

アイデンティティ ファイアウォール

この章では、アイデンティティ ファイアウォール向けに ASA を設定する方法について説明します。

- アイデンティティ ファイアウォールについて （1 ページ）
- アイデンティティ ファイアウォールのガイドライン （8 ページ）
- アイデンティティ ファイアウォールの前提条件 （10 ページ）
- アイデンティティ ファイアウォールの設定 （11 ページ）
- アイデンティティ ファイアウォールのモニタリング （19 ページ）
- アイデンティティ ファイアウォールの履歴 （19 ページ）

アイデンティティ ファイアウォールについて

企業では、ユーザーが 1 つ以上のサーバー 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ー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。ユーザーごとにアクセス ポリシーを設定するには、ユーザー認証プロキシを設定する必要があります。これには、ユーザーとの対話（ユーザー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、ユーザー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ー名とユーザー 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ー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、特定の IP アドレスに対する現在のユーザーのアイデンティティ情報を取得する情報元として Windows Active Directory を使用し、Active Directory ユーザーのトランスペアレント認証を実現します。

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ー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ー アクティビティを容易に検出可能
- ユーザー 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 サーバーです。

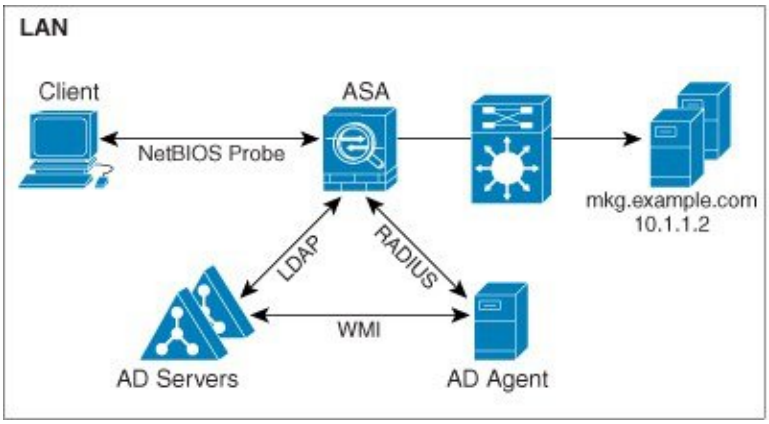
- Active Directory（AD）エージェント

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

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

次の図は、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 *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 ユーザー 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インします。AD サーバーは、ユーザーを認証し、ユーザー 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 サーバー**：ASA は、AD サーバーに設定された Active Directory グループに対する LDAP クエリを送信します。 ASA がローカル グループと Active Directory グループを統合し、ユーザー 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 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ーおよび応答がないユーザーを渡します。
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 とユーザーのデータベースをダウンロードするか、ユーザーの 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 サーバー**：AD エージェントは、ユーザー 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、ASA に変更を通知します。 AD エージェントは syslog サーバー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を実行するか、ユーザー 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ー 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。
- ユーザー 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。
- ユーザー 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。
- 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ー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ーが、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 サーバーをサポートします。
- ドメイン内の各ユーザー 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ー 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ー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ーを集約したものが、ユーザー総数です。
- アクティブな ASA ポリシーでサポートされるユーザー グループは、最大 512 個です。
- 1 つのアクセス ルールに 1 つ以上のユーザー グループまたはユーザー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

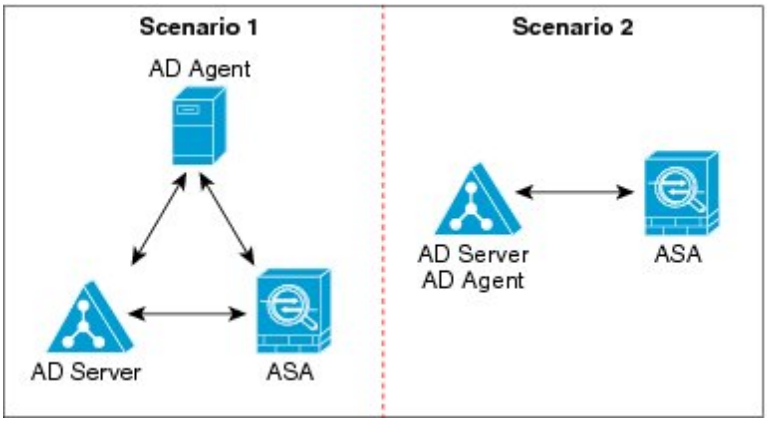
- ASA は、Active Directory からグループ情報を取得し、AD エージェントが送信元 IP アドレスをユーザー アイデンティティにマッピングできない場合に IP アドレスの Web 認証にフォールバックします。
- AD エージェントは、いずれかの Active Directory サーバーまたは ASA が応答しない場合でも機能し続けます。
- ASA でのプライマリ AD エージェントとセカンダリ AD エージェントの設定をサポートします。プライマリ AD エージェントが応答を停止すると、ASA がセカンダリ AD エージェントに切り替えます。
- AD エージェントが使用できない場合、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/ユーザー マッピング データベースを許可します。

導入シナリオ

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。

次の図 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 サーバーと AD エージェントが同一の Windows サーバーに共存しています。

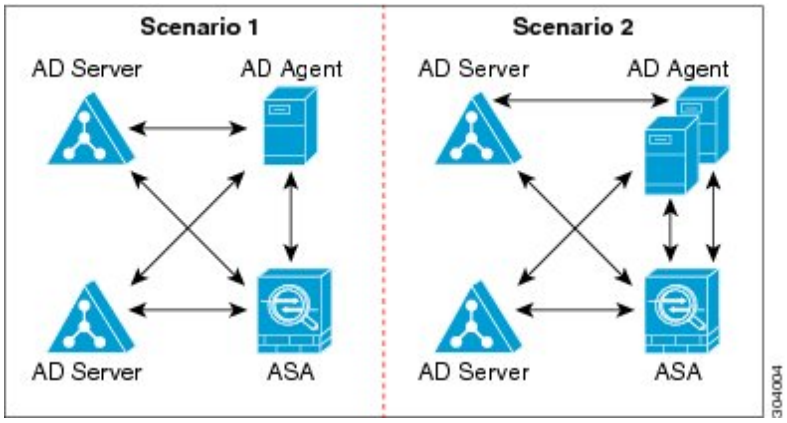
図 *2:* 冗長性のない展開シナリオ



次の図は、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 サーバーと、AD エージェントをインストールした 1 台の Windows サーバーを配置しています。シナリオ 2 では、

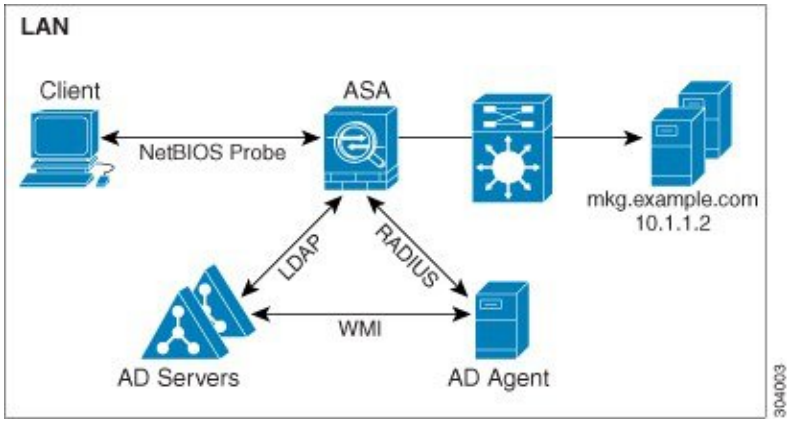
複数の Active Directory サーバーと、それぞれ AD エージェントがインストールされた複数の Windows サーバーを配置しています。

図 *3:* 冗長コンポーネントのある展開シナリオ



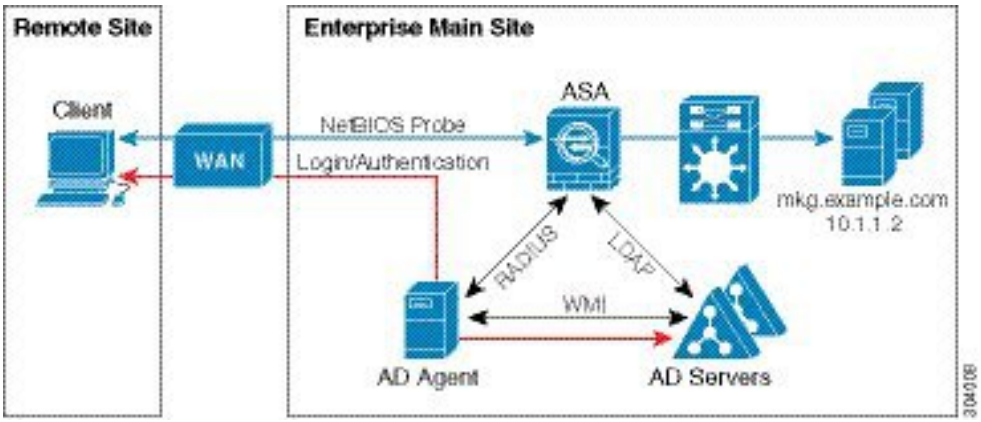
次の図は、LAN 上にすべてのアイデンティティ ファイアウォール コンポーネント（Active Directory サーバー、AD エージェント、クライアント）がインストールされ通信する方法を示しています。

図 *4:* *LAN* ベースの展開



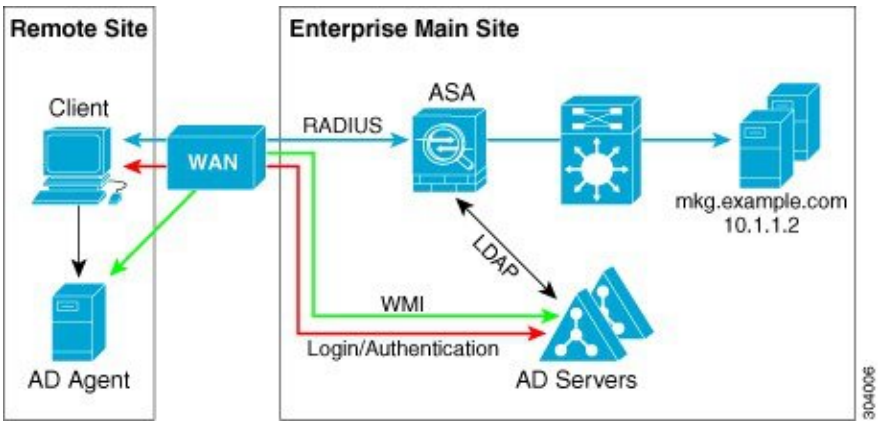
次の図は、WAN を使用したリモート サイトにまたがる展開方法を示しています。Active Directory サーバーと AD エージェントはメイン サイトの LAN 上に配置されています。クライアントはリモート サイトに配置されており、WAN 経由でアイデンティティ ファイアウォール コンポーネントに接続しています。

図 *5 : WAN* ベースの展開



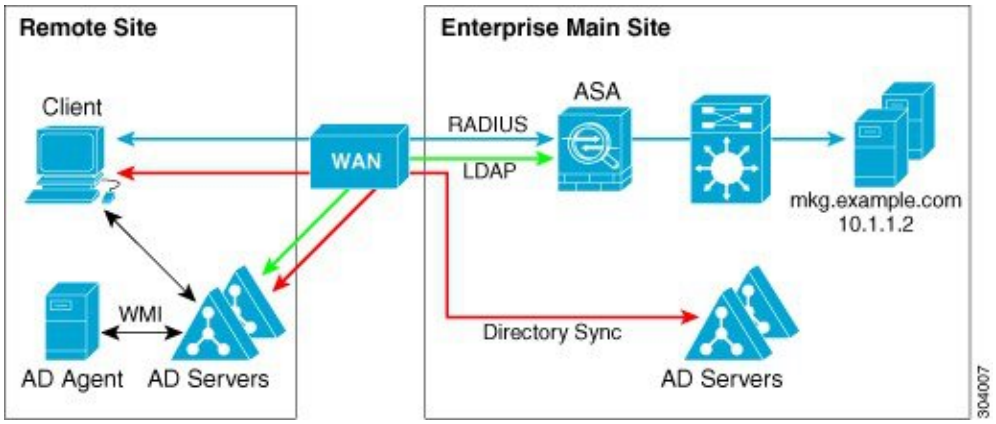
次の図も WAN を使用したリモート サイトにまたがる展開方法を示しています。Active Directory サーバーはメイン サイトの LAN にインストールされています。一方、AD エージェントはリモート サイトに配置され、同じサイト内のクライアントからアクセスされます。リモート クライアントは、WAN 経由でメイン サイトの Active Directory サーバーに接続します。

図 *6 :* リモート *AD* エージェントを使用した *WAN* ベースの展開



次の図は、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 サーバーがリモート 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 サーバーは、メイン サイトに配置された Active Directory サーバーとの間でデータを同期する必要があります。

図 *7: AD* エージェントと *AD* サーバーをリモート 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ガイドライン

ここでは、アイデンティティ ファイアウォールを設定する前に確認する必要があるガイドラインと制限事項について説明します。

フェールオーバー

- 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、ユーザー 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、ユーザー 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。ユーザーおよびユーザー 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ー 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。ユーザー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 サーバーで 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

- 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。AAA サーバーは IPv4 アドレスを使用する必要があります。

- 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

- 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ーには、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。
- VPN フィルタ ACL でユーザー仕様を使用できますが、ユーザーベースのルールは双方向ではなく単方向に解釈され、それが VPN フィルタが通常動作する仕組みです。つまり、ユーザーによって開始されたトラフィックに基づいてフィルタリングできますが、フィルタは宛先からユーザーに戻るものには適用されません。たとえば、サーバーへの ping を特定のユーザーに許可するルールを含めることができますが、そのルールでは、サーバーがユーザーに ping を実行することは許可されません。
- 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。
  - 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ー 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、ユーザー IP データベースが非常に大きく、前のダウンロード 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** コマンドを発行すると、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.”
  ```

  前のセッションが完全に終了するまで待つ必要があります。その後、別の **user-identity update active-user-database** コマンドを発行できます。

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ー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、許可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、その間このエラー 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 への許可要求の変更の送信に使用されます。

- **user-identity action domain-controller-down** *domain_name* **disable user-identity-rule** コマンドが設定されていて指定されたドメインがダウンしている場合、または **user-identity action ad-agent-down disable user-identity-rule** コマンドが設定されていて AD エージェントがダウンしている場合は、ログイン中のユーザーのステータスがディセーブルになります。
- ドメイン名では \/:*?"<>| の文字は無効です。
- ユーザー名では \/[]:;=,+*?"<>|@ の文字は無効です。
- ユーザー グループ名では \/[]:;=,+*?"<>| の文字は無効です。
- 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ー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 がオン デマンド取得とフル ダウンロード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ー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。

アイデンティティ ファイアウォールの前提条件

ここでは、 アイデンティティ ファイアウォールの設定に関する前提条件を示します。

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サーバー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サーバーから情報を取得し、ASAと通信するように設定します。

- サポートされる Windows サーバーは、Windows 2003、Windows 2008、および Windows 2008 R2 です。

（注） Windows 2003 R2 は、AD エージェント サーバー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 サーバー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 サーバーです。
- ASA に Active Directory サーバーを設定する前に、Active Directory に ASA のユーザー 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 サーバーに送信します。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方法については、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ーする各 Microsoft Active Directory サーバーの「*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 サーバー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

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。

手順

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

ステップ 2 ASA に AD エージェントを設定します。

ステップ 3 アイデンティティ オプションを設定します。

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。

Active Directory ドメインの設定

ASA が AD エージェントから IP とユーザーのマッピングを受信するときに、特定のドメインから Active Directory グループをダウンロードし、ユーザー 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。

始める前に

- Active Directory サーバーの 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 ユーザー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。

手順

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

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

ステップ 3 [Add] 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 [a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.] で構成される最大 32 文字のドメイン名を入力します。ただし、先頭に「.」と「 」（スペース）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、既存のユーザーおよびユーザー 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 このドメインに関連付ける Active Directory サーバーを選択するか、[Manage] をクリックして新しいサーバー グループをリストに追加します。

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。

Active Directory サーバー グループの設定

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

手順

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 [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 サーバー グループにサーバーを追加するには、[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。

Active Directory エージェントの設定

始める前に

- 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。

手順

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

ステップ 2 [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 [Add] ボタンをクリックします。

ステップ 5 [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。

Active Directory エージェント グループの設定

AD エージェント サーバー 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 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 サーバーは、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。

手順

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 ASA が AD エージェント サーバー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、[Primary Active Directory Agent] セクションにサーバーの 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 ASA が AD エージェント サーバー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、[Secondary Active Directory Agent] セクションにサーバーの 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 が続けて接続を実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。

アイデンティティ オプションの設定

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。

手順

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

ステップ 2 [Enable User Identity] チェック ボックスをオンにします。

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 [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ーに関連付けられているユーザー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ー IP アドレスがディセーブルとマークされます。

ステップ 5 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、ユーザー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、すべてのユーザーおよびユーザー 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、ユーザー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ー グループまたはユーザー（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ー）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、ユーザーと 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 ユーザー 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 6 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。[Manage] をクリックして、AD エージェント グループを追加します。

ステップ 7 [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 8 各 ID について受領する最後のイベント タイム スタンプを追跡し、イベントのタイム スタンプが ASA のクロックより 5 分以上古い場合、またはタイム スタンプが最後のイベントのタイ

ム スタンプよりも前の場合にすべてのメッセージを破棄するように ASA をイネーブルにするには、[Enable Event Timestamp] チェック ボックスをオンにします。

最後のイベントのタイム スタンプの情報がない新たに起動された ASA の場合は、ASA は自身のクロックとイベントのタイム スタンプを比較します。イベントから少なくとも 5 分以上経過している場合、ASA はメッセージを受け入れません。

NTP を使用して互いにクロックを同期させるように ASA、Active Directory、Active Directory エージェントを設定することを推奨します。

ステップ 9 [Poll Group Timer] フィールドに、完全修飾ドメイン名（FQDN）を解決するために ASA が DNS サーバーにクエリ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] セクションのリストから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 アドレスのユーザーがユーザー 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 アドレスのユーザー 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/ユーザー マッピング テーブル全体をダウンロードし、ユーザーのログインおよびログアウト時に増分 IP/ユーザー 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] を選択すると、受信パケットのユーザー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 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ーに関連付けられているユーザー 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ー 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 NetBIOS プローブが失敗した場合にユーザーの 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、ユーザーに対する NetBIOS プローブがブロックされた場合（たとえば、ユーザー 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。このオプションを選択すると、そのユーザー 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 ASA が現在ユーザーの 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、ユーザーの MAC アドレスを削除するかどうかを選択します。このオ

プションを選択すると、特定のユーザーに関連付けられているユーザー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 見つからないユーザーを追跡するかどうかを選択します。

ステップ 15 [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、アクティブユーザー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 がユーザーの 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、ユーザーの 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 とユーザー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） [Idle Timeout] オプションは VPN ユーザーまたはカットスルー プロキシ ユーザーには適用されません。

ステップ 16 NetBIOS プローブをイネーブルにし、ユーザーの 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 がユーザー ホストのプローブによってユーザー 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ー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 [User Name] リストから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ーのユーザー名が含まれている場合、ユーザー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 サーバー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ーのユーザー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 アドレスのユーザー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 サーバー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、ユーザー 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。

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（[Guidelines] セクション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ー アイデンティティ引数を追加できるようになりました。

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、ユーザー 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。

- 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、ユーザー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、ユーザーの 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ーの場合、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ー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ー名 None（有効なログインのないユーザー）および Any（有効なログインを持つユーザー）を指定します。アクセス ルールでは、ユーザー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 ユーザーを許可する AAA ルールを含めます。これらのユーザーが後で AAA ルールをトリガーできるように、これらのユーザーを許可する必要があります。次に、Any ユーザー（これらのユーザーは、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 ユーザーを許可する 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、レガシー機能ガイド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で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

アイデンティティ ファイアウォールの状態のモニタリングについては、次の画面を参照してください。

- **[Monitoring]** > **[Properties]** > **[Identity]** > **[AD Agent]**

  このペインには、AD エージェントおよびドメインのステータス、AD エージェントの統計情報が表示されます。

- **[Monitoring]** > **[Properties]** > **[Identity]** > **[Memory Usage]**

  このペインには、アイデンティティ ファイアウォールの ASA 上でのメモリ使用率が表示されます。

- **[Monitoring]** > **[Properties]** > **[Identity]** > **[User]**

- このペインには、アイデンティティ ファイアウォールで使用される IP/ユーザー マッピング データベースに含まれるすべてのユーザーに関する情報が表示されます。

- **[Monitoring]** > **[Properties]** > **[Identity]** > **[Group]**

  このペインには、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ー グループのリストが表示されます。

- **[Tools]** > **[Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

アイデンティティ ファイアウォールの履歴

表 *1:* アイデンティティ ファイアウォールの履歴

機能名	リリース	説明
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]**

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。