Context Directory Agent の概要

従来のセキュリティ メカニズムとは異なり、ASA-CX、WSA、ASA、クラウドベース CWS サービスなどのシスコのセキュリティ ゲートウェイでは、アクセスを必要とするエンティティのコンテキストに基づいてネットワークにセキュリティを提供します。従来のネットワークとコンテンツ セキュリティ ゲートウェイはセキュリティ ゲートウェイを通過するかどうかを決定するのにエンティティの IP アドレスのみに依存していましたが、今日のシスコ製品では、詳細な追加情報を考慮して、現在使用しているユーザ、使用するオペレーティング システム、場所など、ネットワーク エンティティの完全なコンテキストに基づいて意思決定を行うことができます。セキュリティ管理者は、このコンテキストへの参照を使用してポリシーを作成します。ネットワーク トラフィックがセキュリティ ゲートウェイにヒットすると、発信元の IP アドレスのコンテキストを（時には、宛先の IP アドレスのコンテキストも）チェックする必要があります。

Cisco Context Directory Agent（CDA）は、ネットワーク内のどの IP アドレスがどのユーザに使用されているのかをセキュリティ ゲートウェイが把握できるように、IP アドレスをユーザ名にマッピングするメカニズムです。それによって、それらのセキュリティ ゲートウェイは、そのユーザ（またはユーザが属するグループ）に基づいて決定を行えるようになります。

CDA は、Cisco Linux マシン上で実行され、Active Directory ドメイン コントローラ（DC）マシンの集合をリアルタイムで監視して、一般にユーザ ログインを示す認証関連イベントの有無を確認し、データベース内の IP アドレスとユーザ ID のマッピングを認識、分析、キャッシュし、コンシューマ デバイスが最新のマッピングを使用できるようにします。

パッチ 2 以降、CDA は、Active Directory に直接ログインしないユーザをマッピングするために、Cisco Identity Services Engine（ISE）および Cisco Secure Access Control Server（ACS）マシンから 802.1x ネットワーク ログインについて情報を受信できるようになりました。CDA は、ISE と ACS から syslog メッセージを受信する syslog サーバとして機能し、ISE と ACS から得られたネットワーク ログイン情報を使用してマッピング テーブルを設定します。

コンシューマ デバイス（Cisco 適応型セキュリティ アプライアンス（ASA）や Cisco IronPort Web セキュリティ アプライアンス（WSA）など）は、最新の IP-to-user-identity マッピング セットを次のいずれかの方法で取得するために、RADIUS プロトコルを使用して CDA と通信します。

- **オンデマンド**：CDA は、特定のマッピングに対するコンシューマ デバイスからの On-Demand クエリに応答できます。
- **フル ダウンロード**：CDA は、現在キャッシュ内にあるマッピング セット全体を求めるコンシューマ デバイスからの要求に応答できます。

オンデマンド方式とフル ダウンロード方式の両方で、コンシューマ デバイスからの要求に、後続の更新に関連する登録も含んでいることを示すタグを特別に付けることができます。

たとえば、コンシューマ デバイスが基本的なオンデマンド クエリを要求すると、CDA は応答してそのキャッシュ内で検出されている可能性のある特定のマッピングを提供しますが、そのマッピングに関するそれ以降の更新は送信しません。ただし、オンデマンド クエリに登録も含まれている場合、CDA からの最初の応答は前述と同様ですが、後でこの特定のマッピングが変更される場合、CDA は要求元のコンシューマ デバイス（および通知登録しているその他のすべてのコンシューマ デバイス）に対し、この特定のマッピングの変更について事前に通知します。

同様に、コンシューマ デバイスが基本的なフル ダウンロードを要求する場合、CDA は現在キャッシュ内にあるすべてのマッピングを含むセッション データのスナップショットを転送しますが、それ以降の更新は送信しません。ただし、要求が複製登録の場合、CDA からの最初の応答は前述と同様です。後でマッピング セットに何か変更（新しいマッピングの追加または特定のマッピングの変更など）がある場合、CDA は要求元のコンシューマ デバイス（および複製登録しているその他のすべてのコンシューマ デバイス）に対し、この変更について以前に送信されたスナップショットを基準に事前に通知します。

CDA によって検出、管理、および提供される IP-to-user-identity マッピングには IPv4 アドレスだけでなく IPv6 アドレスも含めることができます。

CDA は、ログを 1 つ以上の Syslog サーバに送信できます。

いずれかの Active Directory ドメイン コントローラまたはコンシューマ デバイスで障害が発生しても、CDA は引き続き機能します。他のドメイン コントローラから情報を取得します。ただし、CDA のフェールオーバーは行われません。CDA 内蔵の「ウォッチドッグ」機能は、その内部の Linux プロセスを継続的にモニタし、プロセスがクラッシュしたことを検出すると自動的にそのプロセスを再起動します。CDA それ自体のフェールオーバーは行われませんが、全体としての解決策では、プライマリおよびセカンダリ CDA（プライマリおよびセカンダリ RADIUS サーバに類似）を設定する機能を使用してフェールオーバー（コンシューマ デバイスによって制御される）をサポートし、プライマリが無応答の場合にはセカンダリ サーバにフェールオーバーします。プライマリおよびセカンダリ CDA は互いをまったく認識せず、ステート情報の交換も行いません。

関連項目

機能の概要（1-2 ページ）

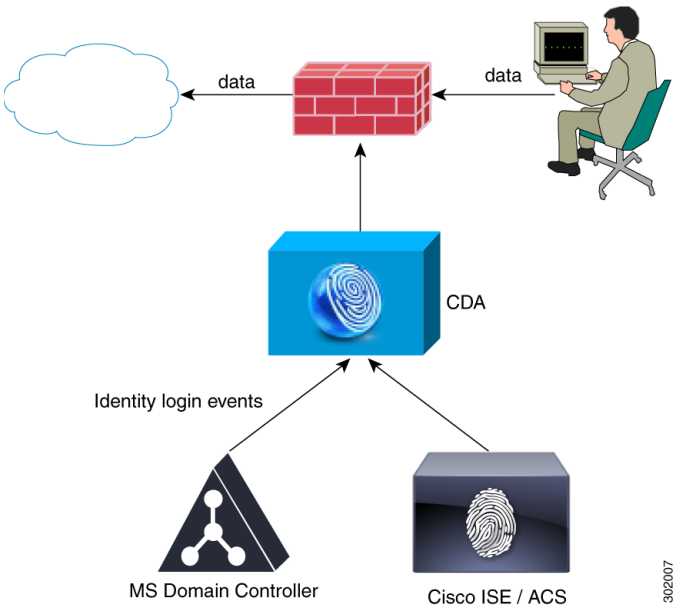
機能の概要

図 1-1 は、CDA ソリューションを表した簡略図です。この例では、ユーザはコンピュータからログインして、サーバへのアクセスを要求することによって Web トラフィックを生成します。コンシューマ デバイスは Web トラフィックをインターセプトし、コンピュータにログインしたユーザを求めている CDA に RADIUS 要求を送信します。CDA は最新の IP-to-user-identity マッピング セットを管理しており、ユーザ情報をコンシューマ デバイスに送信します。コンシューマ デバイスはユーザ ID 情報を使用して、エンド ユーザにアクセス権を付与するかどうかを決定します。

この例で、CDA は、ドメイン コントローラで発生した認証、またはユーザにネットワーク アクセスを付与する ISE で実行された認証のいずれかからユーザについて学習します。ISE と CDA の統合の利点は、Active Directory サーバとは異なる認証アイデンティティ サーバから CDA がユーザ情報を提供できることです。

ASA がネットワークに VPN コンセントレータとして導入された場合、CDA は、Active Directory から受信したログイン イベントに加えてマッピングの更新イベントを受け入れます。

図 1-1　　CDA アーキテクチャ



CDA は次を行います。

- コンシューマ デバイスへの IP-to-user-identity マッピングの提供（プッシュおよびプル、単一およびバルク）。
- コンシューマ デバイスから IP-to-user-identity マッピングに関する通知の受信。
- 各種コンポーネント（CDA およびドメイン コントローラ）のステータスを取得するインターフェイスの提供。
- IP-to-user-identity マッピングのセッション ディレクトリの管理。
- セッション情報のキャッシュ。
- Microsoft ドメイン コントローラ、ISE/ACS または ASA VPN からのリアルタイムでのマッピングの学習。CDA はユーザ変更時にコンシューマ デバイスに通知します。
- ドメイン コントローラからの履歴ログ データの読み取りによる既存の IP-to-user-identity マッピングに関する学習。
- ユーザ インターフェイスを使用して CDA を設定する設定メカニズムの提供、同時マッピング リストおよびログ イベントの表示。
- 期限切れのマッピングの定期的なクリーニング。有効期限はユーザ ログイン TTL によって定義されます。

CDA はネットワーク内の次のコンポーネントと対話します。

- コンシューマ デバイス
- Active Directory ドメイン コントローラ マシン
- Syslog サーバおよびクライアント

コンシューマ デバイス

コンシューマ デバイスは CDA から最新の IP-to-user-identity マッピングをアクティブに取得（およびパッシブに受信）します。コンシューマ デバイスは次を行います。

- CDA から IP-to-user-identity マッピングの取得。
- CDA から IP-to-user-identity マッピングの通知の受信。
- ファイアウォール ポリシーに基づく ID の実施。
- CDA 経由での Active Directory 接続の基本モニタリング。
- グループ情報の Active Directory からの直接取得。
- CDA が ID にマッピングしなかった IP の Web 認証フォールバック。
- コンシューマ デバイスにより明らかになった新しいマッピングの Web 認証経由での CDA への転送。
- VPN セッションの IP-to-user-identity マッピングの転送。
- NetBIOS プローブの実行と切断通知の CDA への転送。

これらの更新は RADIUS Accounting-Request メッセージとして送信されます。

関連トピック：

- Active Directory ドメイン コントローラ マシン（1-4 ページ）
- Syslog サーバおよびクライアント（1-6 ページ）

Active Directory ドメイン コントローラ マシン

CDA は、ユーザ ログインに関する情報を取得し、このデータをコンシューマ デバイスに提供するために、Active Directory ドメイン コントローラのセキュリティ イベント ログをモニタします。

起動時、CDA はすでにログインしているユーザの時間ベースのウィンドウ（履歴）を読み取ります。CDA は稼働するとリアルタイムでユーザ ログインをモニタして取得します。ユーザ ログイン イベントを取得するために、CDA と Active Directory ドメイン コントローラ間に接続が必要です。

Active Directory ドメイン コントローラに接続するために、CDA は Active Directory ユーザを使用します。

CDA で使用される Active Directory ユーザは、Active Directory ドメイン コントローラに接続し、モニタするために必要な権限が付与されている必要があります。

CDA で使用される Active Directory ユーザは、Domain Admin グループのメンバーであることができます。ただし、最新の CDA パッチ（将来、CDA パッチはこの機能も含むようになります）をインストールしている場合は必須ではありません。

CDA と Active Directory ドメイン コントローラ間の接続は、MS NTLM プロトコルを使用しても認証されます。CDA パッチ 2 は NTLMv1 と NTLMv2 をサポートします。

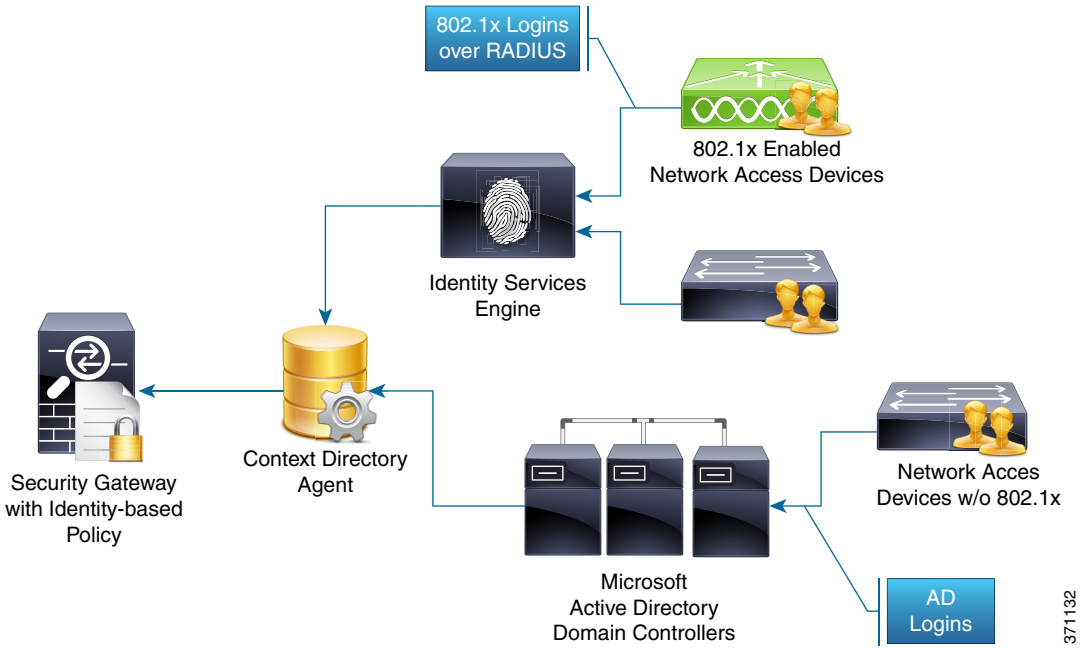
ISE と ACS からのネットワーク ログイン情報の受信

ほとんどのワイヤレス ネットワークと有線ネットワークの従業員の大部分は、現在、ネットワークにアクセスできるユーザおよび対象を制御するために 802.1x を使用します。非 AD ワークステーション（Apple MacBook や iMac、Android または iOS の電話またはタブレット、またはドメイン メンバーになっていないすべて）がネットワークにアクセスする場合、Active Directory にログインしないため、ドメイン コントローラにはそのアイデンティティの跡が残りません。このような場合、CDA は IP とアイデンティティのマップを作成できません。

ISE および ACS と対話を通じて CDA はネットワーク ログインを認識し、ドメインのメンバーかどうかを認識できるようになり、IP アドレス、ネットワークの大部分の IP アドレスとアイデンティティのマップを構築することができます。CDA は、ネットワークにログインしているユーザを取得するために ISE や ACS から syslog メッセージを受け取ると、それらのメッセージを分析して使用している ユーザ名と IP アドレスを抽出し、この情報をアイデンティティ マッピング テーブルに挿入します。

図 1-2 は、CDA が 802.1x ログイン イベントと非 802.1x AD ログイン イベントの両方（AD および非 AD）をマッピングする方法を説明しています。

図 1-2　AD および非 AD イベントの両方のマッピング



この統合により、ASA CX や WSA などのコンシューマ デバイスは、ドメイン メンバーではないものも含めて、ネットワーク エンドポイントの大部分のセキュリティ上の意思決定を行うことができます。CDA は、Windows ドメイン コントローラのイベント ログまたは ISE/ACS との統合のどちらからユーザ/ドメイン情報を受信しても、同じ形式でコンシューマ デバイスに情報を渡します。

関連項目

- Syslog メッセージの送受信（3-13 ページ）
- Syslog サーバ/クライアントの追加と編集（3-14 ページ）

Syslog サーバおよびクライアント

CDA は、管理とトラブルシューティングに関する情報が含まれているログを 1 つ以上の Syslog サーバに転送できます。また、IP-to-user-identity マッピング情報の更新も行います。これらのログの内容は、CDA マシンでローカルに使用可能なカスタマー ログと同じです。Syslog メカニズムにより、Syslog サーバが実行されており、Syslog メッセージを受信できるターゲット マシンにこの情報がリモート配信されます。

CDA は、1 つまたは複数の syslog クライアントが追加されても syslog サーバとして機能できます。Cisco Identity Services Engine（ISE）と Cisco Secure Access Control System（ACS）に接続し、syslog メッセージを受信できます。

関連トピック：

- コンシューマ デバイス（1-4 ページ）
- Active Directory ドメイン コントローラ マシン（1-4 ページ）
- Syslog サーバ/クライアントの追加と編集（3-14 ページ）

CDA のパフォーマンスと拡張性

CDA は最大 80 のドメイン コントローラ マシンに対応でき、また最大 64,000 の IP-to-user-identity マッピングを内部にキャッシュできます。最大 100 個の Identity コンシューマ デバイスに対応します。CDA は、最大 1000 の IP-to-user-identity マッピングを毎秒処理します（入力と出力）。

CDA は、3 つの Syslog クライアント（syslog サーバとして動作する場合）、20 の管理者、および 5 つの同時管理ユーザ インターフェイス セッションをサポートするようにテストされています。

CDA 導入に関する推奨事項

CDA を導入する際に、次の側面を考慮することを推奨します。

- CDA は、UDP プロトコルを使用してコンシューマ デバイスと相互運用できます。したがって、コンシューマ デバイスと地理的に近い場所に CDA を配置することを推奨します。これは、主に CDA が WAN 経由では時間がかかる可能性があるコンシューマ デバイスに大量のデータを送信するときに重要です。
- 導入時に、CDA ノードが Active Directory ドメイン コントローラからユーザ ログイン情報をすべて受け取ることを推奨します。これにより、コンシューマ デバイスは、すべてのユーザ ログイン データに対してローカルの CDA と相互運用できるようになります。さらに、Active Directory ドメイン コントローラを CDA と地理的に近い場所に配置することで信頼性が向上します。
- ハイ アベイラビリティを実現するために、両方の CDA が同じ Active Directory ドメイン コントローラから同じユーザ ログイン情報を取得するように設定された同じコンフィグレーションを持つ 2 つの CDA を使用することができます。最初の CDA が応答しない場合、2 番目の CDA に切替えるのはコンシューマ デバイスの役割です。

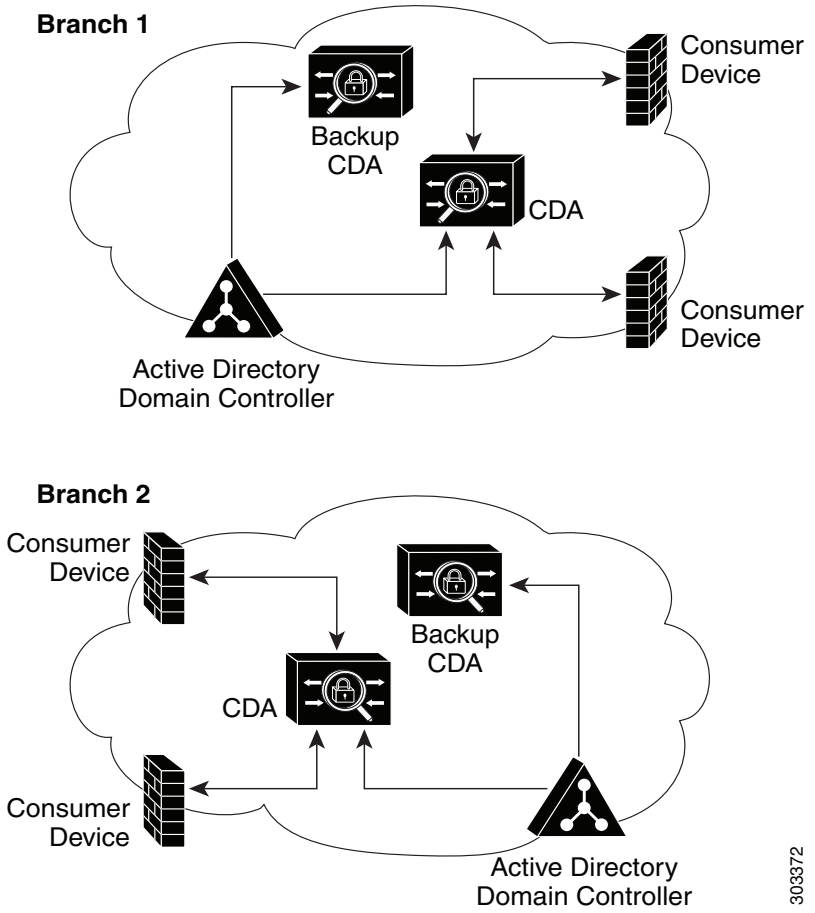



図 1-3　　推奨される CDA の導入タイプ