

ISEポスチャリダイレクトフローとISEポスチャリダイレクトレスフローの比較

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](#)

[ISE 2.2 より前のポスチャフロー](#)

[ISE 2.2後のポスチャフロー](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[クライアントプロビジョニングの設定](#)

[ポスチャポリシーおよび条件](#)

[クライアントプロビジョニングポータルの設定](#)

[認可プロファイルおよびポリシーの設定](#)

[確認](#)

[トラブルシューティング](#)

[一般情報](#)

[一般的な問題のトラブルシューティング](#)

[SSO 関連の問題](#)

[クライアントプロビジョニングポリシーの選択のトラブルシューティング](#)

[ポスチャプロセスのトラブルシューティング](#)

はじめに

このドキュメントでは、ISE 2.2以上のバージョンでサポートされているポスチャリダイレクションレスフローと、以前のISEバージョンからサポートされているポスチャリダイレクションフローとの比較について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISE でのポスチャ フロー
- ISE でのポスチャ コンポーネントの設定
- バーチャル プライベート ネットワーク (VPN) を介したポスチャに対する適応型セキュリティ

ティアプライアンス (ASA) の設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 2.2
- ソフトウェア9.6が稼働するCisco ASA(2)

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

このドキュメントでは、Identity Service Engine(ISE)2.2で導入された新機能について説明します。この機能により、ISEはネットワークアクセスデバイス(NAD)またはISEでリダイレクションをサポートすることなく、ポスチャフローをサポートできます。

ポスチャは Cisco ISE のコア コンポーネントです。コンポーネントとしてのポスチャは、次の 3 つの主要な要素で表現できます。

1. ポリシー設定ディストリビューションおよび意思決定ポイントとしての ISE。
ISEの管理者の観点からは、ポスチャポリシー (デバイスを企業準拠としてマークするために満たす必要がある正確な条件)、クライアントプロビジョニングポリシー (どの種類のデバイスにどのエージェントソフトウェアをインストールする必要があるか)、および許可ポリシー (どの種類の権限を割り当てる必要があるか、ポスチャステータスによって異なる) を設定します。
2. ポリシー適用ポイントとしてのネットワークアクセスデバイス。
NAD側では、実際の許可制限はユーザ認証時に適用されます。ポリシー ポイントとしての ISE は、ダウンロードされた ACL (dACL)、VLAN、リダイレクト URL、リダイレクト アクセス コントロール リスト (ACL) などの認証パラメータを提供します。従来、ポスチャを実行するには、エンドポイントのポスチャステータスが決定された後にユーザを再認証するために、NADはリダイレクション (ユーザまたはエージェントソフトウェアに対して ISEノードへの接続が必要な指示) と認可変更(CoA)をサポートする必要があります。
3. データ収集およびエンドユーザとの対話のポイントとしてのエージェントソフトウェア。
Cisco ISEは、AnyConnect ISEポスチャモジュール、NACエージェント、およびWebエージェントの3種類のエージェントソフトウェアを使用します。エージェントはISEからポスチャ要件に関する情報を受信し、要件のステータスに関するレポートをISEに提供します。

 注：このドキュメントは、リダイレクトなしでポスチャを完全にサポートする唯一のモジュールであるAnyconnect ISEポスチャモジュールに基づいています。

ISE 2.2より前のフローポスチャでは、NADはユーザの認証とアクセスの制限に使用されるだけでなく、接続する必要がある特定のISEノードに関する情報をエージェントソフトウェアに提供するためにも使用されます。リダイレクトプロセスの一部として、ISEノードに関する情報がエージェントソフトウェアに返されます。

従来、NADまたはISE側でのリダイレクションのサポートは、ポスチャ実装に不可欠な要件でした。ISE 2.2では、リダイレクションをサポートする要件は、初期クライアントプロビジョニングとポスチャプロセスの両方で排除されています。

リダイレクトなしのクライアントプロビジョニング：ISE 2.2では、ポータル完全修飾ドメイン名(FQDN)を使用してクライアントプロビジョニングポータル(CPP)に直接アクセスできます。これは、スポンサーポータルまたはMyDeviceポータルへのアクセス方法に似ています。

リダイレクトなしのポスチャプロセス：CPPポータルからのエージェントインストール時に、ISEサーバに関する情報がクライアント側に保存されるため、直接通信が可能になります。

ISE 2.2 より前のポスチャ フロー

次の図に、ISE 2.2より前のAnyconnect ISEポスチャモジュールフローの段階的な説明を示します。

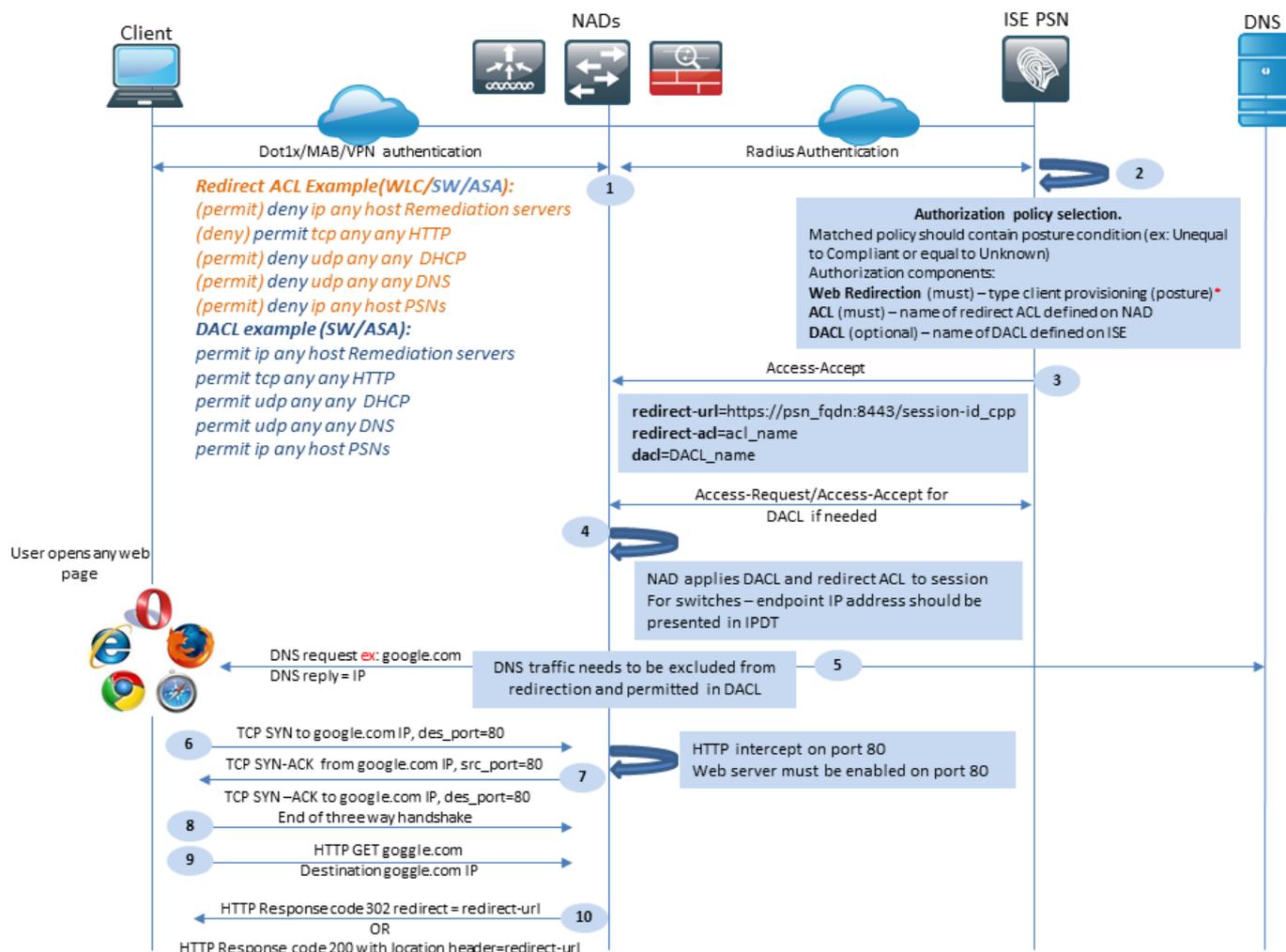


図1-1

ステップ 1：認証はフローの最初のステップであり、dot1x、MAB、またはVPNにすることができます。

ステップ 2：ISEはユーザの認証および認可ポリシーを選択する必要があります。ポスチャシナリオでは、選択した認可ポリシーにポスチャステータスへの参照が含まれている必要があります。この参照は、最初は不明であるか、該当しない必要があります。これらの両方のケースをカバーするために、ポスチャステータスが不均等に準拠している条件を使用できます。

選択した認可プロファイルには、リダイレクトに関する情報が含まれている必要があります。

- Webリダイレクション：ポスチャの場合、Webリダイレクションのタイプはクライアントプロビジョニング（ポスチャ）として指定する必要があります。
- ACL：このセクションには、NAD側で設定されているACL名を含める必要があります。このACLは、どのトラフィックがリダイレクトをバイパスする必要があり、どのトラフィックが実際にリダイレクトされる必要があるかをNADに指示するために使用されます。
- DACL：リダイレクトアクセスリストと一緒に使用できますが、DACLとリダイレクトACLはプラットフォームごとに異なる順序で処理されることに注意してください。

たとえば、ASAは常にDACLを処理してからACLをリダイレクトします。同時に、一部のスイッチプラットフォームではASAと同じ方法でトラフィックを処理し、他のスイッチプラットフォームでは最初にリダイレクトACLを処理してから、トラフィックをドロップまたは許可する必要がある場合はDACL/インターフェイスACLを確認します。

 注：認可プロファイルでWebリダイレクトオプションを有効にした後は、リダイレクトのターゲットポータルを選択する必要があります。

ステップ 3：ISEは認可属性を含むAccess-Acceptを返します。認可属性のリダイレクト URL は、ISE によって自動的に生成されます。次に、この構成要素を示します。

- 認証が実行された ISE ノードの FQDN。場合によっては、Webリダイレクションセクションで認証プロファイル設定（スタティックIP/ホスト名/FQDN）によってダイナミック FQDNを上書きすることができます。静的な値を使用する場合は、認証が処理されたのと同じISEノードを指す必要があります。ロードバランサ(LB)の場合、このFQDNはLB VIPを指すことができますが、これはLBがRADIUS接続とSSL接続を結び付けるように設定されている場合に限られます。
- Port：ポート値は、ターゲットのポータル設定から取得します。
- Session ID：この値は、ISEによってAccess-Requestに示されたCisco AVペア監査セッションIDから取得されます。値自体はNADによって動的に生成されます。
- ポータルID:ISE側のターゲットポータルのID。

ステップ 4：NADは、セッションに認可ポリシーを適用します。また、DACLが設定されている場合、認可ポリシーが適用される前にそのコンテンツが要求されます。

重要な考慮事項：

- すべてのNAD：デバイスには、リダイレクトACLとしてAccess-Acceptで受信したACLと同じ名前の、ローカルに設定されたACLが必要です。
- スイッチ：クライアントのIPアドレスは、 `show authentication session interface details` コマンドを発行して、リダイレクションとACLを正常に適用します。クライアントのIPアドレスは、IPデバイストラッキング機能(IPDT)によって学習されます。

ステップ 5：クライアントは、Webブラウザに入力されたFQDNのDNS要求を送信します。この段階で、DNSトラフィックはリダイレクトをバイパスし、正しいIPアドレスがDNSサーバから返される必要があります。

手順 6：クライアントは、DNS応答で受信したIPアドレスにTCP SYNを送信します。パケットの送信元IPアドレスはクライアントIPであり、宛先IPアドレスは要求されたリソースのIPです。クライアントのWebブラウザでダイレクトHTTPプロキシが設定されている場合を除き、宛先ポートは80です。

ステップ7:NADはクライアント要求を代行受信し、要求されたリソースIPと等しい送信元IP、クライアントIPと等しい宛先IP、および80と等しい送信元ポートを持つSYN-ACKパケットを準備します。

重要な考慮事項：

- NADには、クライアントが要求を送信するポートで実行されているHTTPサーバが必要です。デフォルトでは、ポート80です。
- クライアントがダイレクトHTTPプロキシWebサーバを使用する場合、HTTPサーバはNASのプロキシポートで実行する必要があります。このシナリオは、このドキュメントの対象範囲外です。
- NADがクライアントにローカルIPアドレスを持たない場合、サブネットSYN-ACKはNADルーティングテーブルとともに（通常は管理インターフェイス経由で）送信されます。このシナリオでは、パケットはL3インフラストラクチャ経由でルーティングされ、L3アップストリームデバイスによってクライアントに戻るようにルーティングされる必要があります。L3デバイスがステートフルファイアウォールである場合、このような非対称ルーティングには追加の例外を指定する必要があります。

ステップ 8：クライアントはACKによってTCP 3ウェイハンドシェイクを終了します。

ステップ 9：ターゲットリソースのHTTP GETがクライアントによって送信されます。

ステップ 10：NADはリダイレクトURLをHTTPコード302（ページ移動）でクライアントに返します。一部のNADでは、リダイレクトはロケーションヘッダーのHTTP 200 OKメッセージ内で返されます。

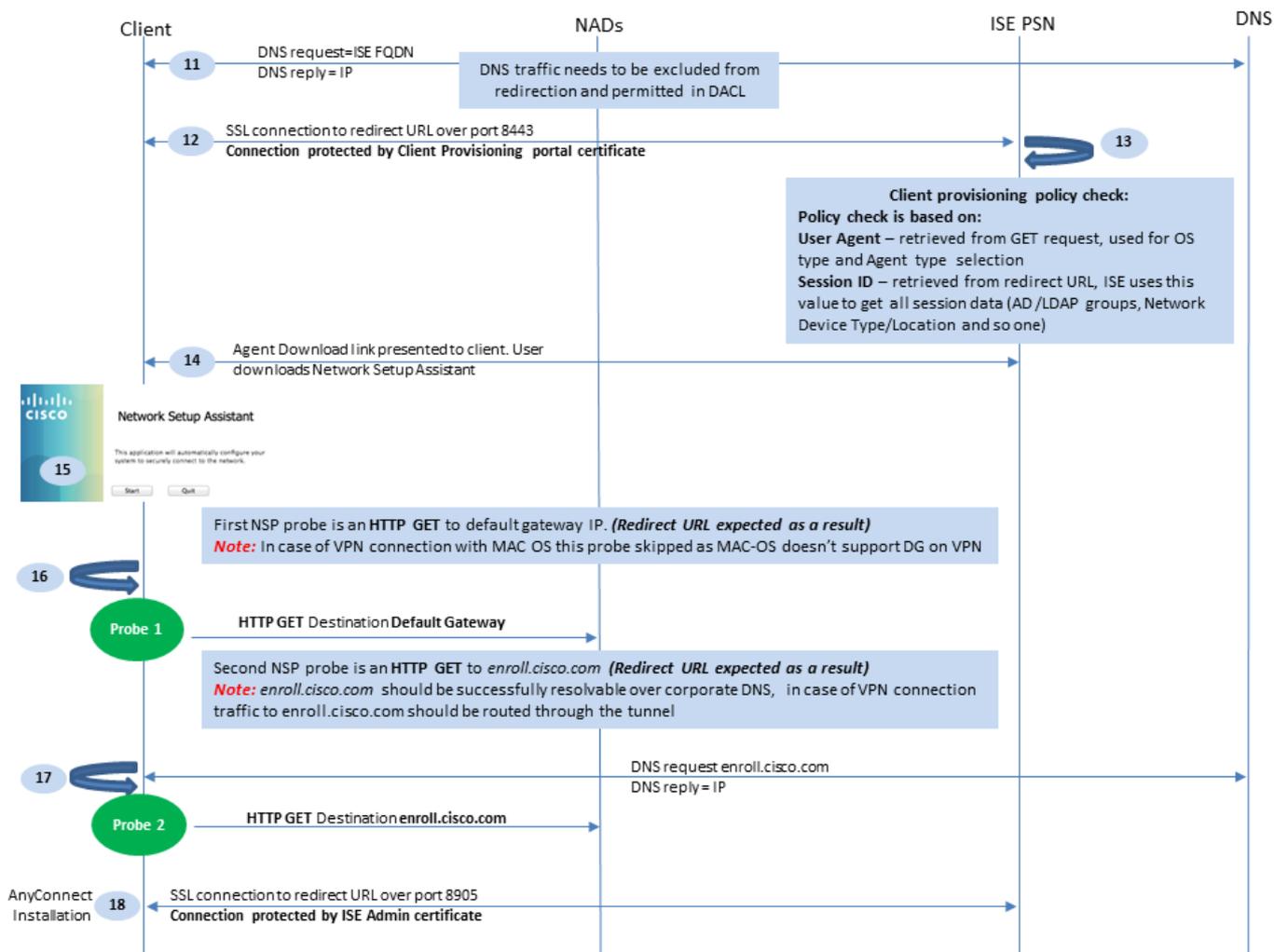


図1-2

ステップ 11クライアントは、リダイレクトURLからFQDNのDNS要求を送信します。FQDNはDNSサーバ側で解決可能である必要があります。

ステップ 12 リダイレクト URL で受け取られたポート経由の SSL 接続が確立されます (デフォルト 8443)。この接続は、ISE側からのポータル証明書によって保護されます。クライアントプロビジョニング ポータル (CPP) がユーザに表示されます。

ステップ 13 : クライアントにダウンロードオプションを提供する前に、ISEはターゲットクライアントプロビジョニング(CP)ポリシーを選択する必要があります。ブラウザユーザエージェントから検出されたクライアントのオペレーティングシステム(OS)と、CPPポリシー選択に必要なその他の情報は、認証セッション (AD/LDAPグループなど) から取得されます。ISEは、リダイレクトURLに示されたセッションIDからターゲットセッションを認識します。

ステップ 14 : Network Setup Assistant(NSA)ダウンロードリンクがクライアントに返されます。クライアントがアプリケーションをダウンロードします。

 注 : 通常、NSAはWindowsおよびAndroidのBYODフローの一部として表示されますが、このアプリケーションを使用してISEからAnyconnectまたはそのコンポーネントをインストー

 ルすることもできます。

ステップ15：ユーザがNSAアプリケーションを実行します。

ステップ 16：NSAが最初の検出プローブ（デフォルトゲートウェイへのHTTP /auth/discovery）を送信します。NSAは結果としてリダイレクトURLを予期します。

 注:MAC OSデバイス上のVPN経由の接続では、MAC OSのVPNアダプタにデフォルトゲートウェイがないため、このプローブは無視されます。

ステップ17:NSAは、最初のプローブが失敗した場合に2番目のプローブを送信します。2番目のプローブはHTTP GET /auth/discoveryです。 enroll.cisco.comを参照。このFQDNは、DNSサーバによって正常に解決できる必要があります。スプリットトンネルを使用するVPNシナリオでは、enroll.cisco.com トンネル経由でルーティングする必要があります。

ステップ 18：プローブのいずれかが成功すると、NSAはリダイレクトURLから取得した情報を使用して、ポート8905経由でSSL接続を確立します。この接続はISE管理証明書によって保護されています。この接続内で、NSAはAnyconnectをダウンロードします。

重要な考慮事項：

- ISE 2.2リリース以前は、ポート8905を介したSSL通信がポスチャの要件でした。
- 証明書の警告を回避するには、ポータル証明書と管理証明書の両方がクライアント側で信頼されている必要があります。
- マルチインターフェイスのISE導入では、G0以外のインターフェイスをシステムFQDNとは異なるFQDNにバインドできます(`ip host` CLIコマンド)。これにより、サブジェクト名(SN)/サブジェクト代替名(SAN)の検証で問題が発生する可能性があります。たとえば、クライアントがインターフェイスG1からFQDNにリダイレクトされる場合、システムFQDNは8905通信証明書のリダイレクトURLのFQDNとは異なる場合があります。このシナリオの解決策として、管理証明書のSANフィールドに追加インターフェイスのFQDNを追加するか、管理証明書にワイルドカードを使用できます。

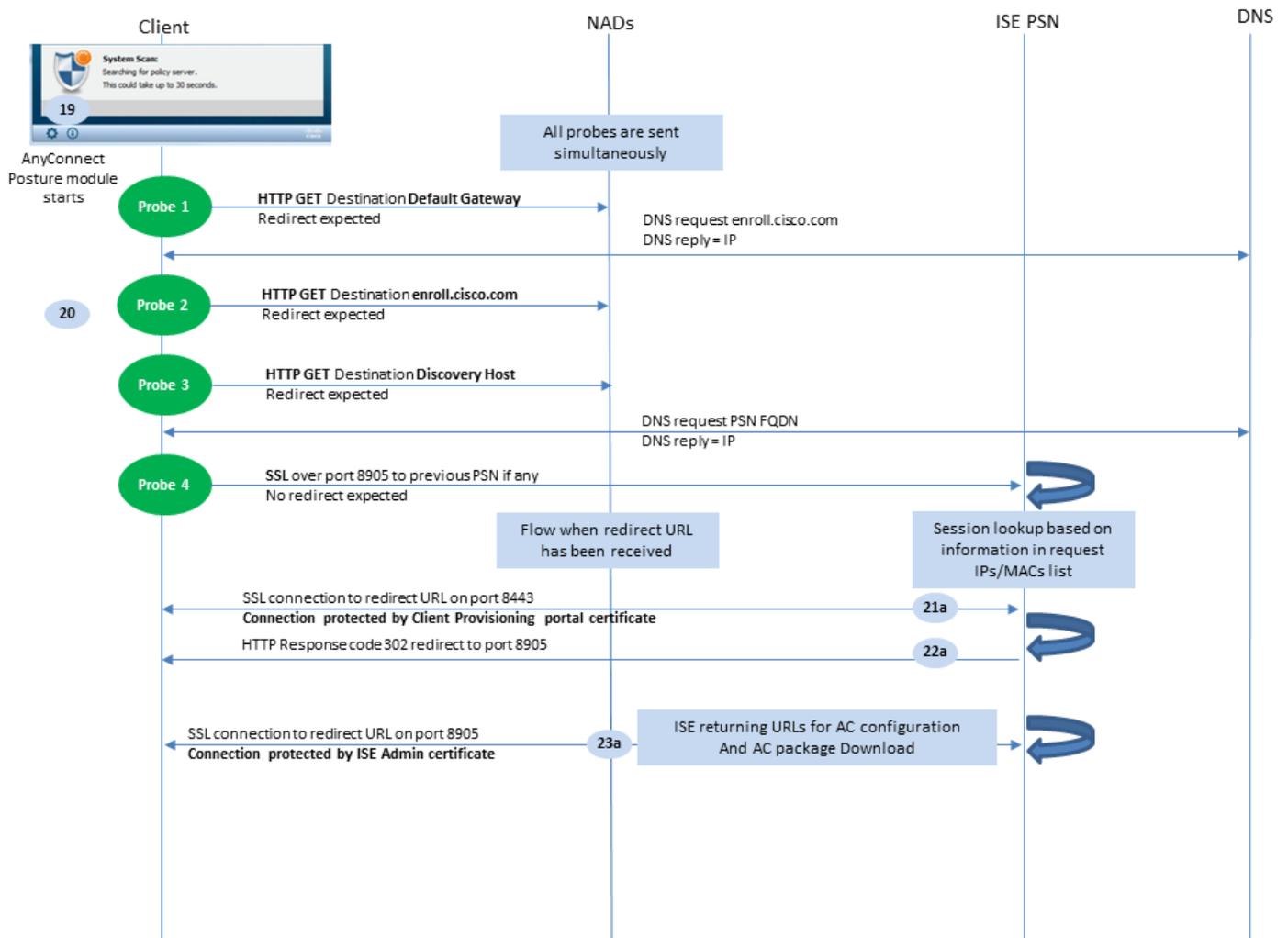


図1-3

ステップ19: Anyconnect ISEポスチャプロセスが起動します。

Anyconnect ISEポスチャモジュールは、次のいずれかの状況で起動します。

- インストール後
- デフォルトゲートウェイ値の変更後
- システムユーザログインイベントの後
- システムの電源イベントの後

ステップ 20： この段階で、Anyconnect ISEポスチャモジュールはポリシーサーバ検出を開始します。これは、Anyconnect ISEポスチャモジュールによって同時に送信される一連のプロープによって実現されます。

- プロープ1： デフォルトゲートウェイIPへのHTTP get /auth/discovery。MAC OSデバイスには、VPNアダプタ上にデフォルトゲートウェイがないことを覚えておいてください。プロープの予期される結果はリダイレクトURLです。
- プロープ2 - HTTP GET /auth/discoveryから enroll.cisco.comを参照。このFQDNは、DNSサーバによって正常に解決できる必要があります。スプリットトンネルを使用するVPNシナリオでは、 enroll.cisco.com トンネル経由でルーティングする必要があります。プロープの予期される結果はリダイレクトURLです。

- プローブ 3：検出ホストへの HTTP get /auth/discovery。Discoveryホストの値は、ACポスチャプロファイルでのインストール中にISEから返されます。プローブの予期される結果はリダイレクトURLです。
- プローブ 4：前に接続されていた PSN に対して、ポート 8905 上で HTTP GET /auth/status が SSL 経由で実行されます。この要求には、ISE側のセッションルックアップ用のクライアントIPおよびMACリストに関する情報が含まれています。この問題は、最初のポスチャ試行時には発生しません。接続はISE管理証明書によって保護されています。このプローブの結果、プローブが取得されたノードがユーザが認証されているのと同じノードである場合、ISEはセッションIDをクライアントに返すことができます。

 注：このプローブの結果、ポスチャは、状況によってはリダイレクトが機能しなくても正常に実行できます。リダイレクトなしの正常なポスチャでは、セッションを認証した現在の PSNが、以前正常に接続されたPSNと同じである必要があります。ISE 2.2よりも前のリリースでは、リダイレクトなしの正常なポスチャはルールではなく例外であることに注意してください。

次の手順では、プローブの1つの結果としてリダイレクトURLを受信した場合のポスチャプロセスについて説明します（フローは文字aでマークされています）。

ステップ 21： Anyconnect ISEポスチャモジュールは、検出フェーズで取得したURLを使用して、クライアントプロビジョニングポータルへの接続を確立します。この段階で、ISEは認証済みセッションからの情報を使用して、クライアントプロビジョニングポリシーの検証を再度行います。

ステップ 22： クライアント プロビジョニング ポリシーが検出された場合、ISE はリダイレクトをポート 8905 に返します。

ステップ 23： エージェントがポート8905経由でISEへの接続を確立します。この接続中に、ISEはポスチャプロファイル、コンプライアンスモジュール、およびAnyConnect更新のURLを返します。

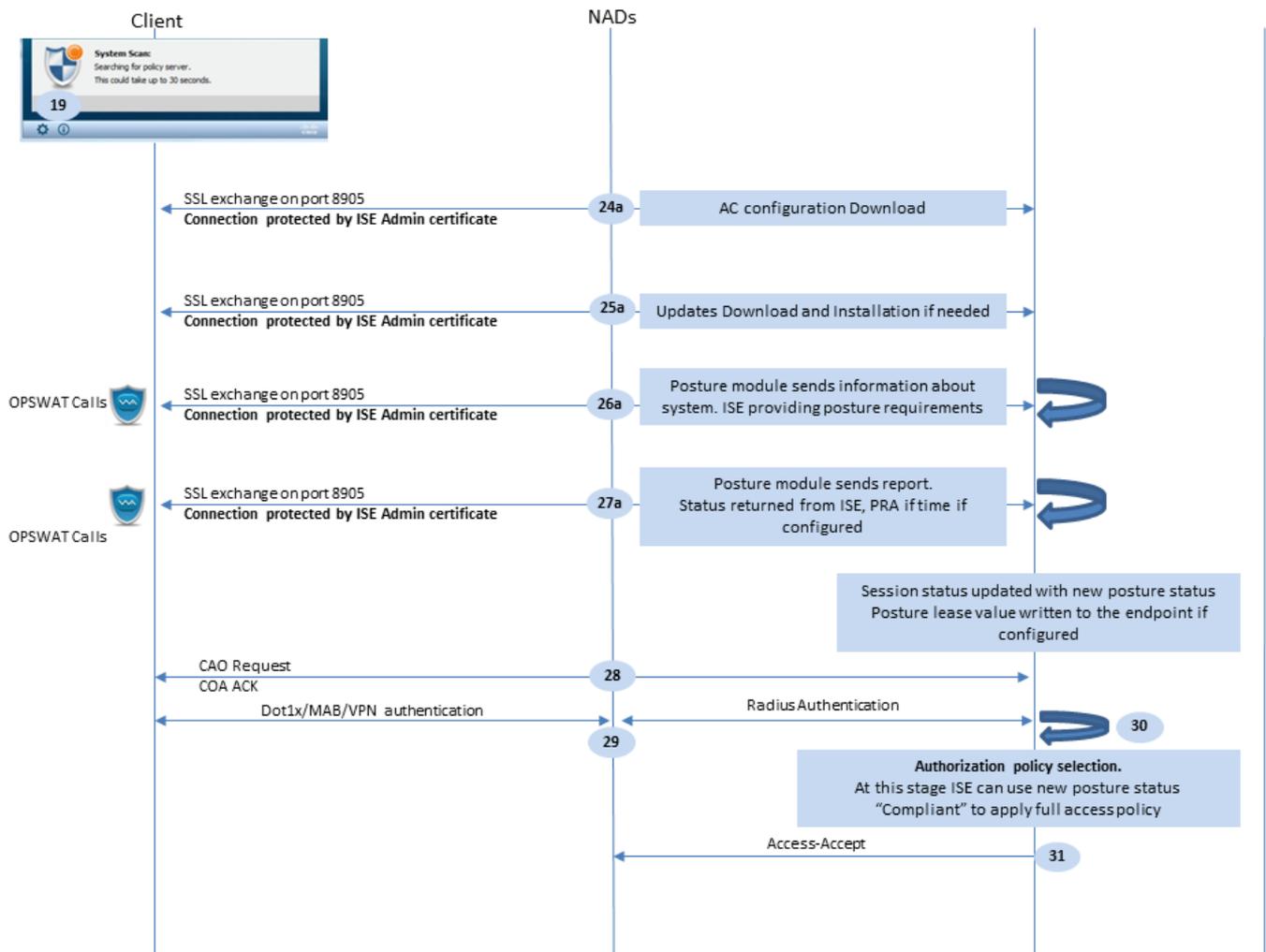


図1-4

ステップ24:AC ISEポスチャモジュール設定をISEからダウンロードします。

ステップ 25： 必要な場合はダウンロードとインストールを更新します。

ステップ 26： AC ISEポスチャモジュールは、システムに関する初期情報（OSバージョン、インストールされているセキュリティ製品、およびそれらの定義バージョンなど）を収集します。この段階で、AC ISEポスチャモジュールは、セキュリティ製品に関する情報を収集するOPSWAT APIを含みます。収集されたデータはISEに送信されます。この要求に対する応答として、ISEはポスチャ要件リストを提供します。要件リストは、ポスチャポリシー処理の結果として選択されます。正しいポリシーに一致させるため、ISEはデバイスOSのバージョン（要求内に存在）とセッションIDの値を使用して、他の必要な属性（AD/LDAPグループ）を選択します。セッションIDの値は、クライアントからも送信されます。

ステップ 27： このステップでは、クライアントはOPSWATコールと、ポスチャ要件を確認するその他のメカニズムを使用します。要件リストとそのステータスを含む最終レポートがISEに送信されます。ISEは、エンドポイントのコンプライアンスステータスに関する最終的な決定を行う必要があります。このステップでエンドポイントが非準拠としてマークされると、一連の修復アクションが返されます。準拠しているエンドポイントの場合、ISEはコンプライアンスステータスをセッションに書き込み、ポスチャリースが設定されている場合は、最後のポスチャタイムスタンプをエンドポイント属性に書き込みます。ポスチャの結果がエンドポイントに送信されま

す。ポスチャ再評価(PRA)の場合、PRAの時間はISEによってこのパケットにも入力されます。

非準拠シナリオでは、次の点を考慮に入れます。

- 一部の修復アクション (テキストメッセージの表示、リンクの修復、ファイルの修復など) は、ポスチャエージェント自体によって実行されます。
- 他の修復タイプ (AV.AS、WSUS、およびSCCM)では、ポスチャエージェントとターゲット製品間のOPSWAT API通信が必要です。このシナリオでは、ポスチャエージェントは単に修復要求を製品に送信します。修復自体は、セキュリティ製品によって直接行われます。

 注：セキュリティ製品が外部リソース (内部/外部更新サーバ) と通信する必要がある場合、この通信がリダイレクトACL/DACLで許可されていることを確認する必要があります。

ステップ28:ISEがCOA要求をNADに送信します。これにより、ユーザに対する新しい認証がトリガーされる必要があります。NADはこの要求をCOA ACKで確認する必要があります。VPNケースではCOAプッシュが使用されるため、新しい認証要求は送信されないことに注意してください。代わりに、ASAは以前の認証パラメータ (リダイレクトURL、リダイレクトACL、およびDACL) をセッションから削除し、COA要求から新しいパラメータを適用します。

ステップ29：ユーザに対する新しい認証要求。

重要な考慮事項：

- 通常、Cisco NAD COAの場合、再認証はISEによって使用され、これはNADに前のセッションIDで新しい認証要求を開始するように指示します。
- ISE側では、同じセッションID値は、以前に収集されたセッション属性を再利用する必要があります (この場合は準拠ステータス)、およびこれらの属性に基づく新しい認証プロファイルを割り当てる必要があることを示します。
- セッションIDが変更された場合、この接続は新規として扱われ、完全なポスチャプロセスが再起動されます。
- 再ポスチャを回避するためセッションidが変更されるたびに、ポスチャリースを使用できます。このシナリオでは、ポスチャステータスに関する情報はエンドポイント属性に保存され、セッションIDがtsが変更されました。

ステップ 30：ポスチャステータスに基づいて、ISE側で新しい認可ポリシーが選択されます。

ステップ 31：新しい承認属性が指定されたアクセス承認が NAD に送信されます。

次のフローは、リダイレクトURLがポスチャプローブによって取得されず (文字bでマークされている)、以前に接続されたPSNが最後のプローブによって照会された場合のシナリオを説明しています。ここで示すすべてのステップは、プローブ 4 の結果として PSN により返されるリプレイを除き、リダイレクト URL の場合とまったく同じです。このプローブが現在の認証セッションの所有者と同じPSNに到達した場合、リプレイには後でプロセスを完了するためにポスチャエージェントによって使用されるセッションID値が含まれます。以前に接続されたヘッドエンドが現在のセッションオーナーと同じでない場合、セッションルックアップは失敗し、空の応答がAC

ISEポスチャモジュールに返されます。最終的な結果として、No Policy Server Detected メッセージがエンドユーザに返されます。

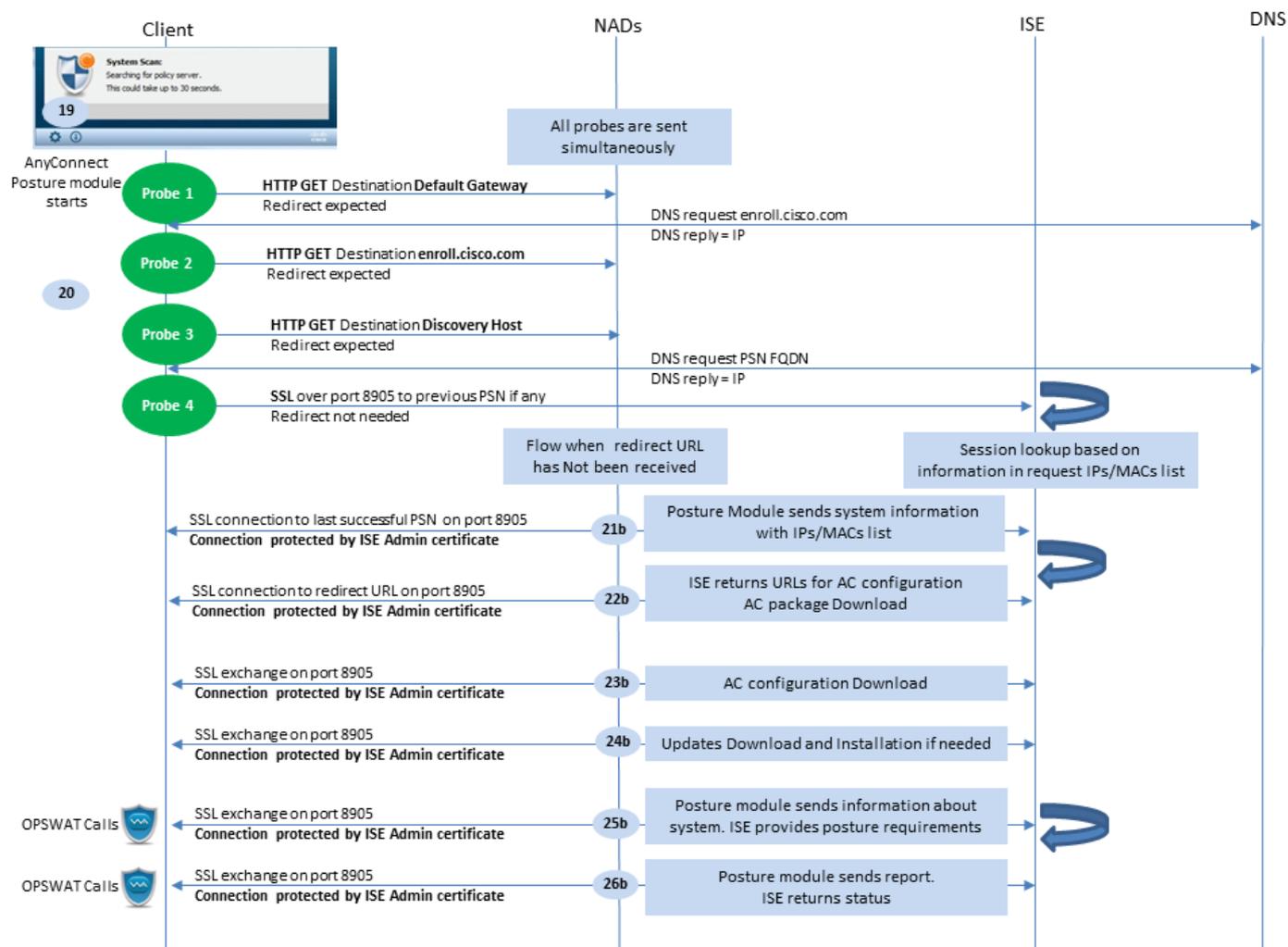


図1-5

ISE 2.2後のポスチャフロー

ISE 2.2以降のバージョンでは、リダイレクトとリダイレクトなしのフローの両方を同時にサポートします。次に、リダイレクトなしのポスチャフローの詳細な説明を示します。

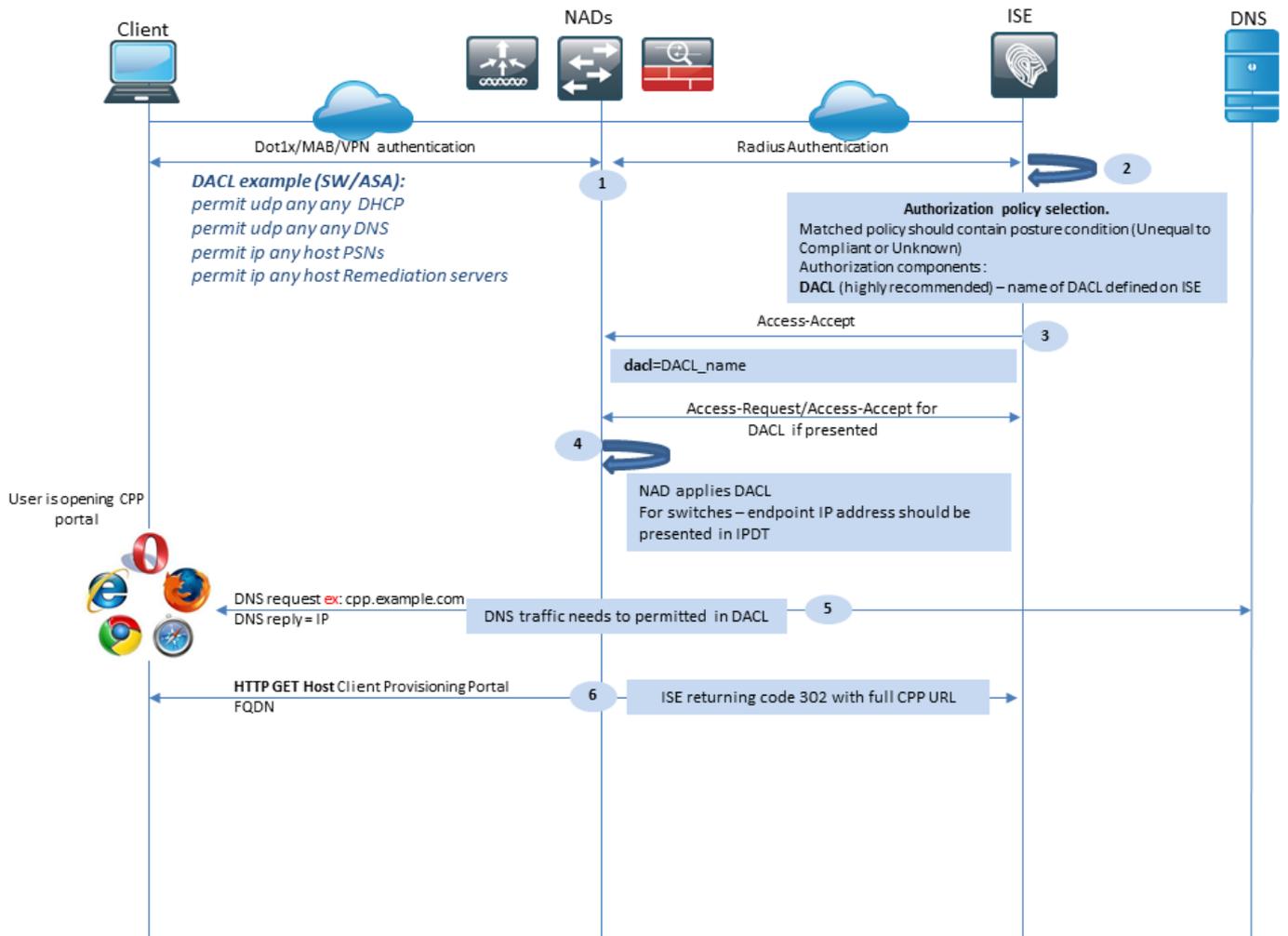


図2-1

ステップ1: 認証はフローの最初のステップです。dot1x、MAB、またはVPNを使用できます。

ステップ2: ISEはユーザの認証および認可ポリシーを選択する必要があります。ポスチャでは、シナリオで選択された認可ポリシーに、最初は不明または該当しないポスチャステータスへの参照が含まれている必要があります。これらの両方のケースをカバーするために、ポスチャステータスが不均等に準拠している条件を使用できます。リダイレクトのないポスチャの場合、認可プロファイルでWebリダイレクト設定を使用する必要はありません。ポスチャステータスが使用できない段階でユーザアクセスを制限するために、DACLまたはAirspace ACLの使用を引き続き検討できます。

ステップ3: ISEは認可属性があるアクセス承認を返します。

ステップ4: DACL名がAccess-Acceptで返された場合、NADはDACLコンテンツのダウンロードを開始し、認可プロファイルを取得後にセッションに適用します。

ステップ5: 新しいアプローチでは、リダイレクトが不可能であることを前提としているため、ユーザはクライアントプロビジョニングポータル(FQDN)を手動で入力する必要があります。CPPポータルのFQDNは、ISE側のポータル設定で定義する必要があります。DNSサーバの観点からは、AレコードはPSNルールが有効になっているISEサーバを指す必要があります。

手順 6 : クライアントはHTTPを送信してクライアントプロビジョニングポータルFQDNに到達します。この要求はISE側で解析され、完全なポータルURLがクライアントに返されます。

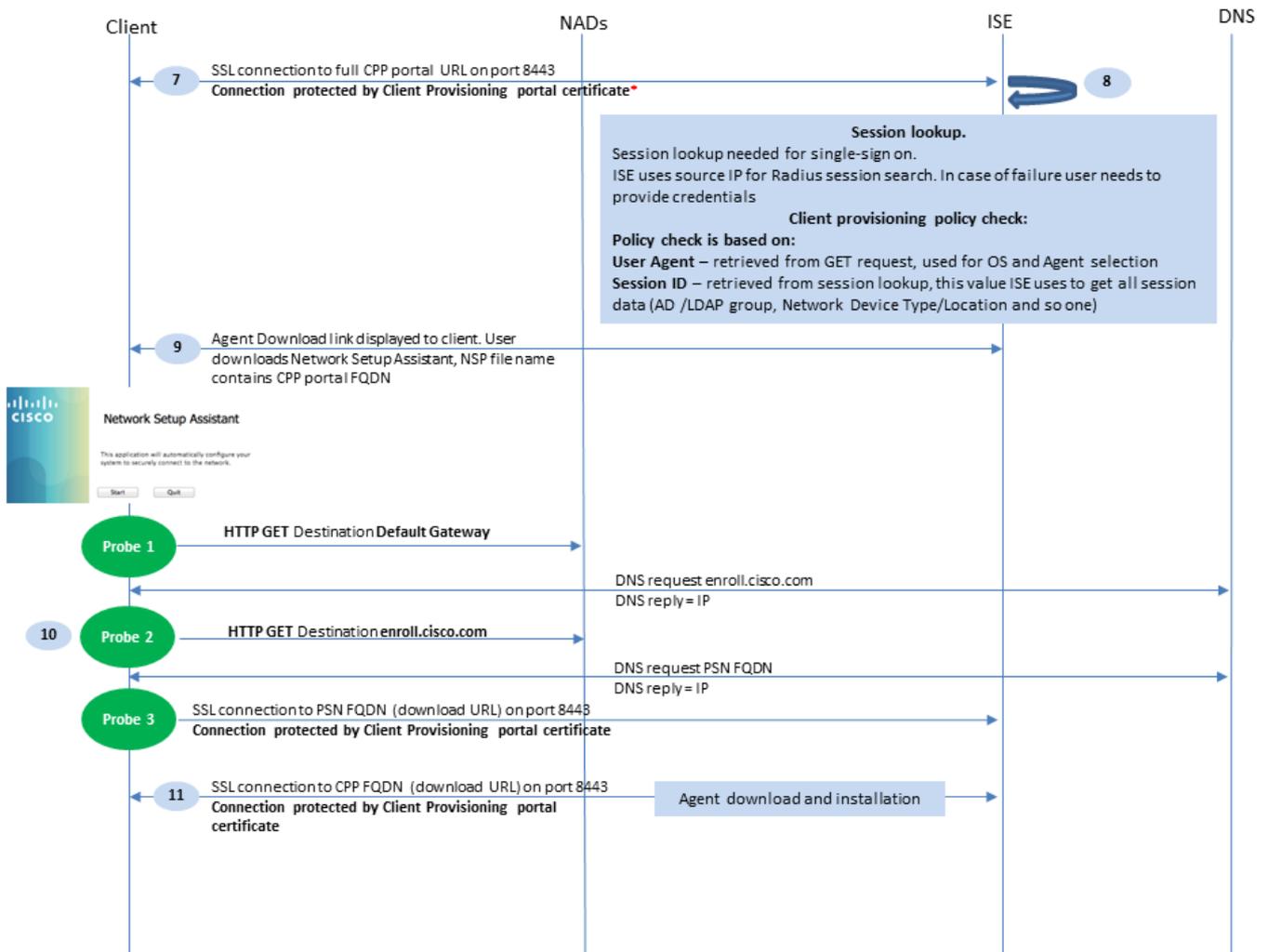


図2-2

ステップ 7 : リダイレクト URL で受け取られたポート経由の SSL 接続が確立されます (デフォルト 8443)。この接続は、ISE側からのポータル証明書によって保護されます。クライアントプロビジョニングポータル(CPP)がユーザに表示されます。

ステップ 8 : このステップでは、ISEで次の2つのイベントが発生します。

- シングルサインオン(SSO):ISEは以前の正常な認証の検索を試行します。ISEは、ライブ RADIUSセッションの検索フィルタとしてパケットの送信元IPアドレスを使用します。

注 : セッションは、パケットの送信元IPとセッションのフレームIPアドレスの一致に基づいて取得されます。フレーム化されたIPアドレスは通常、ISEによって暫定アカウントアップデートから取得されるため、NAD側でアカウントリングを有効にする必要があります。また、SSOはセッションを所有するノードでのみ可能であることにも注意してください。たとえば、セッションがPSN 1で認証されていても、FQDN自体がPSN2を指している場合、SSOメカニズムは失敗します。

- クライアントプロビジョニングポリシーのルックアップ：SSOが成功した場合、ISEは認証済みセッションからのデータとクライアントブラウザからのユーザエージェントを使用できます。SSOが失敗した場合、ユーザはクレデンシャルを提供する必要があります。ユーザ認証情報は、内部および外部IDストア（AD/LDAP/内部グループ）から取得された後、クライアントプロビジョニングポリシーチェックに使用できます。

 注: Cisco Bug ID [CSCvd11574](#)が原因で、外部ユーザが外部IDストア設定で追加された複数のAD/LDAPグループのメンバーである場合、非SSOケースに対するクライアントプロビジョニングポリシー選択時にエラーが表示される場合があります。上記の不具合はISE 2.3 FCSから始まる修正であり、修正ではEQUALではなくADグループを含む条件でCONTAINSを使用する必要があります。

ステップ 9： クライアントプロビジョニングポリシーの選択後、ISEはエージェントのダウンロードURLをユーザに表示します。NSAのダウンロードをクリックすると、アプリケーションがユーザにプッシュされます。NSAファイル名には、CPPポータルFQDNが含まれます。

ステップ10： このステップで、NSAはプローブを実行してISEへの接続を確立します。2つのプローブは従来のプローブであり、3つ目のプローブはURLリダイレクションを使用しない環境でISE検出を行えるように設計されています。

- NSAが最初の検出プローブ（デフォルトゲートウェイへのHTTP /auth/discovery）を送信します。NSAは結果としてリダイレクトURLを予期します。
- NSAは、最初のプローブが失敗すると2番目のプローブを送信します。2番目のプローブはHTTP GET /auth/discoveryです。 [enroll.cisco.com](#)を参照。このFQDNは、DNSサーバによって正常に解決できる必要があります。スプリットトンネルを使用するVPNシナリオでは、[enroll.cisco.com](#) トンネル経由でルーティングする必要があります。
- NSAは、3番目のプローブをCPPポータルポート経由でクライアントプロビジョニングポータルFQDNに送信します。この要求には、ISEが提供する必要があるリソースを識別できるようにするポータルセッションIDに関する情報が含まれます。

ステップ 11 NSAはAnyconnectまたは特定のモジュールをダウンロードします。ダウンロードプロセスは、クライアントプロビジョニングポータルポートを介して実行されます。

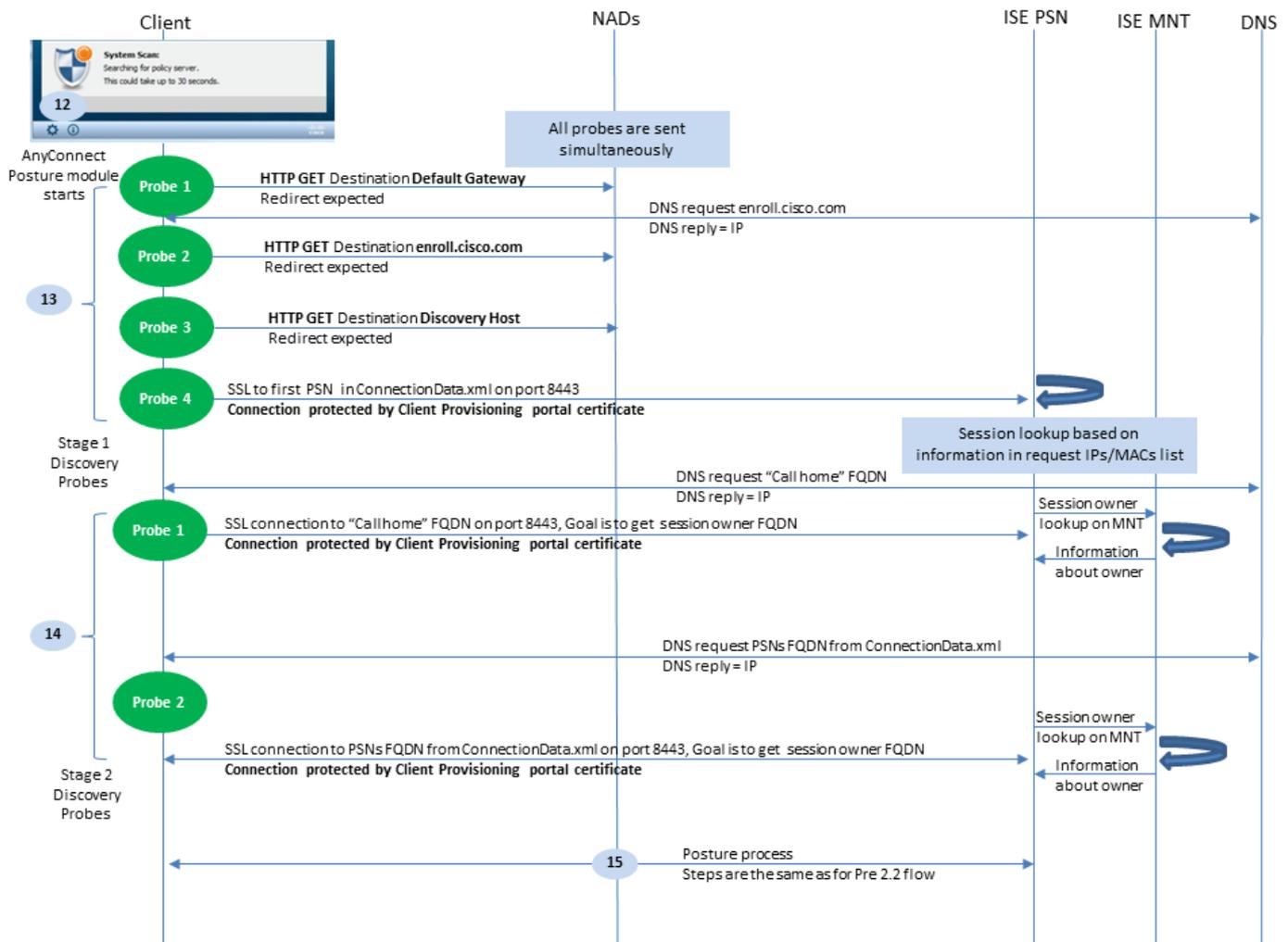


図2-3

ステップ 12 ISE 2.2では、ポスタチャプロセスは2つの段階に分かれています。第1段階には、URLリダイレクトに依存する導入との下位互換性をサポートする従来のポスタチャディスカバリプロブのセットが含まれます。

ステップ 13：第1段階には、従来のポスタチャディスカバリプロブがすべて含まれます。プロブの詳細については、ISE 2.2より前のポスタチャフローのステップ20を確認してください。

手順14：第2段階には、AC ISEポスタチャモジュールが、リダイレクションがサポートされていない環境でセッションが認証されるPSNへの接続を確立できるようにする2つのディスカバリプロブが含まれています。第2段階では、すべてのプロブは連続しています。

- プロブ1：最初のプロブ時に、AC ISEポスタチャモジュールは「Call Homeリスト」からのIP/FQDNとの確立を試行します。プロブのターゲットのリストは、ISE側のACポスタチャプロファイルで設定する必要があります。IP/FQDNはカンマで区切って定義できます。コロンの使用して、各Call Home宛先のポート番号を定義できます。このポートは、クライアントプロビジョニングポータルが実行されるポートと同じである必要があります。Call Homeサーバに関するクライアント側の情報は、ISEPostureCFG.xmlこのファイルは次のフォルダにあります。 C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\を参照。Call Homeターゲットがセッションを所有していない場合は、この段階で所有者を検索する必要があります。AC ISEポスタチャモジュールは、特別なターゲットURLを使用して所有者

検索を開始するようにISEに指示します。 /auth/ng-discovery request.また、クライアントIPとMACのリストも含まれています。このメッセージがPSNセッションで受信されると、最初にローカルでルックアップが行われます (このルックアップでは、AC ISEポスチャモジュールによって送信された要求からのIPとMACの両方が使用されます)。セッションが見つからない場合、PSNはMNTノードクエリを開始します。この要求にはMACリストのみが含まれているため、所有者のFQDNはMNTから取得する必要があります。その後、PSNは所有者のFQDNをクライアントに返します。クライアントからの次の要求は、URLとIPおよびMACのリストにauth/statusが含まれるセッションオーナーFQDNに送信されます。

- プローブ2：この段階で、AC ISEポスチャモジュールは ConnectionData.xml を参照。このファイルは、 C:\Users\

\\AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\

を参照。AC ISEポスチャモジュールは、最初のポスチャ試行後にこのファイルを作成します。このファイルには、ISE PSN FQDNのリストが含まれています。リストの内容は、次の接続試行時に動的に更新できます。このプローブの最終目標は、現在のセッションオーナーのFQDNを取得することです。実装はプローブ1と同じですが、プローブの宛先の選択が異なります。

デバイスが複数のユーザによって使用される場合、ファイル自体は現在のユーザのフォルダに置かれます。別のユーザはこのファイルの情報を使用できません。これにより、Call Homeのターゲットが指定されていない場合、リダイレクトのない環境で鶏と卵の問題が発生する可能性があります。

ステップ 15：セッションオーナーに関する情報を取得すると、後続のすべての手順はISE 2.2より前のフローと同じになります。

設定

このドキュメントでは、ASA v はネットワーク アクセス デバイスとして使用されます。すべてのテストは、VPN 経由でポスチャを使用して実施されます。VPN経由のポスチャをサポートするためのASA設定は、このドキュメントの範囲外です。詳細については、『[ASAバージョン9.2.1 VPNポスチャとISEの設定例](#)』を参照してください。

 注:VPNユーザを使用した導入では、リダイレクトベースのポスチャを設定することを推奨します。callhomelistの設定は推奨されません。非vpnベースのすべてのユーザに対して、ポスチャが設定されているPSNと通信しないようにDACLが適用されていることを確認します。

ネットワーク図

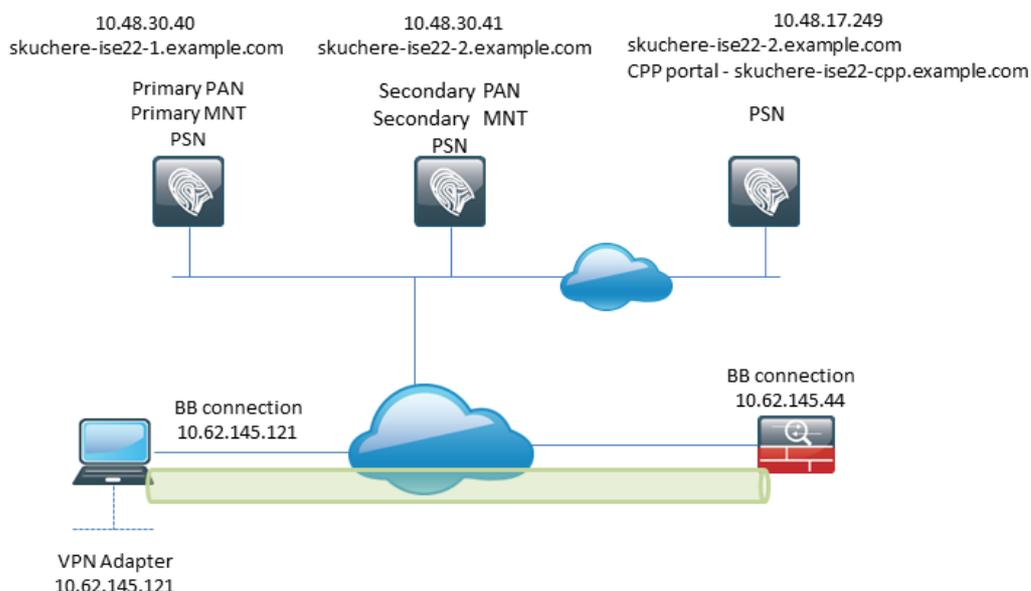


図3-1

このトポロジはテストで使用されます。ASAでは、NAT機能により、クライアントプロビジョニングポータル(SSOメカニズム)がPSN側で失敗した場合のシナリオを簡単にシミュレートできません。VPN上の通常のポスチャフローの場合、NATは通常、ユーザが企業ネットワークに入るときにVPN IPに対して強制されないため、SSOは正常に機能する必要があります。

コンフィギュレーション

クライアントプロビジョニングの設定

Anyconnectの設定を準備する手順は次のとおりです。

ステップ 1 : Anyconnectパッケージのダウンロード。Anyconnect パッケージ自体は ISE からの直接ダウンロードには使用できないので、開始する前に AC が PC 上で使用可能であることを確認してください。次のリンクはACダウンロードに使用できます。

<https://www.cisco.com/site/us/en/products/security/secure-client/index.html> にアクセスしてください。このドキュメントでは、 anyconnect-win-4.4.00243-webdeploy-k9.pkg パッケージが使用されます。

ステップ 2 : ACパッケージをISEにアップロードするには、 Policy > Policy Elements > Results > Client Provisioning > Resources クリックして Addを参照。ローカルディスクからAgent resourcesを選択します。新しいウィンドウで、 Cisco Provided Packages、 クリック browse PCのACパッケージを選択します。

Agent Resources From Local Disk

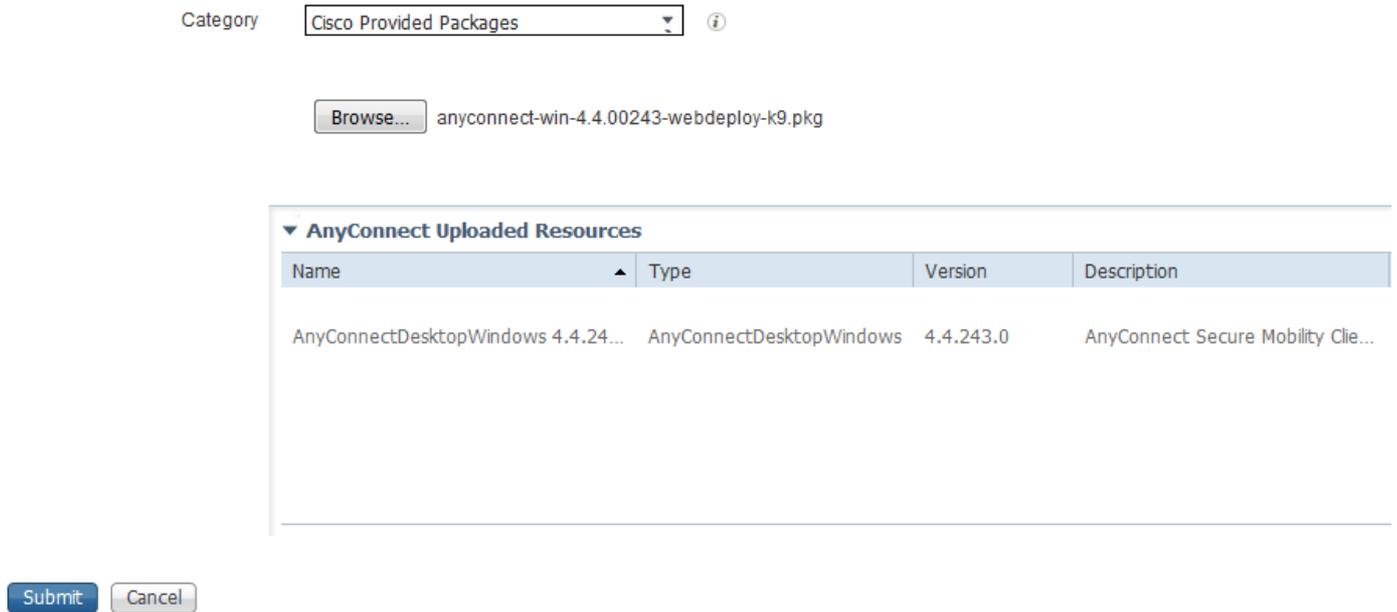


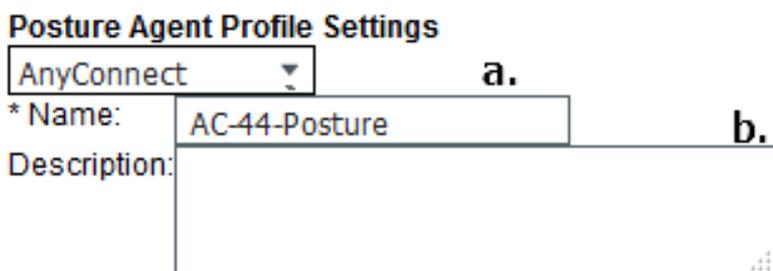
図3-2

クリック **Submit** をクリックしてインポートを完了します。

ステップ 3 : コンプライアンスモジュールをISEにアップロードする必要があります。同じページで、 **Add** を選択し、 **Agent resources from Cisco site** を参照。 リソースリストで、コンプライアンスモジュールを確認する必要があります。このドキュメントでは、 **AnyConnectComplianceModuleWindows 4.2.508.0** コンプライアンスモジュールが使用されます。

ステップ 4 : ここで、ACポスタチャプロファイルを作成する必要があります。クリック **Add** を選択し、 **NAC agent or Anyconnect posture profile** を参照。

ISE Posture Agent Profile Settings > New Profile



Agent Behavior

図3-3

- プロファイルのタイプを選択します。このシナリオではAnyConnectを使用する必要があります

ます。

- プロファイル名を指定します。に移動します。 Posture Protocol セクションを参照してください。

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	<input type="text" value="120"/> secs	
Discovery host	<input type="text"/>	
* Server name rules	<input type="text" value="*"/> a.	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	<input type="text" value="skuchere-ise22-2.examp"/> b.	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPAddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

図3-4

- Specify the Server Name Rules このフィールドを空にすることはできません。このフィールドには、AC ISE ポスチャモジュールの接続を適切な名前空間からPSNに制限する、ワイルドカードを使用したFQDNを含めることができます。いずれかのFQDNを許可する必要がある場合は、星を付けます。
- ここで指定された名前と IP は、ポスチャ ディスカバリの第 2 段階で使用されます。名前はカンマで区切ることができます。また、コロンを使用してFQDN/IPの後にポート番号を追加することもできます。GPOまたはその他のソフトウェアプロビジョニングシステム(PSN)を使用して (ISEクライアントプロビジョニングポータルからではなく) アウトオブバンドで導入されたACでは、Call Homeアドレスの存在が不可欠になります。これは、ISE PSNに正常に到達できる1つのプローブのみであるためです。つまり、アウトオブバンドACプロビジョニングの場合、管理者はACプロファイルエディタを使用してAC ISEポスチャプロファイルを作成し、ACのインストールとともにこのファイルをプロビジョニングする必要があります。

 注:Call Homeアドレスの存在はマルチユーザPCにとって重要であることに注意してください。ISE 2.2以降のポスチャフローのステップ14を確認します。

ステップ 5 : AC 設定を作成します。移動先 Policy > Policy Elements > Results > Client Provisioning > Resources、
クリック Addを選択し、 AnyConnect Configurationを参照。

* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0 a.

* Configuration Name: AC-44-CCO b.

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 4.2.508.0 c.

Notes

AnyConnect Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Umbrella Roaming Security
- Start Before Logon
- Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC-44-Posture d.

図3-5

- ACパッケージを選択します。
- AC 設定名を入力します。
- コンプライアンスモジュールのバージョンを選択します。
- ドロップダウンリストからACポスチャ設定プロファイルを選択します。

手順 6：クライアントプロビジョニングポリシーを設定します。移動先 Policy > Client Provisioning を参照。初期設定の場合は、デフォルトで表示されるポリシーに空の値を入力できます。既存のポスチャ設定にポリシーを追加する必要がある場合は、再利用できるポリシーに移動し、Duplicate Above または Duplicate Below を参照。まったく新しいポリシーを作成することもできます。

このドキュメントで使用されているポリシーの例を次に示します。

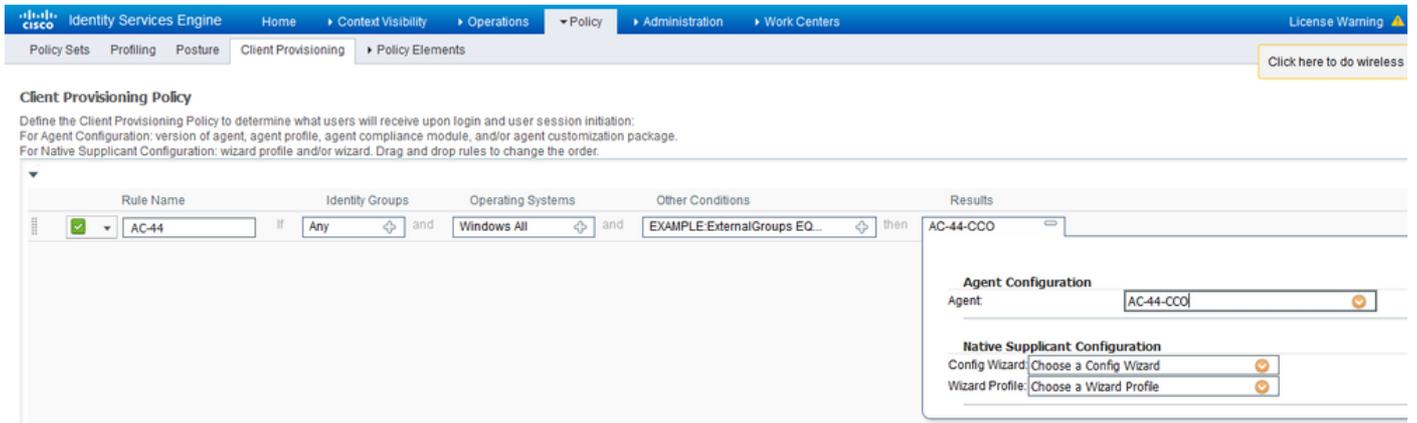


図3-6

結果セクションでAC設定を選択します。SSO が失敗した場合には、ISE はポータルへのログインの属性しか持つことができません。これらの属性は、内部および外部IDストアからユーザーに関して取得できる情報に限定されます。このドキュメントでは、ADグループはクライアントプロビジョニングポリシーの条件として使用されます。

ポスチャ ポリシーおよび条件

簡単なポスチャチェックが使用されます。ISEは、エンドデバイス側でWindow Defenderサービスのステータスを確認するように設定されています。実際のシナリオはもっと複雑になる可能性があります、一般的な設定手順は同じです。

ステップ 1: ポスチャ条件を作成します。ポスチャ条件は、 Policy > Policy Elements > Conditions > Posture を参照。ポスチャ条件のタイプを選択します。 Windows Defenderサービスが実行されているかどうかを確認する必要があるサービス条件の例を次に示します。

Service Conditions List > WinDefend

Service Condition

* Name	<input type="text" value="WinDefend"/>
Description	<input type="text"/>
* Operating Systems	<input type="text" value="Windows All"/>
Compliance Module	Any version
* Service Name	<input type="text" value="WinDefend"/>
Service Operator	<input type="text" value="Running"/>

図3-7

ステップ 2：ポスチャ要件の設定。移動先 [Policy > Policy Elements > Results > Posture > Requirements](#) を参照。次に、Windows Defender チェックの例を示します。



図3-8

新しい要件でポスチャ条件を選択し、修復アクションを指定します。

ステップ 3：ポスチャポリシーの設定移動先 [Policy > Posture](#) を参照。このドキュメントで使用するポリシーの例を次に示します。ポリシーには必須として割り当てられた Windows Defender の要件があり、条件として外部 AD グループ名のみが含まれています。

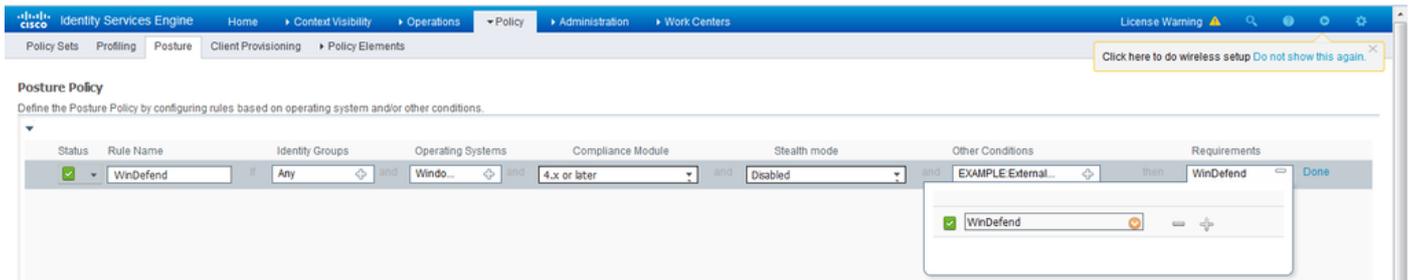
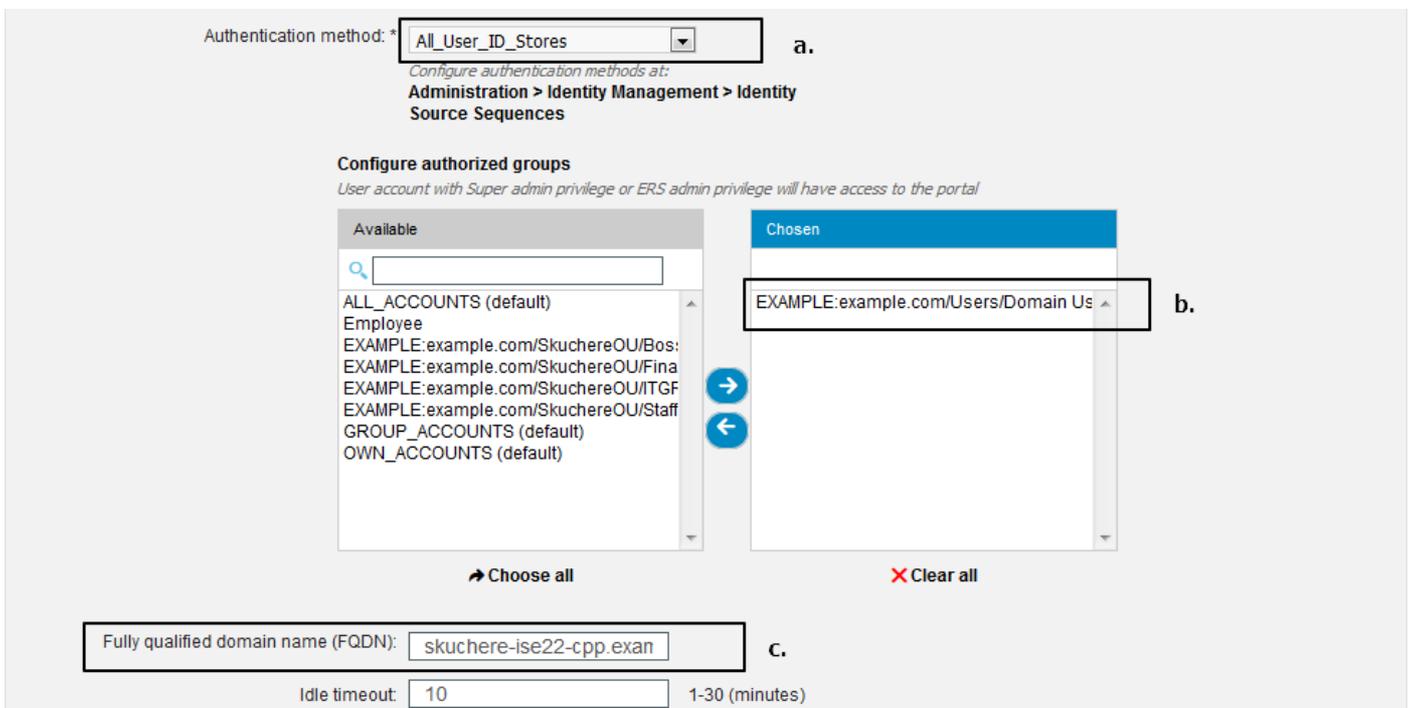


図3-9

クライアントプロビジョニングポータルの設定

リダイレクトなしのポスチャでは、クライアントプロビジョニングポータルの設定を編集する必要があります。移動先 Administration > Device Portal Management > Client Provisioning デフォルトのポータルを使用することも、独自のポータルを作成することもできます。同じポータルを、リダイレクトの有無にかかわらず両方の姿勢に使用できます。



図表3-10

リダイレクト以外のシナリオでは、ポータル設定で次の設定を編集する必要があります。

- [認証]で、SSOがユーザーのセッションを見つけられない場合に使用する必要があるIDソースシーケンスを指定します。
- 選択したIDソースシーケンスに従って、使用可能なグループのリストが読み込まれます。この時点で、ポータルログインが許可されているグループを選択する必要があります。
- クライアントプロビジョニングポータルからACを展開する必要があるシナリオでは、クライアントプロビジョニングポータルのFQDNを指定する必要があります。このFQDNは、ISE PSN IPに解決可能である必要があります。最初の接続試行時に、WebブラウザでFQDNを指定するようにユーザーに指示する必要があります。

認可プロファイルおよびポリシーの設定

ポストチャステータスが使用できない場合のクライアントの初期アクセスを制限する必要があります。これは複数の方法で実現できます。

- DACLの割り当て：アクセス制限フェーズでは、DACLをユーザに割り当ててアクセスを制限できます。このアプローチは、シスコ ネットワーク アクセス デバイスに使用できます。
- VLAN割り当て：ポストチャが成功する前に、ユーザを制限付きVLANに配置できます。このアプローチは、ほぼすべてのNADベンダーで適切に機能する必要があります。
- Radius フィルタ ID：この属性により、NAD でローカルに定義した ACL を、ポストチャステータスが不明なユーザに割り当てることができます。これは標準のRFC属性であるため、このアプローチはすべてのNADベンダーに適している必要があります。

ステップ 1：DACLを設定します。この例は ASA に基づいているため、NAD DACL を使用できません。実際のシナリオでは、可能なオプションとしてVLANまたはフィルタIDを考慮する必要があります。

DACLを作成するには、 Policy > Policy Elements > Results > Authorization > Downloadable ACLs クリックして Addを参照。

不明なポストチャ状態の間、少なくとも次の権限を提供する必要があります。

- DNS トラフィック
- DHCP トラフィック
- ISE PSN (ポート80および443) へのトラフィック。ポータルは友好的なFQDNを開くことができます。CPポータルが実行されているポートは、デフォルトで8443で、下位互換性のためにポートは8905です)。
- 必要な場合、修復サーバへのトラフィック

これは修復サーバなしの DACL の例です。

[Downloadable ACL List > New Downloadable ACL](#)

Downloadable ACL

* Name

Description

* DACL Content

```
1 permit udp any any eq 53
2 permit udp any any eq bootps
3 permit tcp any host 10.48.30.40 eq 80
4 permit tcp any host 10.48.30.40 eq 443
5 permit tcp any host 10.48.30.40 eq 8443
6 permit tcp any host 10.48.30.40 eq 8905
7 permit tcp any host 10.48.30.41 eq 80
8 permit tcp any host 10.48.30.41 eq 443
9 permit tcp any host 10.48.30.41 eq 8443
10 permit tcp any host 10.48.30.41 eq 8905
```

▶ [Check DACL Syntax](#)

図表3-11

ステップ 2：許可プロファイルを設定します。

通常どおり、ポスチャには 2 つの認可プロファイルが必要です。最初のプロファイルには、任意の種類のネットワークアクセス制限（この例で使用するDACLを持つプロファイル）が含まれている必要があります。このプロファイルは、ポスチャステータスが準拠に等しくない認証に適用できません。2番目の認可プロファイルには許可アクセスだけを含めることができ、ポスチャステータスがコンプライアンスに等しいセッションに適用できます。

許可プロファイルを作成するには、次の手順に従います。 Policy > Policy Elements > Results > Authorization > Authorization Profiles を参照。

制限付きアクセスプロファイルの例：

Authorization Profiles > VPN-No-Redirect-Unknown

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ Common Tasks

DACL Name

図表3-12

この例では、ポスチャステータスチェックが成功した後、デフォルトのISEプロファイル PermitAccessがセッションに使用されます。

ステップ 3：許可ポリシーを設定します。この手順では、2つの認可ポリシーを作成する必要があります。1つ目は、不明なポスチャステータスを持つ初期認証要求を照合する方法で、2つ目は、正常なポスチャプロセスの後にフルアクセスを割り当てる方法です。

この場合の単純な認可ポリシーの例を次に示します。

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Posture-Compliant	if (Session:PostureStatus EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then PermitAccess
✓	Posture-Unknown-No-Redirect	if (Session:PostureStatus NOT_EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then VPN-No-Redirect-Unknown
✓	Default	if no matches, then	DenyAccess

図表3-13

認証ポリシーの設定はこのドキュメントの一部ではありませんが、認証ポリシーの処理が成功する前に、認証が実行される必要があることに注意してください。

確認

フローの基本的な検証は、次の3つの主要な手順で構成できます。

ステップ 1：認証フローの検証。

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address
Feb 23, 2017 06:00:07.028 PM	✓			Identity	Endpoint ID	Endpoint Prof	Authenticator	Authorization	Authorization Profiles	IP Address
Feb 23, 2017 06:00:07.028 PM	✓			e.	10.62.145.95				PermitAccess	
Feb 23, 2017 06:00:04.368 PM	ⓘ		0	d. user1	00:0B:7F:D0:F8:F4	Windows7...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	172.16.31.12
Feb 23, 2017 05:59:04.750 PM	✓			c. user1						
Feb 23, 2017 05:44:57.921 PM	✓			b. #ACSACL#IP-VPN-No-Redi...						
Feb 23, 2017 05:44:57.680 PM	✓			a. user1	00:0B:7F:D0:F8:F4	Windows7...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	

図4-1

1. 初期認証。この手順では、認可プロファイルが適用されている検証を調べることができます。予期しない認可プロファイルが適用された場合は、詳細な認証レポートを調査します。このレポートは、[詳細]列の虫眼鏡アイコンをクリックすると開きます。詳細な認証レポートの属性を、照合する予定の認可ポリシーの条件と比較できます。
2. DACL ダウンロード イベント。この文字列は、初期認証用に選択された認可プロファイルにDACL名が含まれている場合にのみ表示されます。

3. ポータル認証：フローのこの手順は、SSOメカニズムがユーザセッションを見つけられなかったことを示します。複数の原因が考えられます。
 - NADがアカウントिंगメッセージを送信するように設定されていないか、フレーム化されたIPアドレスがメッセージ内に存在しません
 - CPPポータルのFQDNは、初期認証が処理されたノードとは異なるISEノードのIPに解決されています
 - クライアントはNATの背後にあります
4. セッションデータの変更。この特定の例では、セッションの状態がUnknownからCompliantに変更されています。
5. ネットワークアクセスデバイスへのCOA。このCOAは、NAD側から新しい認証をプッシュし、ISE側で新しい認可ポリシーを割り当てるために成功する必要があります。COAが失敗した場合は、詳細レポートを開いて原因を調査できます。COAの最も一般的な問題は次のとおりです。
 - COAタイムアウト：この場合、要求を送信したPSNがNAD側のCOAクライアントとして設定されていないか、COA要求が途中でドロップされています。
 - COA 否定 ACK：COA は NAD に受け取られましたが、何らかの理由で COA 操作を確認できなかったことを示します。このシナリオでは、詳細レポートに詳細な説明が含まれている必要があります。

この例ではASAがNADとして使用されているため、ユーザに対する後続の認証要求を確認できません。これは、VPNサービスの中断を回避するためにISEがASAにCOAプッシュを使用するためです。このようなシナリオでは、COA自体に新しい認可パラメータが含まれているため、再認証は必要ありません。

ステップ2：クライアントプロビジョニングポリシーの選択の検証：このために、ユーザに適用されたクライアントプロビジョニングポリシーを理解するのに役立つレポートをISEで実行できます。

移動先 Operations > Reports Endpoint and Users > Client Provisioning 必要な日付のレポートを実行します。

Client Provisioning ⓘ
From 2017-02-04 00:00:00.0 to 2017-03-06 21:06:33.980

+ My Reports | Export To | Schedule

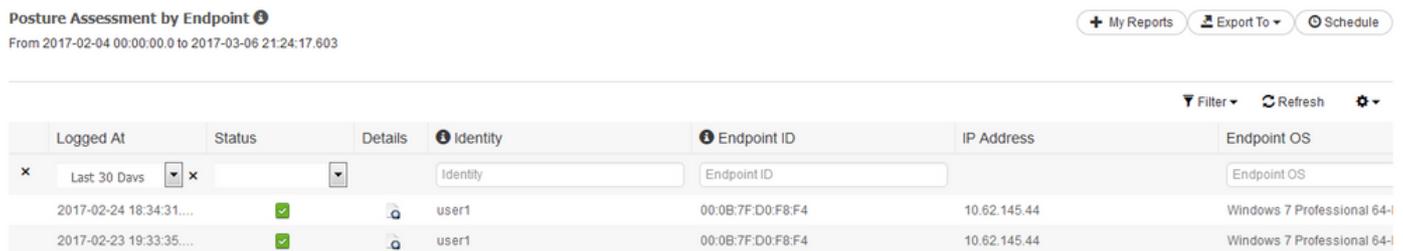
Logged At	Server	Event	Identity	Client Provisioning Policy Matched	Failure Reason
2017-02-24 18:33:46...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 18:46:42...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 17:59:07...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	

図4-2

このレポートでは、選択されたクライアントプロビジョニングポリシーを確認できます。また、障害が発生した場合は、 Failure Reason カラム。

ステップ3：ポスチャレポートの検証：に移動します。 Operations > Reports Endpoint and Users > Posture

Assessment by Endpointを参照。



The screenshot shows the 'Posture Assessment by Endpoint' interface. At the top, it displays the title and a time range: 'From 2017-02-04 00:00:00.0 to 2017-03-06 21:24:17.603'. There are buttons for '+ My Reports', 'Export To', and 'Schedule'. Below the header, there is a table with columns: 'Logged At', 'Status', 'Details', 'Identity', 'Endpoint ID', 'IP Address', and 'Endpoint OS'. The table contains two rows of data, both with a green checkmark in the 'Status' column and 'user1' in the 'Identity' column. The 'Endpoint ID' and 'IP Address' are identical for both rows: '00:0B:7F:D0:F8:F4' and '10.62.145.44'. The 'Endpoint OS' is 'Windows 7 Professional 64-bit'.

Logged At	Status	Details	Identity	Endpoint ID	IP Address	Endpoint OS
2017-02-24 18:34:31...	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-bit
2017-02-23 19:33:35...	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-bit

図4-3

ここから、特定の各イベントの詳細レポートを開くことができます。たとえば、このレポートが属するセッションID、エンドポイントに対してISEによって選択された正確なポスチャ要件、各要件のステータスなどを確認できます。

トラブルシューティング

一般情報

ポスチャプロセスのトラブルシューティングでは、ポスチャプロセスが発生する可能性のあるISEノードでデバッグするために、次のISEコンポーネントを有効にする必要があります。

- client-webapp – エージェントプロビジョニングを担当するコンポーネント。ターゲットログファイル `guest.log` と `ise-psc.log` を参照。
- guestaccess – クライアントプロビジョニングポータルコンポーネントとセッションオーナーのルックアップを担当するコンポーネント（要求が誤ったPSNに到達した場合）。ターゲットログファイル – `guest.log` を参照。
- provisioning – クライアントプロビジョニングポリシー処理を担当するコンポーネント。ターゲットログファイル – `guest.log` を参照。
- posture – すべてのポスチャ関連イベント。ターゲットログファイル – `ise-psc.log` を参照。

クライアント側のトラブルシューティングでは、次のコマンドを使用できます。

- acisensa.log – クライアント側でクライアントプロビジョニングが失敗した場合、このファイルはNSAがダウンロードされたフォルダと同じフォルダに作成されます（通常はWindows用のディレクトリをダウンロードします）。
- AnyConnect_ISEPosture.txt – このファイルは、ディレクトリ内のDARTバンドルにあります。
Cisco AnyConnect ISE Posture Moduleを参照。ISE PSNディスカバリおよびポスチャフローの一般的な手順に関するすべての情報は、このファイルに記録されます。

一般的な問題のトラブルシューティング

SSO 関連の問題

SSOが成功した場合、次のメッセージが `ise-psc.log` にこの一連のメッセージは、セッション検索が正

常に終了し、ポータルでの認証をスキップできることを示します。

<#root>

```
2016-11-09 15:07:35,951 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cisco.cpm.posture.runtime.PostureRu
```

```
looking for Radius session with input values : sessionId: null, MacAddr: null, ipAddr: 10.62.145.121
```

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cisco.cpm.posture.runtime.PostureRu
```

```
Found session c0a801010002600058232bb8 using ipAddr 10.62.145.121
```

テキストウィンドウ5-1

エンドポイントのIPアドレスを検索キーとして使用して、この情報を見つけることができます。

ゲストログの少し後に、認証がスキップされたことを確認する必要があります。

<#root>

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] guestaccess.flowmanager.step.cp.CPI
```

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] com.cisco.ise.portalSessionManager.
```

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] com.cisco.ise.portalSessionManager.
```

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] guestaccess.flowmanager.step.cp.CPI
```

```
Login step will be skipped, as the session =c0a801010002600058232bb8 already established for mac address
```

```
2016-11-09 15:07:36,066 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cpm.guestaccess.flowmanager.process
```

テキストウィンドウ5-2

SSOが機能しない場合、ise-psc log ファイルには、セッションルックアップの失敗に関する情報が含まれています。

<#root>

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
```

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
```

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
```

```
looking for session using IP 10.62.145.44
```

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
```

No Radius session found

テキストウィンドウ5-3

内 guest.log このような場合、ポータルで完全なユーザ認証を確認する必要があります。

<#root>

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste
```

Returning next step =LOGIN

```
2017-02-23 17:59:00,780 INFO [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste
```

テキストウィンドウ5-4

ポータルで認証に失敗した場合は、ポータル設定の検証に重点を置く必要があります。どのIDストアが使用されていますか。どのグループがログインを許可されますか。

クライアント プロビジョニング ポリシーの選択のトラブルシューティング

クライアントプロビジョニングポリシーの障害または誤ったポリシー処理が発生した場合は、guest.log 詳細については、「file」を参照してください。

<#root>

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C
```

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMap
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMap
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
2017-02-23 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
```

:user1:- CP Policy Status =SUCCESS, needToDoVlan=false, CoaAction=NO_COA

テキストウィンドウ5-5

最初の文字列で、セッションに関する情報がポリシー選択エンジンにどのように挿入されるかを確認できます。ポリシーが一致しない場合、またはポリシーが正しく一致しない場合は、ここから得られる属性をクライアントプロビジョニングポリシー設定と比較できます。最後の文字列は、ポリシー選択のステータスを示します。

ポスチャ プロセスのトラブルシューティング

クライアント側では、プローブとその結果の調査に関心がある必要があります。次に、成功したステージ1プローブの例を示します。

Date : 02/23/2017
Time : 17:59:57
Type : Unknown
Source : acise

Description : Function: Target::Probe
Thread Id: 0x4F8
File: SwiftHttpRunner.cpp
Line: 1415
Level: debug

PSN probe skuchere-ise22-cpp.example.com with path /auth/status, status is -1..

テキストウィンドウ5-6

この段階で、PSNはセッションオーナーに関するAC情報に戻ります。これらのメッセージは後で確認できます。

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: Target::probeRecentConnectedHeadEnd
Thread Id: 0xBE4
File: SwiftHttpRunner.cpp
Line: 1674
Level: debug

Target skuchere-ise22-2.example.com, posture status is Unknown..

テキストウィンドウ5-7

セッションの所有者は、必要なすべての情報をエージェントに返します。

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: SwiftHttpRunner::invokePosture
Thread Id: 0xFCC
File: SwiftHttpRunner.cpp
Line: 1339
Level: debug

```
MSG_NS_SWISS_NEW_SESSION, <?xml version="1.0" ?>
<root>
  <IP></IP>
  <FQDN>skuchere-ise22-2.example.com</FQDN>
  <PostureDomain>posture_domain</PostureDomain>
  <sessionId>c0a801010009e00058af0f7b</sessionId>
  <configUri>/auth/anyconnect?uuid=106a93c0-9f71-471c-ac6c-a2f935d51a36</configUri>
  <AcPackUri>/auth/provisioning/download/81d12d4b-ff58-41a3-84db-5d7c73d08304</AcPackUri>
  <AcPackPort>8443</AcPackPort>
  <AcPackVer>4.4.243.0</AcPackVer>
  <PostureStatus>Unknown</PostureStatus>
  <PosturePort>8443</PosturePort>
  <PosturePath>/auth/perfigo_validate.jsp</PosturePath>
  <PRAConfig>0</PRAConfig>
  <StatusPath>/auth/status</StatusPath>
  <BackupServers>skuchere-ise22-1.example.com,skuchere-ise22-3.example.com</BackupServers>
</root>
```

テキストウィンドウ5-8

PSN側からは、これらのメッセージに焦点を当てることができます。 `guest.log` ノードに送信される最初の要求がセッションを所有していないと予想される場合：

<#root>

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
mac_list from http request ==> 00:0B:7F:D0:F8:F4,00:0B:7F:D0:F8:F4
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi  
iplist from http request ==> 172.16.31.12,10.62.145.95
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi  
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov  
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov  
2017-02-23 17:59:56,368 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi  
2017-02-23 17:59:56,369 ERROR [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
```

Session Info is null

```
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi  
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi  
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
```

Performing MNT look up for macAddress ==> 00-0B-7F-D0-F8-F4

```
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi  
Performed MNT lookup, found session 0 with session id c0a801010009e00058af0f7b
```

```
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov  
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov  
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov  
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov  
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov  
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi  
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi  
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi  
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov  
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
```

テキストウィンドウ5-9

ここでは、PSNが最初にローカルでセッションを検出しようとし、障害発生後にIPとMACのリストを使用してセッションオーナーを特定するMNTへの要求を開始することがわかります。

少し後に、正しいPSNでクライアントからの要求が表示されます。

<#root>

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun  
ooking for session using session ID: null, IP addr: [172.16.31.12, 10.62.145.95], mac Addr [00:0B:7F:D0:F8:F4]
```

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun  
2017-02-23 17:59:56,791 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun  
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun  
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
```

Found session c0a801010009e00058af0f7b using ipAddr 172.16.31.12

テキストウィンドウ5-10

次のステップとして、PSNはこのセッションのクライアントプロビジョニングポリシー検索を実行します。

<#root>

```
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 17:59:58,203 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:58,907 DEBUG [http-bio-10.48.30.41-8443-exec-10] [] cisco.cpm.posture.util.AgentUtil -:
```

```
Increase MnT counter at CP:ClientProvisioning.ProvisionedResource.AC-44-Posture
```

テキストウィンドウ5-11

次のステップでは、ポスチャ要件の選択プロセスを確認できます。手順の最後に、要件のリストが作成され、エージェントに返されます。

<#root>

```
2017-02-23 18:00:00,372 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan
```

```
About to query posture policy for user user1 with endpoint mac 00-0b-7f-d0-f8-f4
```

```
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureMan
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan
```

```
<version>ISE: 2.2.0.470</version>
```

```
<encryption>0</encryption>
```

```
<package>
```

```
<id>10</id>
```

WinDefend

Enable WinDefend

0

3

WinDefend

301

WinDefend

running

(WinDefend)

```
</package>  
</cleanmachines>
```

テキストウィンドウ5-12

後で、ポスチャレポートがPSNによって受信されたことを確認できます。

```
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan  
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan
```

テキストウィンドウ5-13

フローの最後で、ISEはエンドポイントを準拠としてマークし、COAを開始します。

```
2017-02-23 18:00:04,272 INFO [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureMana  
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA  
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA  
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA  
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA  
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA
```

テキストウィンドウ5-14

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。