [すべて（All）]：設定されたすべての基準に一致。
- [なし（None）]：設定された基準のいずれにも一致しない。

ステップ 6 [追加（Add）] をクリックして、必要な **Cisco VPN 基準**を追加します。

Cisco VPN 基準には、グループポリシー、割り当てられた IPv4 アドレス、割り当てられた IPv6 アドレス、接続プロファイル、ユーザー名、ユーザー名 2、必要な SCEP の事前定義された属性が含まれます。

a) [属性ID（Attribute ID）] と演算子を選択し、[値（Value）] に一致する値をを指定します。
b) [別の条件を追加（Add another criteria）] をクリックして、さらに AAA 条件を追加します。
c) [保存（Save）] をクリックします。

ステップ 7 [LDAP基準（LDAP Criteria）]、[RADIUS基準（RADIUS Criteria）]、または [SAML基準（SAML Criteria）] を選択します。[属性 ID（Attribute ID）] と [値（Value）] を指定します。

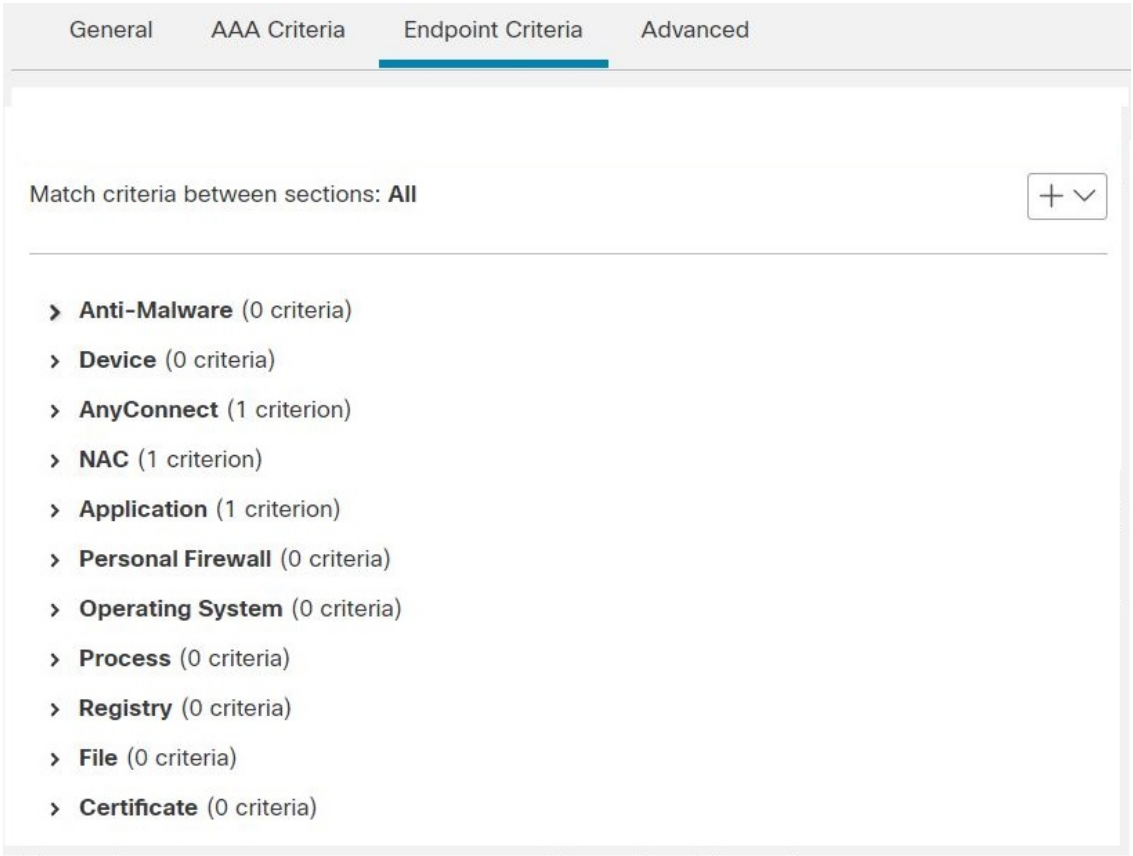
これらの属性は、入力する値に対して = または ≠ のいずれかに設定できます。各 DAP レコードに任意の数の AAA 属性を追加できます。

ステップ 8 [保存（Save）] をクリックします。

DAP のエンドポイント属性選択基準の設定

エンドポイント属性には、エンドポイント システム環境、ポスチャ評価結果、およびアプリケーションに関する情報が含まれています。脅威に対する防御は、エンドポイント属性の集合をセッション確立時に動的に生成し、セッションに関連付けられたデータベースにその属性を保存します。各 DAP レコードには、脅威に対する防御 がセッションの DAP レコードを選択するために満たす必要があるエンドポイント選択属性が指定されます。脅威に対する防御は、設定されたすべての条件を満たす DAP レコードだけを選択します。

図 *4 : DAP* エンドポイント属性



手順

ステップ 1 **[デバイス（Devices）] > [ダイナミックアクセスポリシー（Dynamic Access Policy）] > [ダイナミックアクセスポリシーの作成（Create Dynamic Access Policy）]**を選択します。

ステップ 2 DAP ポリシーを編集してから、DAP レコードを編集します。

（注） DAP ポリシーと DAP レコードをまだ作成していない場合は作成します。

ステップ 3 [エンドポイント基準（Endpoint Criteria）] をクリックし、次の属性タイプから必要なエンドポイント基準属性を設定します。

- マルウェア対策（Anti-Malware）
- デバイス
- Secure Client
- NAC
- アプリケーション（Application）
- Firewall
- オペレーティング システム
- プロセス
- レジストリ
- ファイル（File）
- 証明書

（注） 各タイプのエンドポイント属性のインスタンスを複数作成できます。各 DAP レコードに任意の数のエンドポイント属性を追加することもできます。

ステップ 4 [保存（Save）] をクリックします。

DAP の詳細設定を構成する

[詳細設定（ Advanced）] タブを使用して、AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加できます。

Lua で適切な論理式を作成し、ここに入力します。Lua スクリプトで assert 関数を使用できます。この関数は、引数を true またはコードの条件として返します。それ以外の場合は、assert エラーメッセージが表示されます。assert 関数と Lua スクリプトの詳細については、『Lua Reference Manual』を参照してください。

手順

ステップ 1 [デバイス（Devices）] > [ダイナミック アクセス ポリシー（Dynamic Access Policy）] を選択します。 >

ステップ 2 DAP ポリシーを編集してから、DAP レコードを編集します。

（注） DAP ポリシーと DAP レコードをまだ作成していない場合は作成します。

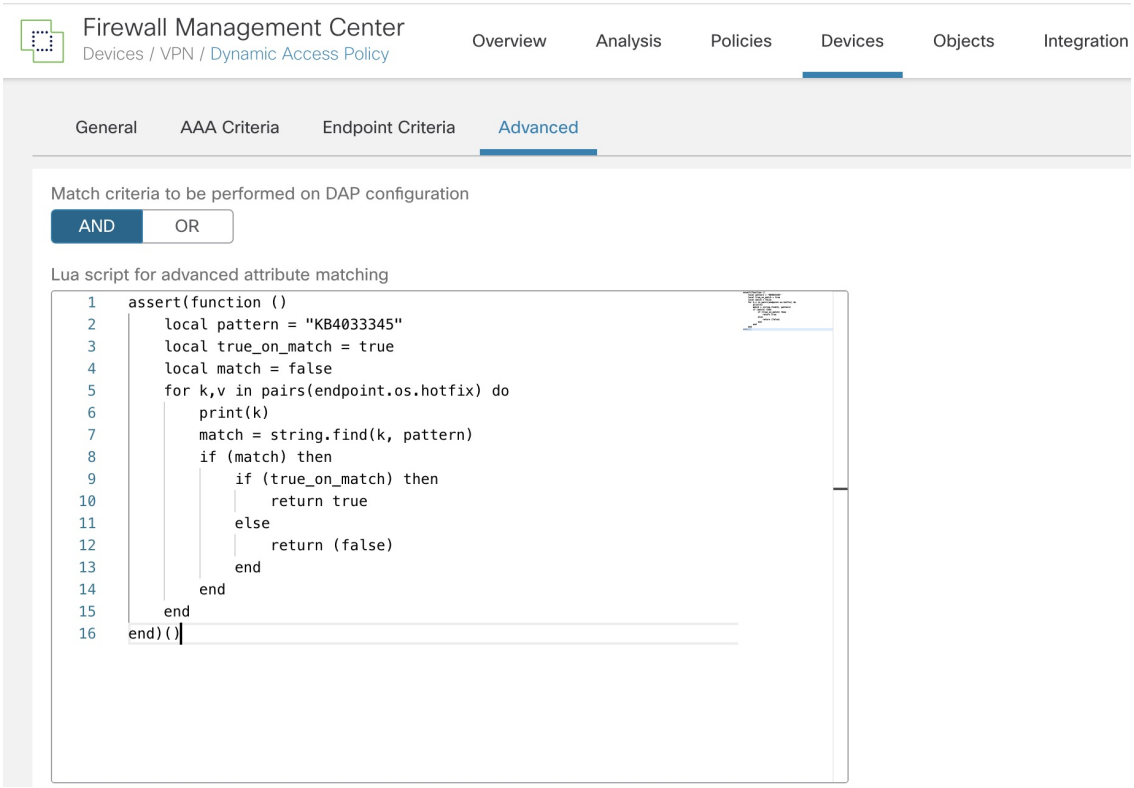
ステップ 3 [Advanced] タブをクリックします。

ステップ 4 DAP 設定で照合する一致基準として [AND] または [OR] を選択します。

ステップ 5 [高度な属性照合用のLuaスクリプト（Lua script for advanced attribute matching）] フィールドに Lua スクリプトを追加します。

次のスクリプトは、クライアントの OS（Secure Client がインストール済み）で特定のホットフィックスをチェックし、true または false を返します。

図 5 : *Lua* スクリプトを使用した高度な基準照合



ステップ 6 [保存（Save）] をクリックします。

ダイナミック アクセス ポリシーのトラブルシューティング

DAP の問題をトラブルシューティングする前に、次を実行します。

- プラットフォーム設定ポリシーで VPN Syslog を有効にします。
- **[デバイス（Devices）] > [VPN] > [トラブルシューティング（Troubleshooting）] >** で DAP 関連のログを確認します。

問題 1：**DAP** の設定を保存できない

ソリューション

Management Center Web インターフェイスから DAP 設定を保存できない場合は、適切なログを確認して失敗の理由を見つけます。

- `/var/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log.*`
- `/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log.*`

キーワード `vpn` または `sso` を使用して、関連するログをフィルタリングできます。

問題 2：**DAP** の展開が失敗する

ソリューション：

DAPの展開に失敗した場合は、展開のトランスクリプトの詳細を確認してから、ログファイル `/var/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log.*` を確認します。

ダイナミック アクセス ポリシーの例

この項では、VPN ユーザーとそのエンドポイントに対する VPN アクセスを許可またはブロックするダイナミック アクセス ポリシー（DAP）設定の例を示します。

（注） このドキュメントに記載されている手順は設定例です。さまざまな DAP 設定を使用して、要件に応じて単一の DAP レコードまたは複数の DAP レコードを設定できます。DAP 設定の [AAA 基準（AAA Criteria）]、[エンドポイント基準（Endpoint Criteria）]、および Lua スクリプトを使用した [詳細設定（Advanced）] 設定に属性が含まれます。

セキュリティ要件に基づいて、複数の条件に一致する単一の DAP レコードを設定するか、複数の DAP レコードを作成し、必要に応じてそれらに優先順位を付けることができます。

オペレーティングシステムに基づいて VPN アクセスを許可またはブロックする

オペレーティングシステムに基づいて、エンドポイントの VPN アクセスを決定できます。ここに示す例を使用して、Windows オペレーティング システム バージョン 7 を実行していて、サービスパック SP1 Convenience Rollup を使用していないエンドポイントをブロックします。

手順

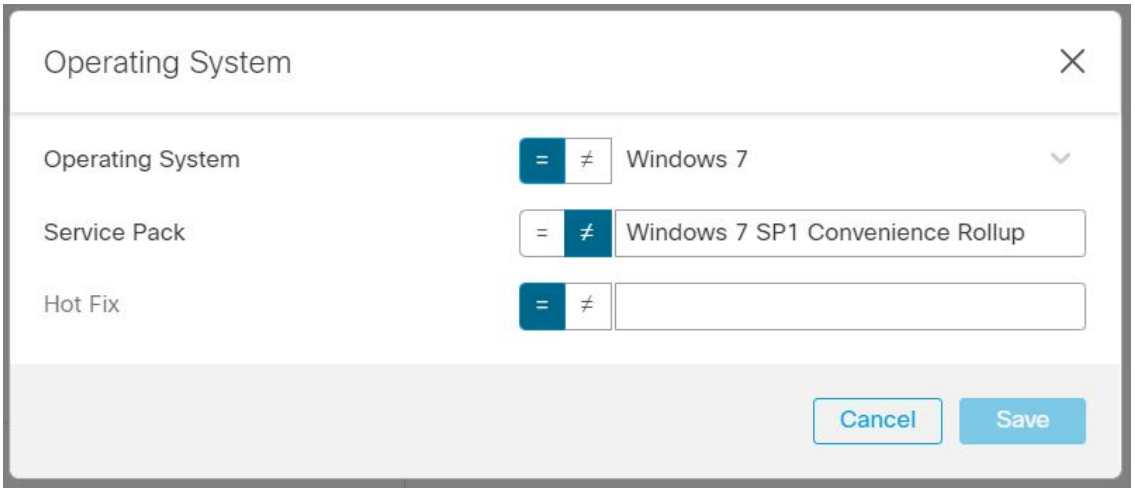
ステップ 1 DAP レコードを作成するか、**[終了（Terminate）]** アクションで既存のレコードを編集します。

ステップ 2 **[エンドポイント基準（Endpoint Criteria）]** > **[オペレーティングシステム（Operating System）]** を選択します。

ステップ 3 設定されたすべての属性が一致する場合にのみ条件を選択するには、一致基準[すべて（All）]を選択します。

ステップ 4 [追加（Add）] をクリックして、オペレーティングシステム属性を追加します。

図 *6 : DAP* オペレーティングシステムのエンドポイント基準



ステップ 5 [オペレーティングシステム（Operating System）]で等しい（=）演算子を選択し、[Windows 7]を選択します。

ステップ 6 [サービスパック（Service Pack）] で等しくない（≠）演算子を選択し、[SP1 Convenience Rollup]を指定します。

ステップ 7 [保存（Save）] をクリックします。

エンドポイントのマルウェア対策属性に基づいてトラフィックをブロックする

ここにリストされている手順を使用して、エンドポイントが VPN に接続を試みるときにチェックされるマルウェア対策属性を設定できます。DAP レコードの属性を使用して、次をチェックできます。

- エンドポイントに Cisco Secure Endpoint がインストールされていて、リアルタイムスキャンが有効になっているかどうか。
- Cisco Secure Endpoint のバージョンが 1.2 以降で、マルウェア対策が 15 日以内に更新されているかどうか。

脅威に対する防御で DAP を設定する詳細な手順については、ダイナミック アクセス ポリシーを設定する （4 ページ）を参照してください。

手順

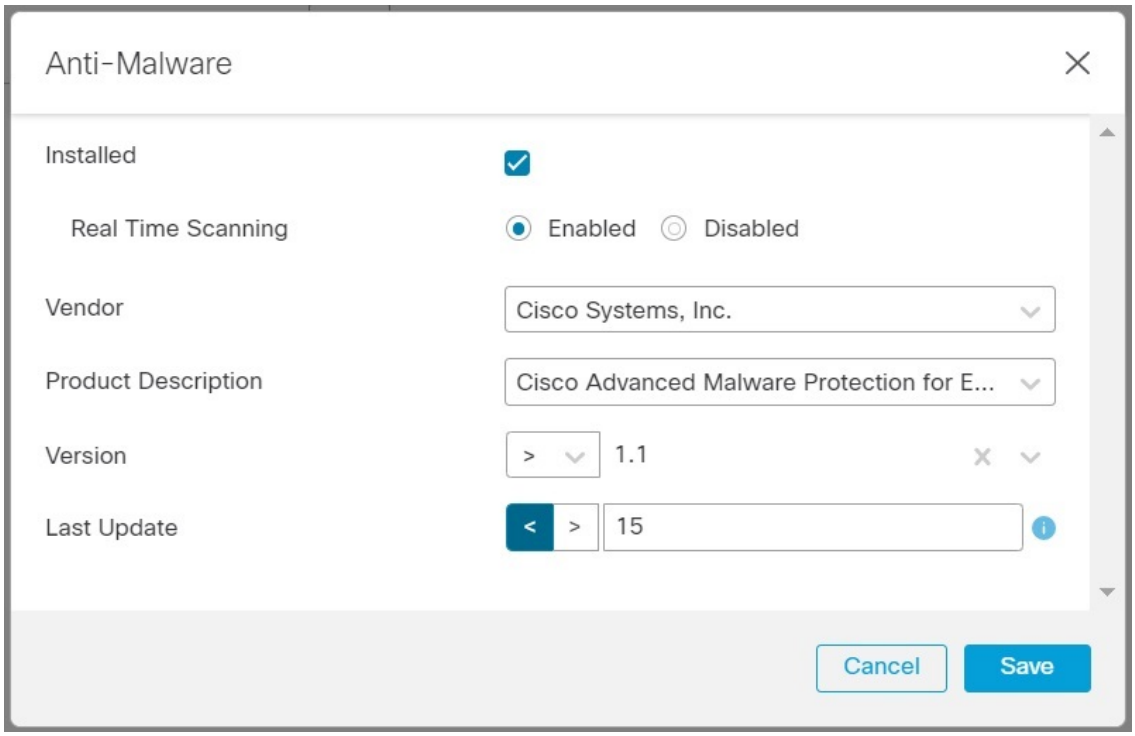
ステップ 1 [終了（Terminate）] アクションで DAP レコードを作成するか、既存の DAP レコードを編集します。

ステップ 2 DAP レコードで**[エンドポイント基準（Endpoint Criteria）] > [マルウェア大対策（Anti-Malware）]**を選択します。

ステップ 3 設定されたすべての属性が一致する場合にのみ基準を選択するには、一致基準[すべて（All）] を選択し、いずれかの属性に一致する場合は [任意（Any）] を選択します。

ステップ 4 [追加（Add）] をクリックして、属性を追加します。

図 *7: DAP* マルウェア対策エンドポイントの基準



ステップ 5 [インストール済み（Installed）] をクリックして、マルウェア対策製品がインストールされているかどうかを示します。

ステップ 6 [有効（Enabled）] を選択して、リアルタイムのマルウェアスキャンがアクティブかどうかをチェックします。

ステップ 7 [ベンダー（Vendor）] のリストからマルウェア対策ベンダーの名前を選択します。

この例では、Cisco Secure Endpoint のベンダーとして [Cisco Systems, Inc.] を選択しています。希望のベンダーを選択します。

ステップ 8 マルウェア対策製品の [製品の説明（Product Description）] で [Cisco Secure Endpoint] を選択します。

（注） VPN に接続するエンドポイントで実行されているマルウェア対策製品に基づいて、希望する別のベンダーと製品を選択します。

ステップ 9 マルウェア対策製品の [バージョン（Version）] には 1.2 以降のバージョンを選択します。

ステップ 10 [最終更新（Last Update）] からの日数を指定します。

マルウェア対策製品の更新が 15 日未満である必要があることを示します。

ステップ 11 [保存（Save）] をクリックします。

リモート アクセス アプリケーションの VPN アクセスを許可またはブロックする

リモートアクセス接続のタイプをチェックしてユーザーの VPN アクセスを許可または拒否するには、DAP レコードでアプリケーション エンドポイント基準を使用します。

手順

ステップ 1 DAP レコードを作成するか、必要に応じて [続行（Continue）] または [終了（Terminate）] アクションで既存のレコードを編集します。

ステップ 2 **[エンドポイント基準（Endpoint Criteria）]** > **[アプリケーション（Application）]** を選択します。

ステップ 3 設定されたすべての属性が一致する場合にのみ基準を選択するには、一致基準[すべて（All）] を選択し、いずれかの属性に一致する場合は [任意（Any）] を選択します。

ステップ 4 [追加（Add）] をクリックして、オペレーティングシステム属性を追加します。

図 *8 : DAP* アプリケーションのエンドポイント基準

（注） この例を使用して、Secure Client アプリケーションを使用して接続する VPN ユーザーを許可またはブロックできます。

確認する項目だけを選択し、必要な値を入力できます。また、デバイスチェックを、複数のエンドポイントまたは AAA 基準を持つ別の DAP レコードと組み合わせることもできます。

ステップ 5 等しい（=）または等しくない（≠）演算子を選択し、リモートアクセスの [クライアントタイプ（Client Type）] を選択します。

リストされているクライアントタイプは、[クライアントレス（Clientless）]、[カットスループロキシ（Cut-Through-Proxy）]、[Secure Client]、[IPsec]、[L2TP]、および [IPsec-IKEv2-Generic-RA] です。

ステップ 6 [保存（Save）] をクリックします。

エンドポイントデバイスをチェックして VPN アクセスを許可またはブロックする

特定のデバイスの VPN アクセスを許可またはブロックする DAP 基準を作成できます。ユーザーが VPN 接続を試みるときに確認するデバイスの詳細を設定します。

手順

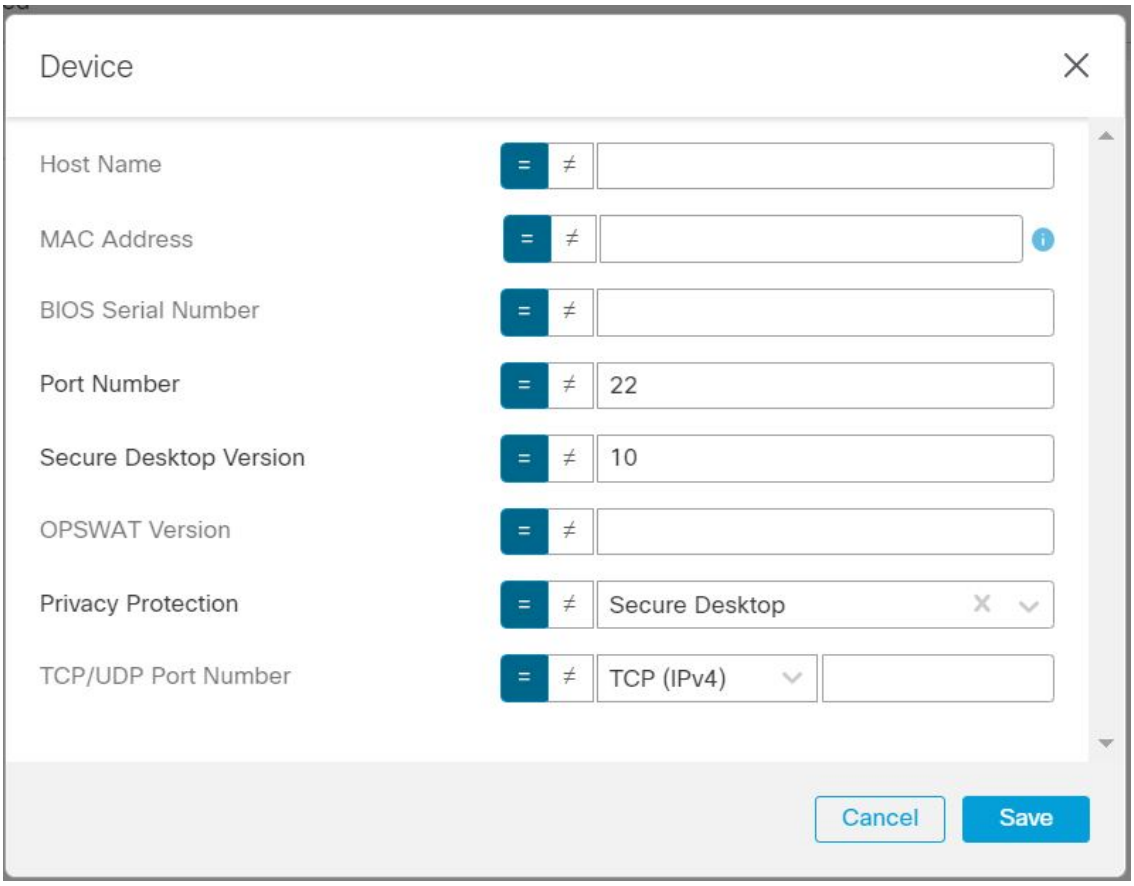
ステップ 1 DAP レコードを作成するか、必要に応じて [続行（Continue）] または [終了（Terminate）] アクションで既存のレコードを編集します。

ステップ 2 **[エンドポイント基準（Endpoint Criteria）] > [デバイス（Device）]**を選択します。

ステップ 3 設定されたすべての属性が一致する場合にのみ基準を選択するには、一致基準 [すべて（All）] を選択し、いずれかの属性に一致する場合は [任意（Any）] を選択します。

ステップ 4 [追加（Add）] をクリックして、オペレーティングシステム属性を追加します。

図 *9 : DAP* デバイスのエンドポイント基準の例



（注） この例を使用して、ポート番号 22、Secure Desktop バージョン 10、プライバシー保護をSecure Desktop として接続しているエンドポイントを許可またはブロックします。

チェックする項目のみを選択してから、必要な値を入力できます。また、デバイスチェックを、複数のエンドポイントまたはAAA 基準を持つ別の DAP レコードと組み合わせることもできます。

ステップ 5 等しい（=）または等しくない（≠）演算子を選択し、デバイス情報を指定します。必須フィールドを選択し、[ホスト名（Host Name）]、[MAC アドレス（MAC Address）]、[BIOSシリアル番号（BIOS Serial Number）]、[ポート番号（Port Number）]、[セキュアデスクトップバージョン（Secure Desktop Version）]、および [OPSWATバージョン（OPSWAT Version）] の値を入力します。

ステップ 6 等しい（=）または等しくない（≠）演算子を選択し、[プライバシー保護（Privacy Protection）] と [TCP/UDPポート番号（TCP/UDP Port Number）] を選択します。

ステップ 7 [保存（Save）] をクリックします。

Lua スクリプトを使用してエンドポイントのマルウェア対策をチェックする

この項に示す設定例では、エンドポイントでマルウェア対策製品の有無をチェックするために必要な Lua スクリプトを提供しています。

Lua スクリプトを使用して論理式を作成するには、LUA の知識が必要です。LUA のプログラミングの詳細については、http://www.lua.org/manual/5.1/manual.html を参照してください。

詳細については、『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Cisco Secure Firewall Threat Defense Dynamic Access Policies*」セクションを参照してください。

手順

ステップ 1 DAP レコードを作成するか、既存の DAP レコードを編集します。

ステップ 2 DAP レコードで [詳細設定（Advanced）] をクリックします。

ステップ 3 一致基準 [AND] または [OR] を選択します。

ステップ 4 次のスクリプトを Lua スクリプト領域にコピーします。

```
assert(function()
local am_count = 0;
CheckAndMsg( true, "endpoint.av="..type(endpoint.am), nil)
for k,v in pairs(endpoint.am) do
am_count = am_count + 1
-- CheckAndMsg( true, "v.exists"..v.exists, nil)
-- CheckAndMsg( true, "v.description"..v.description, nil)
-- CheckAndMsg( true, "v.version"..v.version, nil)
-- CheckAndMsg( true, "v.activescan"..v.activescan, nil)
end
CheckAndMsg( true, "Your request has "..am_count.." Ams", nil)
return true
end)()
```

ステップ 5 [保存（Save）] をクリックします。

DAP でサポートされる AAA およびエンドポイント属性

脅威に対する防御 デバイスは、ユーザー属性が、設定済みの AAA 属性およびエンドポイント属性に一致する場合に DAP ポリシーを使用します。Cisco Secure Client のホストスキャンモジュールは、設定されたエンドポイント属性に関する情報をデバイスに返します。DAP サブシステムはその情報を使用して、それらの属性の値に一致する DAP レコードを選択します。

アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラムのほとんど（すべてではなく）は、アクティブスキャンをサポートしています。つまり、それらのプログラムはメモリ常駐型であり、常に動作しています。ホストスキャンは、エンドポイントにプログラムがインストールされているかどうか、およびそのプログラムがメモリ常駐型かどうかを、次のようにしてチェックします。

- インストールされているプログラムがアクティブ スキャンをサポートしない場合、ホスト スキャンはそのソフトウェアの存在をレポートします。DAP システムは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがイネーブルになっている場合、ホスト スキャンはそのソフトウェアの存在をレポートします。この場合も、セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがディセーブルになっている場合、ホスト スキャンはそのソフトウェアの存在を無視します。セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択しません。

DAP でサポートされる AAA 属性

DAP レコードの選択基準として AAA 属性を設定するには、[Add/Edit AAA Attributes] ダイアログボックスで、使用する Cisco、LDAP、または RADIUS 属性を設定します。これらの属性は、入力する値に対して「=」または「!=」のいずれかに設定できます。各 DAP レコードに設定可能な AAA 属性の数に制限はありません。

Cisco VPN の基準

Cisco VPN の基準は、AAA 階層モデルに保存されているユーザー認可属性を参照します。DAP レコードの AAA 選択属性に、これらの属性の小規模なサブセットを指定できます。次のものがあります。

- [グループポリシー（Group Policy）]：VPN ユーザーセッションに関連付けられているグループ ポリシー名。セキュリティ アプライアンスでローカルに設定するか、IETF クラス（25）属性として RADIUS/LDAP から送信します。最大 64 文字です。
- [割り当て済みIPv4アドレス（Assigned IPv4 Address）]：ポリシーに指定する IPv4 アドレスを入力します。フルトンネル VPN クライアントに割り当てられた IP アドレス（IPsec、L2TP/IPsec、SSL VPN AnyConnect）です。
- [割り当て済みIPv6アドレス（Assigned IPv6 Address）]：ポリシーに指定する IPv6 アドレスを入力します。
- [接続プロファイル（Connection Profile）]：リモート アクセス VPN 接続プロファイル名。最大 64 文字です。
- [ユーザー名（Username）]：認証されたユーザーのユーザー名。最大 64 文字です。ローカル認証、RADIUS 認証、LDAP 認証のいずれかを、またはその他の認証タイプ（RSA/SDI、NT Domain など）のいずれかを使用している場合に適用されます。
- [ユーザー名2（Username2）]： 認証されたユーザーのセカンダリユーザー名。最大 64 文字です。

LDAP 基準

LDAP クライアント（セキュリティアプライアンス）は、ユーザーの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ LDAP 応答属性値のペアを保存します。LDAP クライアントでは、受信した順に応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザー レコードとグループ レコードの両方が LDAP サーバーから読み込まれると、このシナリオが発生する場合があります。ユーザー レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

Active Directory（AD）グループメンバーシップをサポートするために、AAA LDAP クライアントでは、LDAP memberOf応答属性に対する特別な処理が行われます。AD memberOf属性は、AD 内のグループ レコードの DN 文字列を指定します。グループの名前は、DN 文字列内の最初の CN 値です。LDAP クライアントでは、DN 文字列からグループ名を抽出して、AAA memberOf 属性として格納し、応答属性データベースに LDAP memberOf 属性として格納します。LDAP応答メッセージ内に追加のmemberOf属性が存在する場合、それらの属性からグループ名が抽出され、前のAAA memberOf属性と結合されて、グループ名がカンマで区切られた文字列が生成されます。この文字列は応答属性データベース内で更新されます。

LDAP 認証/認可サーバーへの VPN リモートアクセスセッションが次の 3 つの Active Directory グループ（memberOf列挙）のいずれかを返す場合、Threat Defenseデバイスは次の3つの Active Directory グループを処理します。

cn=Engineering,ou=People,dc=company,dc=com

cn=Employees,ou=People,dc=company,dc=com

cn=EastCoastast,ou=People,dc=company,dc=com

これらのグループは、aaa.ldap 選択基準として任意の組み合わせで使用できます。

LDAP 属性は、DAP レコード内の属性名と属性値のペアで構成されています。LDAP 属性名は、構文に従う必要があり、大文字、小文字を区別します。たとえば、AD サーバーが部門として返す値の代わりに、LDAP 属性の Department を指定した場合、DAP レコードはこの属性設定に基づき一致しません。

（注） [Value]フィールドに複数の値を入力するには、セミコロン（;）をデリミタとして使用します。次に例を示します。

eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

RADIUS 基準

RADIUS クライアントは、ユーザの AAA セッションに関連付けられたデータベースにすべてのRADIUS応答属性値のペアを格納します。RADIUSクライアントは、受け取った順序で応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザー レコードおよびグループ レコードの両方が RADIUS サーバーから読み込まれた場合、このシナリオが発生する可能性があります。ユーザー レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

RADIUS 属性は、DAP レコード内の属性番号と属性値のペアで構成されています。

（注） RADIUS 属性について、DAP は Attribute ID = 4096 + RADIUS ID と定義します。

たとえば、RADIUS 属性「Access Hours」の Radius ID は 1 であり、したがって DAP 属性値は 4096 + 1 = 4097 となります。

RADIUS 属性「Member Of」の Radius ID は 146 であり、したがって DAP 属性値は 4096 + 146 = 4242 となります。

SAML 基準

外部サーバー（RADIUS または LDAP）に依存して認可属性を取得することなく、DAP を使用して SAML 認可およびグループポリシーの選択を設定できます。

SAML ID プロバイダーは、認証アサーションに加えて認可属性を送信するように設定できます。Threat Defense デバイスの SAML サービス プロバイダー コンポーネントは、SAML アサーションを解釈し、受信したアサーションに基づいて認可またはグループポリシーの選択を行います。アサーション属性は、管理センターで設定された DAP ルールを使用して処理されます。

グループポリシー属性は、属性名 **cisco_group_policy** を使用する必要があります。この属性は、設定されている DAP に依存しません。ただし、DAP が設定されている場合は、DAP ポリシーの一部として使用できます。

cisco_group_policy という名前の属性が受信されると、対応する値を使用して接続 group-policy が選択されます。

接続が確立されると、複数のソースからグループポリシー情報が取得され、それらが組み合わされて、接続に適用される有効な group-policy が作成されます。

DAP でサポートされるエンドポイント属性

HostScan アプリケーションで検出できるマルウェア対策およびファイアウォールのベンダーとアプリケーション、およびシスコがサポートするベンダーから利用可能なポスチャ属性のリストについては、「HostScan Antimalware and Firewall Support Charts」を参照してください [英語]。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。