CHAPTER 38

アイデンティティ ファイアウォールの設定

この章では、アイデンティティ ファイアウォールに対する ASA の設定方法について説明します。次の項目を取り上げます。

アイデンティティ ファイアウォールに関する情報

この項では、次のトピックについて取り上げます。

アイデンティティ ファイアウォールの概要

企業では、ユーザが 1 つ以上のサーバ リソースにアクセスする必要が生じることがよくあります。通常、ファイアウォールではユーザのアイデンティティは認識されないため、アイデンティティに基づいてセキュリティ ポリシーを適用することはできません。ユーザごとにアクセス ポリシーを設定するには、ユーザ認証プロキシを設定する必要があります。これには、ユーザとの対話（ユーザ名とパスワードのクエリー）が必要です。

ASA のアイデンティティ ファイアウォールでは、ユーザのアイデンティティに基づいたより細かなアクセス コントロールが実現されます。送信元 IP アドレスではなくユーザ名とユーザ グループ名に基づいてアクセス ルールとセキュリティ ポリシーを設定できます。ASA は、IP アドレスと Windows Active Directory のログイン情報の関連付けに基づいてセキュリティ ポリシーを適用し、ネットワーク IP アドレスではなくマッピングされたユーザ名を使用してイベントを報告します。

アイデンティティ ファイアウォールは、実際のアイデンティティ マッピングを提供する外部 Active Directory（AD）エージェントと連携する Microsoft Active Directory と統合されます。ASA では、Windows Active Directory を送信元として使用して特定の IP アドレスについて現在のユーザのアイデンティティ情報を取得し、Active Directory ユーザにトランスペアレント認証を許可します。

アイデンティティに基づくファイアウォール サービスは、送信元 IP アドレスの代わりにユーザまたはグループを指定できるようにすることにより、既存のアクセス コントロールおよびセキュリティ ポリシー メカニズムを拡張します。アイデンティティに基づくセキュリティ ポリシーは、従来の IP アドレス ベースのルール間の制約を受けることなくインターリーブできます。

アイデンティティ ファイアウォールの主な利点には、次のようなものがあります。

- セキュリティ ポリシーからのネットワーク トポロジの分離
- セキュリティ ポリシー作成の簡略化
- ネットワーク リソースに対するユーザ アクティビティを容易に検出可能
- ユーザ アクティビティ モニタリングの効率化

アイデンティティ ファイアウォールの展開アーキテクチャ

アイデンティティ ファイアウォールは、実際のアイデンティティ マッピングを提供する外部 Active Directory（AD）エージェントとの連携により、Microsoft Active Directory と統合されます。

アイデンティティ ファイアウォールは、次の 3 つのコンポーネントにより構成されます。

- ASA
- Microsoft Active Directory

  Active Directory は ASA のアイデンティティ ファイアウォールの一部ですが、管理は Active Directory の管理者が行います。データの信頼性と正確さは、Active Directory のデータによって決まります。

  サポートされているバージョンは、Windows 2003、Windows Server 2008、および Windows Server 2008 R2 サーバです。

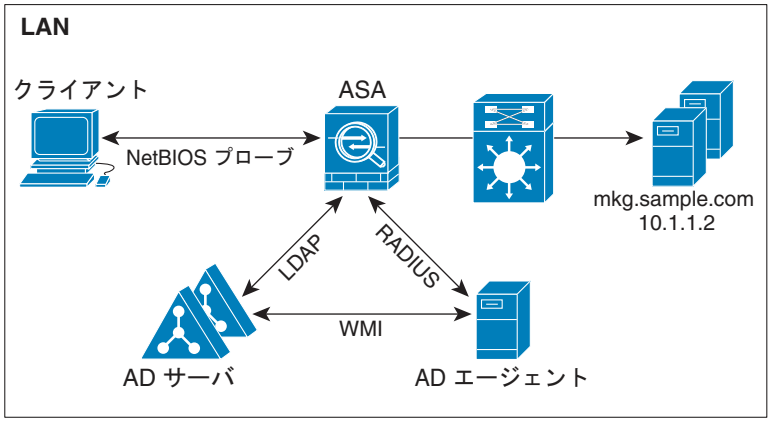
- Active Directory（AD）エージェント

  AD エージェントは Windows サーバ上で実行されます。サポートされる Windows サーバは、Windows 2003、Windows 2008、および Windows 2008 R2 です。

（注） Windows 2003 R2 は、AD エージェント サーバとしてはサポートされていません。

図 38-1 は、アイデンティティ ファイアウォールのコンポーネントを示しています。次の表は、これらのコンポーネントのロールと相互に通信する方法を示しています。

図 38-1　アイデンティティ ファイアウォールのコンポーネント



1	ASA 上：管理者がローカル ユーザ グループとアイデンティティ ファイアウォール ポリシーを設定します。	4	**クライアント <-> ASA**：クライアントは Microsoft Active Directory を介してネットワークにログオンします。AD サーバは、ユーザを認証し、ユーザ ログイン セキュリティ ログを生成します。 または、クライアントはカットスルー プロキシまたは VPN 経由でネットワークにログオンすることもできます。
2	**ASA <-> AD サーバ**：ASA は、AD サーバに設定された Active Directory グループに対する LDAP クエリーを送信します。 ASA がローカル グループと Active Directory グループを統合し、ユーザ アイデンティティに基づくアクセス ルールおよびモジュラー ポリシー フレームワーク セキュリティ ポリシーを適用します。	5	**ASA <-> クライアント**：ASA は設定されているポリシーに基づいて、クライアントにアクセスを許可または拒否します。 設定されている場合、ASA ではクライアントの NetBIOS をプローブして、非アクティブなユーザおよび応答がないユーザを渡します。
3	**ASA <-> AD エージェント**：アイデンティティ ファイアウォールの設定に応じて、ASA は IP とユーザのデータベースをダウンロードするか、ユーザの IP アドレスをたずねる AD エージェントに RADIUS 要求を送信します。 ASA は、AD エージェントに対する Web 認証および VPN セッションから学習した新しいマッピング エントリを転送します。	6	**AD エージェント <-> AD サーバ**：AD エージェントは定期的にまたはオンデマンドで、WMI 経由で AD サーバ セキュリティ イベント ログ ファイルをモニタし、クライアントのログインおよびログアウト イベントを確認します。 AD エージェントは、ユーザ ID と IP アドレスのマッピング エントリのキャッシュを保持しており、マッピングに変更があった場合は ASA に通知します。 AD エージェントは syslog サーバにログを送信します。

アイデンティティ ファイアウォールの機能

アイデンティティ ファイアウォールの主な機能は次のとおりです。

柔軟性

- ASA は、新しい IP アドレスごとに AD エージェントにクエリーを実行するか、ユーザ アイデンティティおよび IP アドレスのデータベース全体のローカル コピーを保持することにより、AD エージェントからユーザ アイデンティティと IP アドレスのマッピングを取得できます。
- ユーザ アイデンティティ ポリシーの送信先として、ホスト グループ、サブネット、または IP アドレスをサポートします。
- ユーザ アイデンティティ ポリシーの送信元および送信先として、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）をサポートします。
- 5 タプル ポリシーと ID ベースのポリシーの組み合わせをサポートします。アイデンティティ ベースの機能は、既存の 5 タプル ソリューションと連携して動作します。
- IPS およびアプリケーション インスペクションの使用をサポートします。
- リモート アクセス VPN、AnyConnect VPN、L2TP VPN、およびカットスルー プロキシからユーザのアイデンティティ情報を取得します。取得されたすべてのユーザが、AD エージェントに接続しているすべての ASA に読み込まれます。

拡張性

- 各 AD エージェントは 100 台の ASA をサポートします。複数の ASA が 1 つの AD エージェントと通信できるため、より大規模なネットワーク展開での拡張性が提供されます。
- すべてのドメインが固有の IP アドレスを持つ場合に、30 台の Active Directory サーバをサポートします。
- ドメイン内の各ユーザ アイデンティティには、最大で 8 個の IP アドレスを含めることができます。
- ASA 5500 シリーズ モデルのアクティブなポリシーでサポートされるユーザ アイデンティティと IP アドレスのマッピング エントリは、最大 64,000 個です。この制限により、ポリシーが適用されるユーザの最大数が決まります。すべてのコンテキストに設定された全ユーザを集約したものが、ユーザ総数です。
- ASA 5505 のアクティブなポリシーでサポートされるユーザ アイデンティティと IP アドレスのマッピング エントリは、最大 1024 個です。
- アクティブな ASA ポリシーでサポートされるユーザ グループは、最大 256 個です。
- 1 つのアクセス ルールに 1 つ以上のユーザ グループまたはユーザを含めることができます。
- 複数のドメインをサポートします。

可用性

- ASA は、Active Directory からグループ情報を取得し、AD エージェントが送信元 IP アドレスをユーザ アイデンティティにマッピングできない場合に IP アドレスの Web 認証にフォールバックします。
- AD エージェントは、いずれかの Active Directory サーバまたは ASA が応答しない場合でも機能し続けます。
- ASA でのプライマリ AD エージェントとセカンダリ AD エージェントの設定をサポートします。プライマリ AD エージェントが応答を停止すると、ASA がセカンダリ AD エージェントに切り替えます。
- AD エージェントが使用できない場合、ASA はカットスルー プロキシや VPN 認証などの既存のアイデンティティ取得元にフォールバックできます。
- AD エージェントは、ダウンしたサービスを自動的に再開するウォッチドッグ プロセスを実行します。
- ASA 内で使用する分散 IP アドレス/ユーザ マッピング データベースを許可します。

展開シナリオ

環境要件に応じた次の方法で、アイデンティティ ファイアウォールのコンポーネントを展開できます。

図 38-2 は、冗長性のためのアイデンティティ ファイアウォールのコンポーネントの展開方法を示しています。シナリオ 1 は、コンポーネントの冗長性がない単純なインストールを示しています。シナリオ 2 も、冗長性がない単純なインストールを示しています。ただし、この展開シナリオでは、Active Directory サーバと AD エージェントが同一の Windows サーバに共存しています。

図 38-2　冗長性のない展開シナリオ

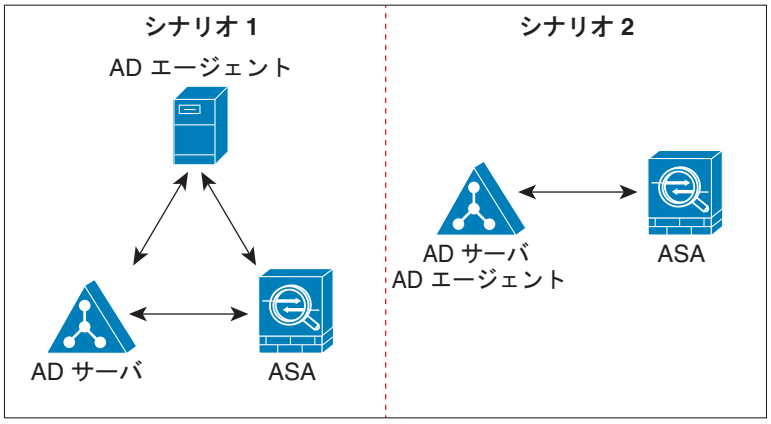


図 38-3 は、冗長性をサポートするためのアイデンティティ ファイアウォールのコンポーネントの展開方法を示しています。シナリオ 1 では、複数の Active Directory サーバと、AD エージェントをインストールした 1 台の Windows サーバを配置しています。シナリオ 2 では、複数の Active Directory サーバと、それぞれ AD エージェントがインストールされた複数の Windows サーバを配置しています。

図 38-3　冗長コンポーネントのある展開シナリオ

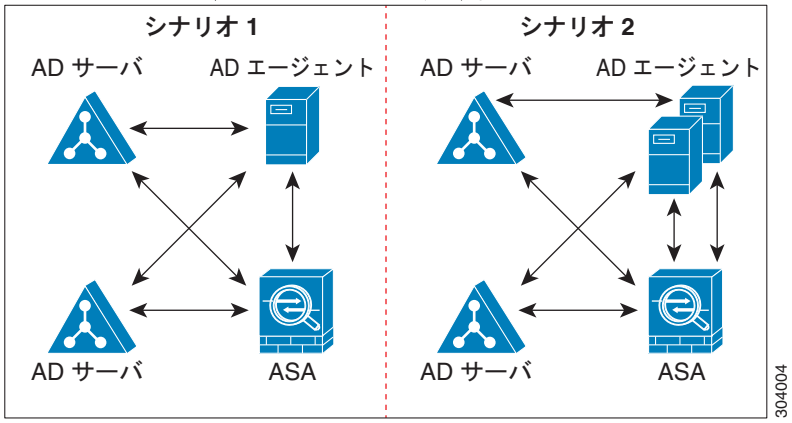


図 38-4 は、LAN 上にすべてのアイデンティティ ファイアウォール コンポーネント（Active Directory サーバ、AD エージェント、クライアント）がインストールされ通信する方法を示しています。

図 38-4　LAN ベースの展開

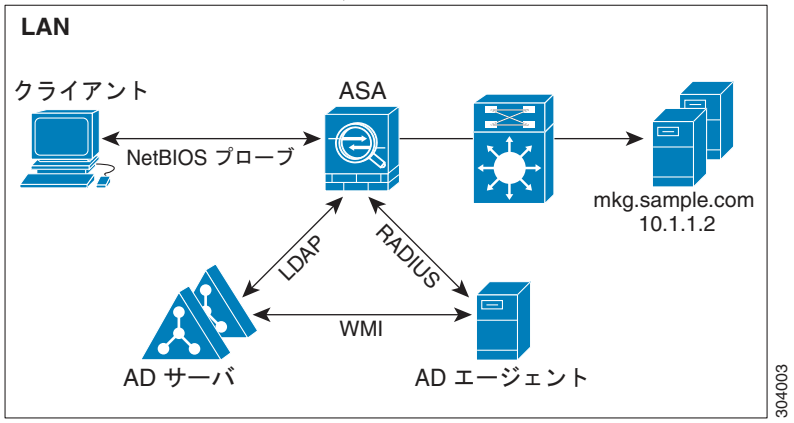


図 38-5 は、WAN を使用してリモート サイトと接続した展開方法を示しています。Active Directory サーバと AD エージェントはメイン サイトの LAN 上に配置されています。クライアントはリモート サイトに配置されており、WAN 経由でアイデンティティ ファイアウォール コンポーネントに接続しています。

図 38-5　WAN ベースの展開

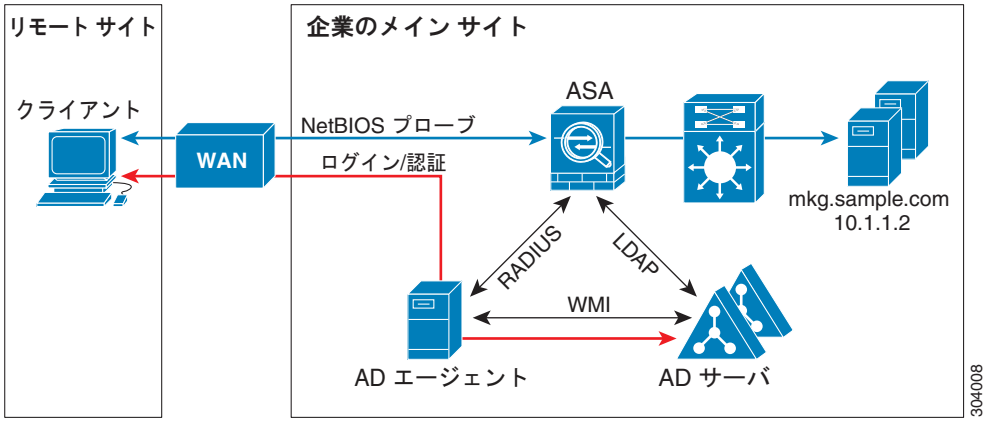


図 38-6 も WAN を使用したリモート サイトにまたがる展開方法を示しています。Active Directory サーバはメイン サイトの LAN にインストールされています。一方、AD エージェントはリモート サイトに配置され、同じサイト内のクライアントからアクセスされます。リモート クライアントは、WAN 経由でメイン サイトの Active Directory サーバに接続します。

図 38-6　リモート AD エージェントを使用した WAN ベースの展開

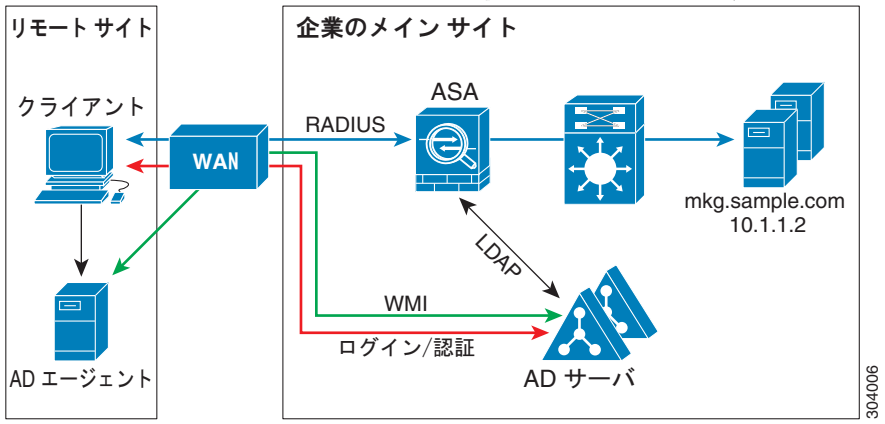
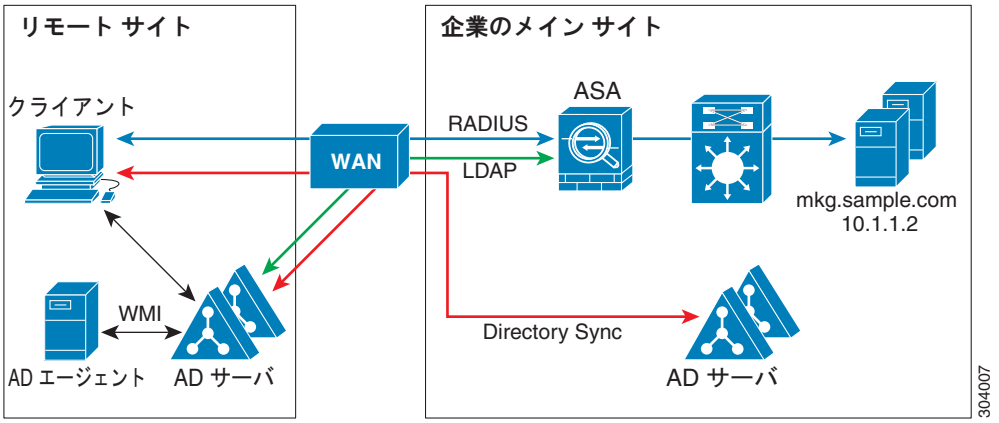


図 38-7 は、リモート サイトを拡張した WAN ベースの展開を示しています。AD エージェントと Active Directory サーバがリモート サイトに配置されています。クライアントは、メイン サイトに配置されているネットワーク リソースにログインする際に、これらのコンポーネントにローカルでアクセスします。リモート Active Directory サーバは、メイン サイトに配置された Active Directory サーバとの間でデータを同期する必要があります。

図 38-7　AD エージェントと AD サーバをリモート サイトに配置した WAN ベースの展開



アイデンティティ ファイアウォールのライセンス

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

フェールオーバーのガイドライン

- アイデンティティ ファイアウォールは、ステートフル フェールオーバーがイネーブルになっている場合、ユーザ アイデンティティと IP アドレスのマッピングおよび AD エージェント ステータスのアクティブからスタンバイへの複製をサポートします。ただし、複製されるのは、ユーザ アイデンティティと IP アドレスのマッピング、AD エージェント ステータス、およびドメイン ステータスだけです。ユーザおよびユーザ グループのレコードはスタンバイ ASA に複製されません。
- フェールオーバーを設定するときには、スタンバイ ASA についても、AD エージェントに直接接続してユーザ グループを取得するように設定する必要があります。スタンバイ ASA は、アイデンティティ ファイアウォールに NetBIOS プローブ オプションが設定されていても、クライアントに NetBIOS パケットを送信しません。
- クライアントが非アクティブであるとアクティブ ASA が判断した場合、情報はスタンバイ ASA に伝搬されます。ユーザ統計情報はスタンバイ ASA に伝搬されません。
- フェールオーバーを設定した場合は、AD エージェントをアクティブとスタンバイの両方の ASA と通信するように設定する必要があります。AD エージェント サーバで ASA を設定する手順については、『*Installation and Setup Guide for the Active Directory Agent*』を参照してください。

IPv6 のガイドライン

- IPv6 をサポートします。
- AD エージェントは IPv6 アドレスのエンドポイントをサポートします。AD エージェントは、ログイベントで IPv6 アドレスを受け取り、それをキャッシュに保存し、RADIUS メッセージによって送信します。
- IPv6 上の NetBIOS はサポートされていません。

その他のガイドラインと制限事項

- 宛先アドレスとしての完全な URL の使用はサポートされていません。
- NetBIOS プローブが機能するためには、ASA、AD エージェント、およびクライアントを接続するネットワークが UDP でカプセル化された NetBIOS トラフィックをサポートしている必要があります。
- アイデンティティ ファイアウォールによる MAC アドレスのチェックは、仲介ルータがある場合は機能しません。同じルータの背後にあるクライアントにログオンしたユーザには、同じ MAC アドレスが割り当てられます。この実装では、ASA がルータの背後の実際の MAC アドレスを特定できないため、同じルータからのパケットはすべてチェックに合格します。
- 次の ASA 機能は、拡張 ACL でのアイデンティティに基づくオブジェクトおよび FQDN の使用をサポートしません。
  - ルート マップ
  - クリプト マップ

  - WCCP
  - NAT
  - グループ ポリシー（VPN フィルタを除く）
  - DAP
- **user-identity update active-user-database** コマンドを使用して、実行中に AD エージェントからのユーザ IP アドレスのダウンロードを開始できます。

  設計的に、前のダウンロード セッションが終了すると、ASA はこのコマンドを再度発行することを許しません。

  その結果、ユーザ IP データベースが非常に大きく、前のセッションが終了していない場合に、もう一度 **user-identity update active-user-database** を発行すると、次のエラー メッセージが表示されます。

  ```
  "ERROR: one update active-user-database is already in progress."
  ```

  You need to wait until the previous session is completely finished, then you can issue another **user-identity update active-user-database** command.

  この動作のもう 1 つの例は、AD エージェントから ASA へのパケット損失で発生します。

  user-identity update active-user-database コマンドを発行すると、ASA はダウンロードされるユーザ IP マッピング エントリの総数を要求します。次に AD エージェントは ASA への UDP 接続を開始し、認証要求パケットの変更を送信します。

  何らかの理由でパケットが失われた場合、ASA にはこれを検出する機能はありません。その結果 ASA は 4 ～ 5 分間セッションを維持し、**user-identity update active-user-database** コマンドを発行すると、このエラー メッセージを表示し続けます。
- ASA または Cisco Ironport Web Security Appliance（WSA）とともに Cisco Context Directory Agent（CDA）を使用する場合は、次のポートを開くことを確認してください。
  - UDP の認証ポート：1645
  - UDP のアカウンティング ポート：1646
  - UDP のリスニング ポート：3799

    リスニング ポートは、CDA から ASA または WSA への認証要求の変更の送信に使用されます。

前提条件

ASA でアイデンティティ ファイアウォールを設定する前に、AD エージェントおよび Microsoft Active Directory の前提条件を満たす必要があります。

AD エージェント

- AD エージェントは、ASA がアクセスできる Windows サーバにインストールする必要があります。さらに、AD エージェントを Active Directory サーバから情報を取得し、ASA と通信するように設定します。
- サポートされる Windows サーバは、Windows 2003、Windows 2008、および Windows 2008 R2 です。

（注） Windows 2003 R2 は、AD エージェント サーバとしてはサポートされていません。

- AD エージェントをインストールし設定する手順については、『*Installation and Setup Guide for the Active Directory Agent*』を参照してください。
- ASA に AD エージェントを設定する前に、AD エージェントと ASA が通信に使用する秘密キーの値を取得します。この値は AD エージェントと ASA で一致している必要があります。

Microsoft Active Directory

- Microsoft Active Directory は、Windows サーバにインストールされ、ASA からアクセス可能である必要があります。サポートされているバージョンは、Windows 2003、2008、および 2008 R2 サーバです。
- ASA に Active Directory サーバを設定する前に、Active Directory に ASA のユーザ アカウントを作成します。
- さらに、ASA は、LDAP 上でイネーブルになった SSL を使用して、暗号化されたログイン情報を Active Directory サーバに送信します。Active Directory で SSL をイネーブルにする必要があります。Active Directory で SSL をイネーブルにする手順については、Microsoft Active Directory のマニュアルを参照してください。

（注）　AD エージェントのインストーラを実行する前に、AD エージェントがモニタする各 Microsoft Active Directory サーバの「*Readme First for the Cisco Active Directory Agent*」に一覧表示されているパッチをインストールします。これらのパッチは、AD エージェントをドメイン コントローラ サーバに直接インストールする場合でも必要です。

アイデンティティ ファイアウォールの設定

ここでは、次の内容について説明します。

アイデンティティ ファイアウォールの設定のタスク フロー

アイデンティティ ファイアウォールを設定するには、次の作業を実行します。

ステップ 1　ASA に Active Directory ドメインを設定します。

「Active Directory ドメインの設定」（P.38-11）および「Active Directory サーバ グループの設定」（P.38-12）を参照してください。

個々の環境の要件に合わせて Active Directory サーバを展開する方法については、「展開シナリオ」（P.38-5）を参照してください。

ステップ 2　ASA に AD エージェントを設定します。

「Active Directory サーバ グループの設定」（P.38-12）および「Active Directory エージェント グループの設定」（P.38-13）を参照してください。

個々の環境の要件に合わせて AD エージェントを展開する方法については、「展開シナリオ」（P.38-5）を参照してください。

ステップ 3　アイデンティティ オプションを設定します。

「アイデンティティ オプションの設定」（P.38-14）を参照してください。

ステップ 4　Identity-Based セキュリティ ポリシーの設定 AD ドメインと AD エージェントを設定した後、多くの機能で使用するために、アイデンティティに基づくオブジェクト グループおよび ACL を作成できます。

「Identity-Based セキュリティ ポリシーの設定」（P.38-16）を参照してください。

Active Directory ドメインの設定

ASA が AD エージェントから IP とユーザのマッピングを受信したときに特定のドメインから Active Directory グループをダウンロードし、ユーザ アイデンティティを受け取るためには、ASA 上の Active Directory ドメイン設定が必要となります。

前提条件

- Active Directory サーバの IP アドレス
- LDAP ベース DN の識別名
- アイデンティティ ファイアウォールが Active Directory ドメイン コントローラへの接続に使用する、Active Directory ユーザの識別名とパスワード

Active Directory ドメインを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Identity Options] の順に選択します。

ステップ 2　必要に応じて、[Enable User Identity] チェックボックスをオンにして、ユーザのアイデンティティをイネーブルにします。

ステップ 3　[Domains] セクションで、[Add] をクリックするか、リストからドメインを選択して [Edit] をクリックします。

[Domain] ダイアログボックスが表示されます。

ステップ 4　[Domain NETBIOS Name] フィールドに、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.] で構成される最大 32 文字の名前を入力します。ただし、先頭に "." と " " を使用することはできません。ドメイン名にスペースを含める場合は、スペースを引用符で囲む必要があります。ドメイン名では、大文字と小文字が区別されません。

既存のドメインの名前を編集する場合、既存のユーザおよびユーザ グループに関連付けられているドメイン名は変更されません。

ステップ 5　[AD Server Group] リストで、このドメインに関連付ける Active Directory サーバを選択するか、[Manage] をクリックして新しいサーバ グループをリストに追加します。「Active Directory サーバ グループの設定」（P.38-12）を参照してください。

ステップ 6　[OK] をクリックしてドメイン設定を保存し、ダイアログボックスを閉じます。

次の作業

「Active Directory サーバ グループの設定」（P.38-12）および「Active Directory エージェント グループの設定」（P.38-13）を参照してください。

Active Directory サーバ グループの設定

Active Directory サーバ グループを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Identity Options] > [Add] > [Manage] の順に選択します。

[Configure Active Directory Server Groups] ダイアログボックスが表示されます。

ステップ 2　アイデンティティ ファイアウォールの Active Directory サーバ グループを追加するには、[Add] をクリックします。

[Add Active Directory Server Group] ダイアログボックスが表示されます。

ステップ 3　Active Directory サーバ グループにサーバを追加するには、[Active Directory Server Groups] リストから選択して、[Add] をクリックします。

[Add Active Directory Server] ダイアログボックスが表示されます。

ステップ 4　[OK] をクリックして設定を保存し、ダイアログボックスを閉じます。

次の作業

「Active Directory エージェントの設定」（P.38-12）および「Active Directory エージェント グループの設定」（P.38-13）を参照してください。

Active Directory エージェントの設定

AD エージェントは、定期的に、または要求に応じて、WMI を介して Active Directory サーバのセキュリティ イベント ログ ファイルをモニタし、ユーザのログインおよびログオフ イベントを調べます。AD エージェントは、ユーザ ID と IP アドレスのマッピング エントリのキャッシュを保持しており、マッピングに変更があった場合は ASA に通知します。

前提条件

AD エージェントを設定する前に、次の情報を用意してください。

- AD エージェントの IP アドレス
- ASA と AD エージェントとの共有秘密

AD エージェントを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Identity Options] の順に選択します。

ステップ 2　必要に応じて、[Enable User Identity] チェックボックスをオンにして、機能をイネーブルにします。

ステップ 3　[Active Directory Agent] セクションで、[Manage] をクリックします。

[Configure Active Directory Agents] ダイアログボックスが表示されます。

ステップ 4　AD エージェントを追加するには、[Add] ボタンをクリックします。またリストでエージェント グループを選択し、[Edit] をクリックします。

以降の手順については、「Active Directory エージェント グループの設定」（P.38-13）を参照してください。

ステップ 5　[OK] をクリックして変更を保存します。

次の作業

AD エージェント グループを設定します。「Active Directory エージェント グループの設定」（P.38-13）を参照してください。

アイデンティティ ファイアウォールのアクセス ルールを設定します。「Identity-Based セキュリティ ポリシーの設定」（P.38-16）を参照してください。

Active Directory エージェント グループの設定

AD エージェント サーバ グループのプライマリ AD エージェントとセカンダリ AD エージェントを設定します。プライマリ AD エージェントが応答していないことを ASA が検出し、セカンダリ AD エージェントが指定されている場合、ASA はセカンダリ AD エージェントに切り替えます。AD エージェントの Active Directory サーバは、通信プロトコルとして RADIUS を使用します。そのため、ASA と AD エージェントとの共有秘密のキー属性を指定する必要があります。

AD エージェント グループを設定するには、次の手順を実行します。

ステップ 1　[Configure Active Directory Agents] ダイアログボックスで、[Add] をクリックします。

[Add Active Directory Agent Group] ダイアログボックスが表示されます。

ステップ 2　AD エージェント グループの名前を入力します。

ステップ 3　[Primary Active Directory Agent] セクションで、ASA が AD エージェント サーバのトラフィックをリッスンするインターフェイスを指定し、サーバの FQDN または IP アドレスを入力します。

ステップ 4　[Primary Active Directory Agent] セクションに、AD エージェントが応答しない場合に ASA が続けて接続を試行する際のタイムアウト間隔と再試行間隔を入力します。

ステップ 5　プライマリ AD エージェントと ASA の間で使用される共有秘密キーを入力します。

ステップ 6　[Secondary Active Directory Agent] セクションで、ASA が AD エージェント サーバのトラフィックをリッスンするインターフェイスを指定し、サーバの FQDN または IP アドレスを入力します。

ステップ 7　[Secondary Active Directory Agent] セクションに、AD エージェントが応答しない場合に ASA が続けて接続を試行する際のタイムアウト間隔と再試行間隔を入力します。

ステップ 8　セカンダリ AD エージェントと ASA の間で使用される共有秘密キーを入力します。

ステップ 9　[OK] をクリックして変更を保存し、ダイアログボックスを閉じます。

次の作業

アイデンティティ ファイアウォールのアクセス ルールを設定します。「Identity-Based セキュリティ ポリシーの設定」（P.38-16）を参照してください。

アイデンティティ オプションの設定

このペインを使用して、アイデンティティ ファイアウォール機能を追加または編集するには、[Enable] チェックボックスをオンにします。デフォルトでは、アイデンティティ ファイアウォール機能はディセーブルになっています。

前提条件

アイデンティティ ファイアウォールのアイデンティティ オプションを設定する前に、AD エージェントおよび Microsoft Active Directory の前提条件を満たす必要があります。AD エージェントおよび Microsoft Active Directory のインストール要件については、「前提条件」（P.38-9）を参照してください。

アイデンティティ ファイアウォールのアイデンティティ オプションを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Identity Options] の順に選択します。

ステップ 2　必要に応じて、[Enable User Identity] チェックボックスをオンにして、機能をイネーブルにします。

ステップ 3　アイデンティティ ファイアウォールのドメインを追加するには、[Add] をクリックして [Add Domain] ダイアログボックスを表示します。

ステップ 4　以降の手順については、「Active Directory ドメインの設定」（P.38-11）を参照してください。

ステップ 5　[Domains] リストにすでに追加されているドメインについて、Active Directory ドメイン コントローラが応答していないため、そのドメインがダウンしている場合にルールをディセーブルにするかどうかを指定します。

ドメインがダウンしており、そのドメインに対してこのオプションが指定されている場合、ASA により、そのドメイン内のユーザに関連付けられているユーザ アイデンティティ ルールがディセーブルにされます。さらに、[Monitoring] > [Properties] > [Identity] > [Users] ペインでは、そのドメイン内のすべてのユーザ IP アドレスがディセーブルとマークされます。

ステップ 6　[Default Domain] ドロップダウン リストで、アイデンティティ ファイアウォールのデフォルト ドメインを選択します。

デフォルト ドメインは、ユーザまたはグループにドメインが明示的に設定されていない場合に、すべてのユーザおよびユーザ グループで使用されます。デフォルト ドメインを指定しない場合、ユーザおよびグループのデフォルト ドメインは LOCAL となります。

さらに、アイデンティティ ファイアウォールは、ローカルに定義されたすべのユーザ グループまたはユーザ（VPN または Web ポータルを使用してログインおよび認証を行うユーザ）に対して LOCAL ドメインを使用します。

（注）　選択するデフォルト ドメイン名は、Active Directory ドメイン コントローラに設定された NetBIOS ドメイン名と一致している必要があります。ドメイン名が一致しない場合、AD エージェントは、ユーザと IP のマッピングを ASA の設定時に入力されたドメイン名に誤って関連付けます。
NetBIOS ドメイン名を表示するには、任意のテキスト エディタで Active Directory ユーザ イベント セキュリティ ログを開きます。

マルチ コンテキスト モードでは、システム実行スペース内だけでなく、各コンテキストについてデフォルト ドメイン名を設定できます。

ステップ 7　[Active Directory Agent] セクションで、ドロップダウン リストから AD エージェント グループを選択します。AD エージェント グループを追加するには、[Manage] をクリックします。詳細については、「Active Directory エージェントの設定」（P.38-12）を参照してください。

ステップ 8　[Hello Timer] フィールドに、10 ～ 65535 秒の数値を入力します。

ASA と AD エージェントとの間の Hello タイマーは、ASA が hello パケットを交換する頻度を定義します。ASA は、hello パケットを使用して、ASA 複製ステータス（in-sync または out-of-sync）とドメイン ステータス（up または down）を取得します。ASA は、AD エージェントから応答を受信しなかった場合、指定された間隔が経過した後、hello パケットを再送信します。

ASA が AD エージェントに hello パケットを送信する回数を指定します。デフォルトでは、秒数は 30 に設定され、再試行回数は 5 に設定されます。

ステップ 9　[Poll Group Timer] フィールドで、完全修飾ドメイン名（FQDN）を解決するために ASA が DNS サーバにクエリーを実行する時間数を入力します。デフォルトでは、poll タイマーは 4 秒に設定されます。

ステップ 10　[Retrieve User Information] で、リストから次のいずれかのオプションを選択します。

- [On Demand] : ASA が新しい接続を必要とするパケットを受信し、その送信元 IP アドレスのユーザがユーザ アイデンティティ データベースに含まれていない場合に、ASA が AD エージェントから IP アドレスのユーザ マッピング情報を取得することを指定します。
- [Full Download] : ASA が、ASA の起動時に IP/ユーザ マッピング テーブル全体をダウンロードし、ユーザのログインおよびログアウト時に増分 IP/ユーザ マッピングを受信するように指示する要求を AD エージェントに送信することを指定します。

（注）　on-demand には、受信パケットのユーザだけが取得および保存されるためにメモリの使用量が少なくなるというメリットがあります。

ステップ 11　[Error Conditions] セクションで、AD エージェントが応答していない場合にルールをディセーブルにするかどうかを選択します。

AD エージェントがダウンしており、このオプションが選択されている場合、ASA により、そのドメイン内のユーザに関連付けられているユーザ アイデンティティ ルールがディセーブルにされます。さらに、[Monitoring] > [Properties] > [Identity] > [Users] ペインでは、そのドメイン内のすべてのユーザ IP アドレスがディセーブルとマークされます。

ステップ 12　[Error Conditions] セクションで、NetBIOS プローブが失敗した場合にユーザの IP アドレスを削除するかどうかを選択します。

このオプションを選択すると、ユーザに対する NetBIOS プローブがブロックされた場合（たとえば、ユーザ クライアントが NetBIOS プローブに応答しない場合）のアクションが指定されます。また、そのクライアントへのネットワーク接続がブロックされている場合や、クライアントがアクティブでない場合もあります。このオプションが選択されている場合、そのユーザ IP アドレスに関連付けられているアイデンティティ ルールが ASA によってディセーブルにされます。

ステップ 13　[Error Conditions] セクションで、ASA が現在ユーザの MAC アドレスにマッピングしている IP アドレスと、その MAC アドレスが一致しない場合に、ユーザの MAC アドレスを削除するかどうかを選択します。このオプションが選択されている場合、特定のユーザに関連付けられているユーザ アイデンティティ ルールが ASA によってディセーブルにされます。

ステップ 14　[Error Conditions] セクションで、見つからないユーザを追跡するかどうかを選択します。

ステップ 15　[Users] セクションで [Idle Timeout] オプションを選択し、1 ～ 65535 分の分数を入力します。デフォルトでは、アイドル タイムアウトは 60 分に設定されます。

このオプションをイネーブルにすると、アクティブ ユーザがアイドル状態であると考えられる場合（指定された時間を超えても ASA がユーザの IP アドレスからトラフィックを受信しない場合）のタイマーが設定されます。タイマーの期限が切れると、ユーザの IP アドレスが非アクティブとマークされ、ローカル キャッシュ内の IP とユーザのデータベースから削除されます。これ以降、ASA は、この IP アドレスについて AD エージェントに通知しません。既存のトラフィックは通過を許可されます。[Idle Timeout] オプションをイネーブルにすると、ASA は NetBIOS ログアウト プローブが設定されている場合でも非アクティブ タイマーを実行します。

（注）　アイドル タイムアウト オプションは VPN ユーザまたはカットスルー プロキシ ユーザには適用されません。

ステップ 16　[NetBIOS Logout Probe] セクションで、NetBIOS プローブをイネーブルにし、ユーザの IP アドレスがプローブされるまでのプローブ タイマー（1 ～ 65535 分）とプローブの再試行間の再試行間隔（1 ～ 256 回の再試行）を設定します。

このオプションをイネーブルにすることにより、ASA がユーザ ホストのプローブによってユーザ クライアントがアクティブであるかどうかを確認する頻度を設定します。NetBIOS パケットを最小限に抑えるために、ASA は、[Idle Timeout minutes] フィールドで指定された分数を超えてユーザがアイドル状態である場合のみ NetBIOS プローブをクライアントに送信します。

ステップ 17　[NetBIOS Logout Probe] セクションで、[User Name] リストから次のいずれかのオプションを選択します。

- [Match Any] : ホストからの NetBIOS 応答に IP アドレスに割り当てられたユーザのユーザ名が含まれている場合、ユーザ アイデンティティは有効と見なされます。このオプションを指定する場合は、ホストで Messenger サービスがイネーブルになっており、WINS サーバが設定されている必要があります。
- [Exact Match] : NetBIOS 応答に IP アドレスに割り当てられたユーザのユーザ名だけが含まれている必要があります。そうでない場合、その IP アドレスのユーザ アイデンティティは無効と見なされます。このオプションを指定する場合は、ホストで Messenger サービスがイネーブルになっており、WINS サーバが設定されている必要があります。
- [User Not Needed] : ASA がホストから NetBIOS 応答を受信した場合、ユーザ アイデンティティは有効と見なされます。

ステップ 18　[Apply] をクリックし、アイデンティティ ファイアウォールの設定を保存します。

次の作業

Active Directory ドメインとサーバ グループを設定します。「Active Directory ドメインの設定」（P.38-11）および「Active Directory サーバ グループの設定」（P.38-12）を参照してください。

AD エージェントを設定します。「Active Directory サーバ グループの設定」（P.38-12）を参照してください。

Identity-Based セキュリティ ポリシーの設定

Identity-Based ポリシーは、多くの ASA 機能に組み込むことができます。拡張 ACL を使用する機能（「注意事項と制限事項」（P.38-8）でサポート対象外としてリストされている機能を除く）でアイデンティティ ファイアウォールを使用できます。拡張 ACL に、ネットワークベースのパラメータとともにユーザ アイデンティティ引数を追加できるようになりました。

- 拡張 ACL を設定するには、Chapter 17, “Adding an Extended Access Control List.” を参照してください。
- ACL で使用できるローカル ユーザ グループを設定するには、「ローカル ユーザ グループの設定」（P.20-8）を参照してください。

次のような機能で、アイデンティティを使用できます。

- アクセス ルール：アクセス ルールは、ネットワーク情報を使用してインターフェイスのトラフィックを許可または拒否します。アイデンティティ ファイアウォールを使用して、ユーザ アイデンティティに基づいてアクセスを制御できるようになりました。ファイアウォール コンフィギュレーション ガイドの Chapter 46, “Configuring Access Rules,” を参照してください。
- AAA ルール：認証ルール（「カットスルー プロキシ」とも呼ばれます）は、ユーザに基づいてネットワーク アクセスを制御します。この機能がアクセス ルールとアイデンティティ ファイアウォールに非常に似ているため、AAA ルールは、ユーザの AD ログインの期限が切れた場合、認証のバックアップ方式として使用できます。たとえば、有効なログインのないユーザの場合、AAA ルールをトリガーできます。AAA ルールが有効なログインがないユーザに対してだけトリガーされるようにするには、拡張 ACL でアクセス ルールと AAA ルールに使用される特別なユーザ名 None（有効なログインのないユーザ）および Any（有効なログインを持つユーザ）を指定します。アクセス ルールでは、ユーザおよびグループのポリシーを通常どおりに設定しますが、すべての None ユーザを許可する AAA ルールを含めます。これらのユーザが後で AAA ルールをトリガーできるように、これらのユーザを許可する必要があります。次に、Any ユーザ（これらのユーザは、AAA ルールの対象ではなく、アクセス ルールによってすでに処理されています）を拒否し、すべての None ユーザを許可する AAA ルールを設定します。次に例を示します。

```
access-list 100 ex permit ip user CISCO\xyz any any
access-list 100 ex deny ip user CISCO\abc any any
access-list 100 ex permit ip user NONE any any
access-list 100 ex deny any any
access-group 100 in interface inside

access-list 200 ex deny ip user ANY any any
access-list 200 ex permit user NONE any any
aaa authenticate match 200 inside user-identity
```

詳細については、ファイアウォール コンフィギュレーション ガイドの Chapter 47, “Configuring AAA Rules for Network Access,” を参照してください。

- クラウド Web セキュリティ：クラウド Web セキュリティ プロキシ サーバに送信されるユーザを制御できます。また、クラウド Web セキュリティに送信される ASA トラフィック ヘッダーに含まれているユーザ グループに基づくクラウド Web セキュリティ ScanCenter ポリシーを設定できます。ファイアウォール コンフィギュレーション ガイドの Chapter 64, “Configuring the ASA for Cisco Cloud Web Security,” を参照してください。
- VPN フィルタ：通常、VPN はアイデンティティ ファイアウォール ACL をサポートしませんが、VPN トラフィックにアイデンティティに基づくアクセス ルールを適用するように ASA を設定できます。デフォルトでは、VPN トラフィックはアクセス ルールの対象になりません。VPN クライアントをアイデンティティ ファイアウォール ACL（**no sysopt connection permit-vpn** コマンドによる）を使用するアクセス ルールに強制的に従わせることができます。また、アイデンティティ ファイアウォール ACL を VPN フィルタ機能とともに使用できます。VPN フィルタは、アクセス ルールを一般的に許可することと同様の効果を実現します。

アイデンティティ ファイアウォールのモニタリング

この項では、次の内容について説明します。

AD エージェントのモニタリング

アイデンティティ ファイアウォールの AD エージェント コンポーネントをモニタするには、次の手順を実行します。

ステップ 1　[Monitoring] > [Properties] > [Identity] > [AD Agent] の順に選択します。

ステップ 2　[Refresh] をクリックして、ペイン内のデータを更新します。

このペインには、プライマリ AD エージェントおよびセカンダリ AD エージェントに関する次の情報が表示されます。

- AD エージェントのステータス
- ドメインのステータス
- AD エージェントの統計情報

グループのモニタリング

アイデンティティ ファイアウォールに設定されたユーザ グループをモニタするには、次の手順の実行します。

ステップ 1　[Monitoring] > [Properties] > [Identity] > [Group] の順に選択します。

ステップ 2　選択したグループを使用するアクセス ルールのリストを表示するには、[Where used] をクリックします。

ステップ 3　[Refresh] をクリックして、ペイン内のデータを更新します。

このペインには、ユーザ グループのリストが *domain**group_name* の形式で表示されます。

アイデンティティ ファイアウォールのメモリ使用率のモニタリング

ASA 上でアイデンティティ ファイアウォールが消費するメモリ使用率をモニタするには、次の手順を実行します。

ステップ 1　[Monitoring] > [Properties] > [Identity] > [Memory Usage] の順に選択します。

ステップ 2　[Refresh] をクリックして、ペイン内のデータを更新します。

このペインには、アイデンティティ ファイアウォールの各種モジュールのメモリ使用率がバイト単位で表示されます。

- ユーザ
- グループ
- ユーザ統計
- LDAP

ASA は、Active Directory サーバに設定された Active Directory グループに対する LDAP クエリーを送信します。Active Directory サーバは、ユーザを認証し、ユーザ ログイン セキュリティ ログを生成します。

- AD エージェント
- その他
- メモリ使用率合計

（注）　アイデンティティ ファイアウォールで設定した AD エージェントからユーザ情報を取得する方法によって、この機能が使用するメモリの量が変わります。ASA で on-demand 取得と full-download 取得のどちらを使用するかを指定します。on-demand を選択すると、受信パケットのユーザだけが取得および保存されるためにメモリの使用量が少なくなるというメリットがあります。詳細については、「アイデンティティ オプションの設定」（P.38-14）を参照してください。

アイデンティティ ファイアウォールのユーザのモニタリング

アイデンティティ ファイアウォールで使用される IP ユーザ マッピング データベースに含まれるすべてのユーザに関する情報を表示するには、次の手順の実行します。

ステップ 1　[Monitoring] > [Properties] > [Identity] > [User] の順に選択します。

（注）　アクティブ ユーザは緑色で強調表示されます。

ステップ 2　アクティブ ユーザに関する詳細情報を表示するには、リスト内のユーザを選択し、[Details] をクリックします。[Details] ボタンは、アクティブ ユーザでのみイネーブルになります。

ステップ 3　選択したユーザを使用するアクセス ルールのリストを表示するには、[Where used] をクリックします。

ステップ 4　[Refresh] をクリックして、ペイン内のデータを更新します。

このペインには、ユーザに関する次の情報が表示されます。

domain\user_name	ステータス（アクティブまたは非アクティブ）	接続	アイドル時間（分数）

デフォルトのドメイン名は、実際のドメイン名、特別な予約語、LOCAL のいずれかです。アイデンティティ ファイアウォールは、ローカルに定義されたすべのユーザ グループまたはユーザ（VPN または Web ポータルを使用してログインおよび認証を行うユーザ）に対して LOCAL ドメイン名を使用します。デフォルト ドメインを指定しない場合、LOCAL がデフォルト ドメインとなります。

アイドル時間は、ユーザの IP アドレスごとではなくユーザごとに保存されます。

Active Directory サーバがダウンしている場合にルールをディセーブルにするオプションが指定されていて、ドメインがダウンしている場合、または AD エージェントがダウンしている場合にルールをディセーブルにするオプションが指定されていて、AD エージェントがダウンしている場合、ログインしているすべてのユーザのステータスがディセーブルになります。これらのオプションは、[Identity Options] ペインで設定します。

または、[Firewall Dashboard] ペインにアクセスして、ユーザの統計を表示することもできます。[Firewall Dashboard] タブでは、ASA を通過するトラフィックに関する重要な情報を確認できます。[Home] > [Firewall Dashboard] > [Top Usage Statistics] > [Top 10 Users] タブを選択します。

[Top 10 Users] タブには、ASA でアイデンティティ ファイアウォール機能を設定している場合（Microsoft Active Directory や Cisco Active Directory（AD）エージェントなどの追加コンポーネントの設定を含む）にのみデータが表示されます。詳細については、「アイデンティティ ファイアウォールの設定」（P.38-10）を参照してください。

選択したオプションに応じて、[Top 10 Users] タブに、上位 10 ユーザの受信した EPS パケット、送信した EPS パケット、および送信された攻撃に関する統計情報が表示されます。（*domain\user_name* として表示される）各ユーザに関して、このタブには、そのユーザの平均 EPS パケット、現在の EPS パケット、トリガー、および合計イベント数が表示されます。

（注） [Top Usage Status] 領域の最初の 3 つのタブには脅威検出のデータが表示されます。これは、アイデンティティ ファイアウォール機能とは関係ありません。

アイデンティティ ファイアウォールの機能履歴

表 38-1 に、この機能のリリース履歴を示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 38-1　アイデンティティ ファイアウォールの機能履歴

機能名	リリース	機能情報
アイデンティティ ファイアウォール	8.4(2)	アイデンティティ ファイアウォール機能が導入されました。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Identity Options] [Configuration] > [Firewall] > [Objects] > [Local User Groups] [Monitoring] > [Properties] > [Identity]