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

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、特定の IP アドレスに対する現在のユーザ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。

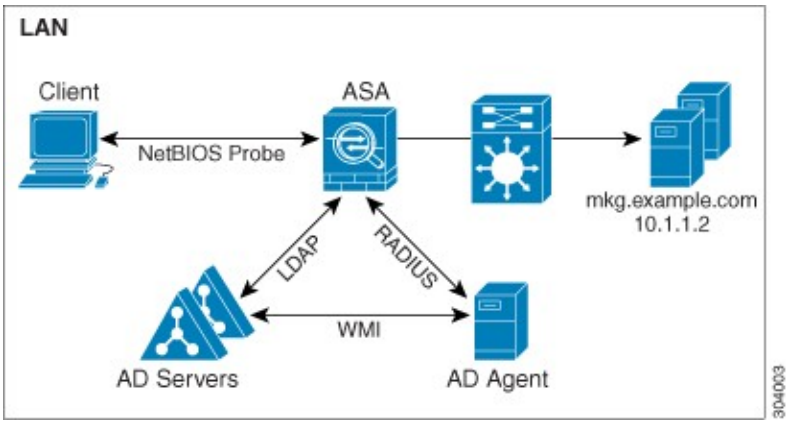
- Active Directory（AD）エージェント

  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。

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 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 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、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、ASA に変更を通知します。 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。
- 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 512 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。

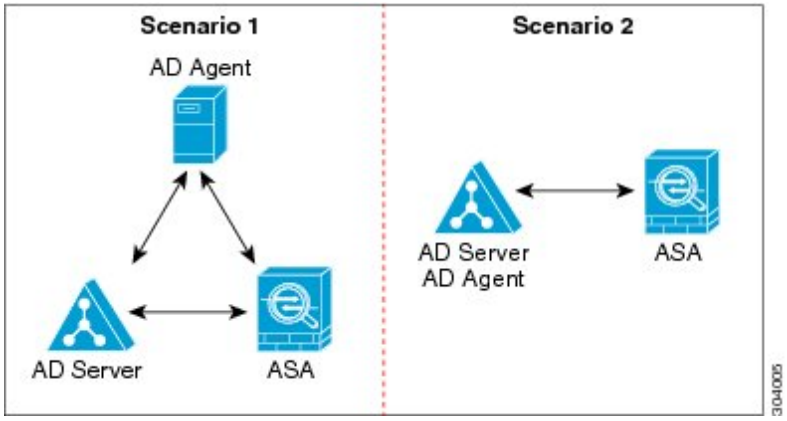
- ASA でのプライマリ AD エージェントとセカンダリ AD エージェントの設定をサポートします。プライマリ AD エージェントが応答を停止すると、ASA がセカンダリ AD エージェントに切り替えます。
- AD エージェントが使用できない場合、ASA はカットスルー プロキシや VPN 認証などの既存のアイデンティティ取得元にフォールバックできます。
- AD エージェントは、ダウンしたサービスを自動的に再開するウォッチドッグ プロセスを実行します。
- ASA 内で使用する分散 IP アドレス/ユーザ マッピング データベースを許可します。

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。

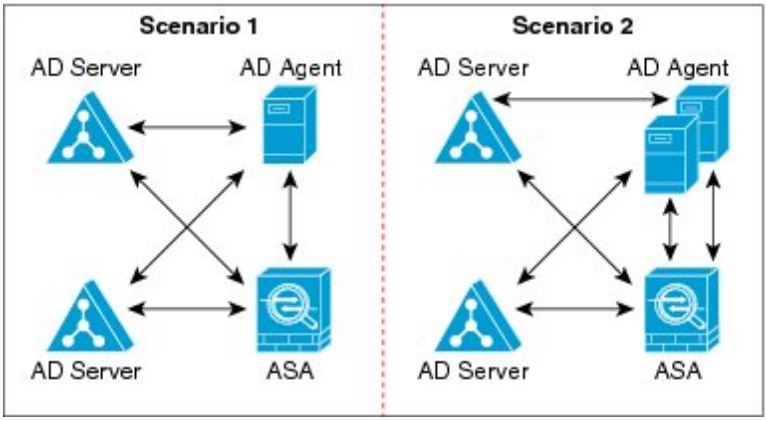
次の図 は、冗長性のためのアイデンティティ ファイアウォールのコンポーネントの展開方法を示しています。シナリオ1は、コンポーネントの冗長性がない単純なインストールを示しています。シナリオ2も、冗長性がない単純なインストールを示しています。ただし、この展開シナリオでは、Active Directory サーバと AD エージェントが同一の Windows サーバに共存しています。

図 *2:* 冗長性のない展開シナリオ



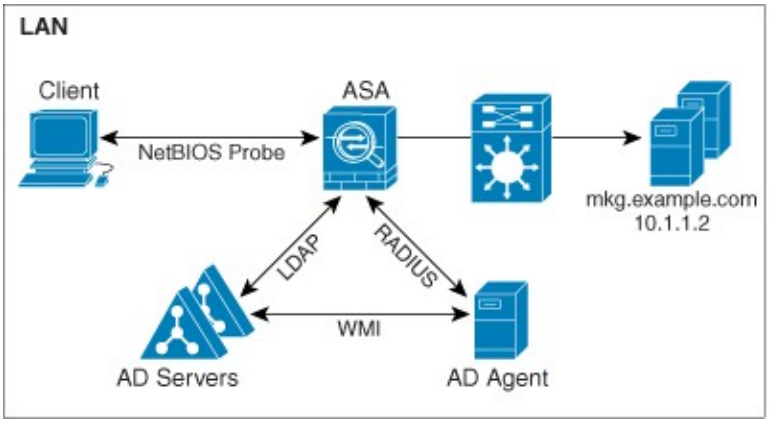
次の図は、冗長性をサポートするためのアイデンティティ ファイアウォールのコンポーネントの展開方法を示しています。シナリオ 1 では、複数の Active Directory サーバと、AD エージェントをインストールした 1 台の Windows サーバを配置しています。シナリオ 2 では、複数の Active Directory サーバと、それぞれ AD エージェントがインストールされた複数の Windows サーバを配置しています。

図 *3 :* 冗長コンポーネントのある展開シナリオ



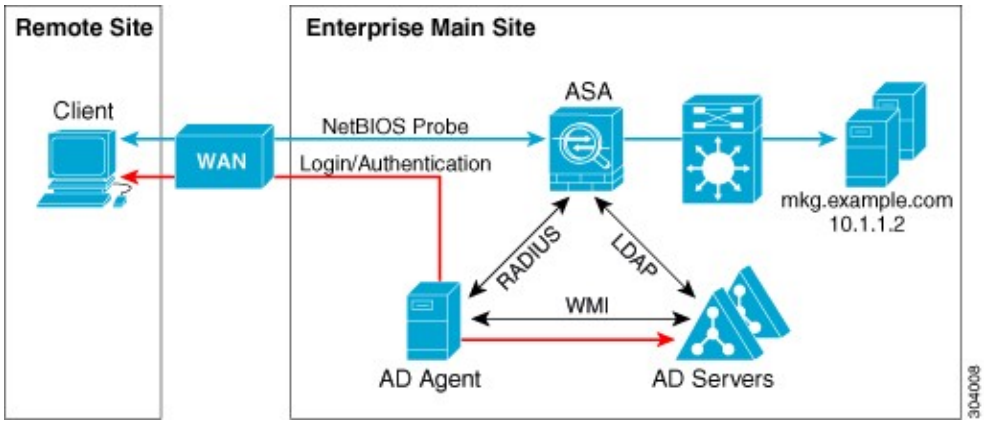
次の図は、LAN 上にすべてのアイデンティティ ファイアウォール コンポーネント（Active Directory サーバ、AD エージェント、クライアント）がインストールされ通信する方法を示しています。

図 *4 : LAN* ベースの展開



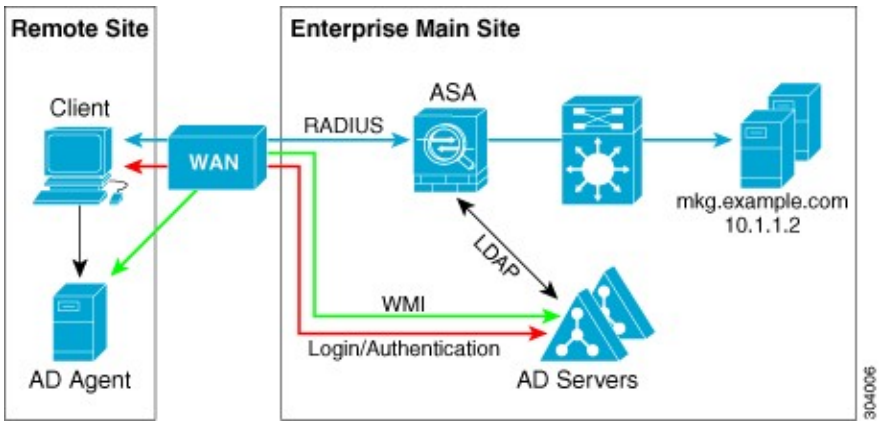
次の図は、WAN を使用したリモート サイトにまたがる展開方法を示しています。Active Directory サーバと AD エージェントはメイン サイトの LAN 上に配置されています。クライアントはリモート サイトに配置されており、WAN 経由でアイデンティティ ファイアウォール コンポーネントに接続しています。

図 *5 : WAN* ベースの展開



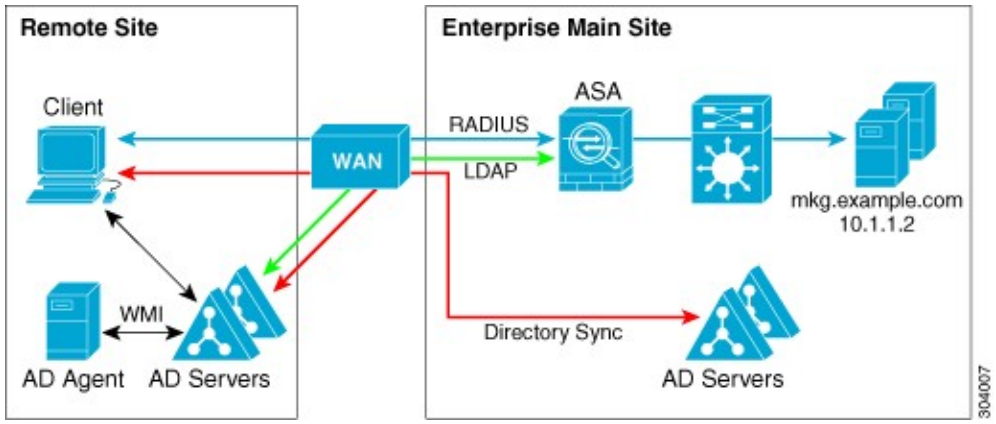
次の図も WAN を使用したリモート サイトにまたがる展開方法を示しています。Active Directory サーバはメイン サイトの LAN にインストールされています。一方、AD エージェントはリモート サイトに配置され、同じサイト内のクライアントからアクセスされます。リモート クライアントは、WAN 経由でメイン サイトの Active Directory サーバに接続します。

図 *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 *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

- 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 でユーザ仕様を使用できますが、ユーザ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に戻るものには適用されません。たとえば、サーバへの ping を特定のユーザ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、サーバがユーザに 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 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 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。
- ユーザ名では \/[]:;=,+*?"<>|@ の文字は無効です。
- ユーザ 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

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 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。

手順

ステップ 1 AAA サーバ グループを作成し、Active Directory サーバの AAA サーバ パラメータを設定します。

aaa-server *server-tag* **protocol ldap**

例：

```
ciscoasa(config)# aaa-server adserver protocol ldap
```

ステップ 2 AAA サーバを AAA サーバ グループの一部として設定し、Active Directory サーバに対してホスト固有の AAA サーバ パラメータを設定します。

aaa-server *server-tag* [(*interface-name*)] **host**{*server-ip* | *name*} [*key*] [**timeout***seconds*]

例：

```
ciscoasa(config-aaa-server-group)# aaa-server adserver (mgmt) host 172.168.224.6
```

ステップ 3 サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。

ldap-base-dn *string*

例：

```
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=SAMPLE,DC=com
```

ldap-base-dn コマンドの指定は任意です。このコマンドを指定しなかった場合、ASA は Active Directory から defaultNamingContext を取得し、それをベース DN として使用します。

ステップ 4 サーバが許可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-scope subtree

例：

```
ciscoasa(config-aaa-server-host)# ldap-scope subtree
```

ステップ 5 LDAP サーバのログイン パスワードを指定します。

ldap-login-password *string*

例：

```
ciscoasa(config-aaa-server-host)# ldap-login-password obscurepassword
```

ステップ 6 システムがバインドするディレクトリ オブジェクトの名前を指定します。

ldap-login-dn *string*

例：

```
ciscoasa(config-aaa-server-host)# ldap-login-dn SAMPLE\user1
```

ASAは、ログインDNフィールドをユーザ認証要求にアタッチして、認証済みバインディングに対して識別情報を示します。ログイン DN フィールドには、ASA の認証特性が記述されます。

string 引数は、LDAP 階層内のディレクトリ オブジェクトの名前を指定する、最大 128 文字の文字列です。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

従来の形式と簡易形式のどちらでも指定できます。

一般的な **ldap-login-dn** コマンドの形式は次のとおりです。CN= ユーザ名、OU= 従業員、OU= サンプル ユーザ、DC= サンプル、DC=com。

ステップ 7 Microsoft Active Directory サーバの LDAP サーバ モデルを設定します。

server-type microsoft

例：

```
ciscoasa(config-aaa-server-host)# server-type microsoft
```

ステップ 8 Active Directory ドメイン コントローラにおける Active Directory グループ設定の場所を指定します。

ldap-group-base-dn *string*

例：

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Sample Groups,DC=SAMPLE,DC=com
```

指定しない場合は、**ldap-group-base-dn**コマンドの値を使用します。このコマンドの指定は任意です。

ステップ 9 ASA が SSL 経由で Active Directory ドメイン コントローラとアクセスできるようにします。

ldap-over-ssl enable

例：

```
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
```

LDAP over SSL をサポートするには、Active Directory サーバがこのサポートを確保するように設定する必要があります。

デフォルトでは、Active Directory に SSL は設定されていません。Active Directory に SSL が設定されていない場合は、アイデンティティ ファイアウォールのために ASA に SSL を設定する必要はありません。

ステップ 10 サーバ ポートを指定します。

server-port *port-number*

例：

```
ciscoasa(config-aaa-server-host)# server-port 389

ciscoasa(config-aaa-server-host)# server-port 636
```

デフォルトでは、**ldap-over-ssl** コマンドがイネーブルになっていない場合、デフォルトのサーバ ポートは 389 になり、**ldap-over-ssl** コマンドがイネーブルになっている場合、デフォルトのサーバ ポートは 636 になります。

ステップ 11 LDAP クエリーがタイムアウトになるまでの時間を設定します。

group-search-timeout *seconds*

例：

```
ciscoasa(config-aaa-server-host)# group-search-timeout 300
```

Active Directory エージェントの設定

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 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。

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 AAA サーバ グループを作成し、AD エージェントの AAA サーバ パラメータを設定します。

aaa-server *server-tag* **protocol radius**

例：

```
ciscoasa(config)# aaa-server adagent protocol radius
```

ステップ 2 AD エージェント モードをイネーブルにします。

ad-agent-mode

例：

```
ciscoasa(config)# ad-agent-mode
```

ステップ 3 AAA サーバを AAA サーバ グループの一部として設定し、AD エージェントに対してホスト固有の AAA サーバ パラメータを設定します。

aaa-server *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout***seconds*]

例：

```
ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
```

ステップ 4 AD エージェント サーバに対する ASA の認証に使用されるサーバ秘密値を指定します。

key *key*

例：

```
ciscoasa(config-aaa-server-host)# key mysecret
```

ステップ 5 AD エージェントのサーバ グループを定義します。

user-identity ad-agent aaa-server *aaa_server_group_tag*

例：

```
ciscoasa(config-aaa-server-hostkey# user-identity ad-agent aaa-server adagent
```

aaa_server_group_tag 引数に定義する最初のサーバがプライマリ AD エージェントとなり、次に定義するサーバがセカンダリ ADエージェントとなります。アイデンティティ ファイアウォールでは、2 つの AD エージェント ホストのみ定義できます。

プライマリ AD エージェントが停止していることを 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、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 AAA サーバは通信プロトコルとして RADIUS を使用するため、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。

ステップ 6 ASA と AD エージェント サーバとの通信をテストします。

test aaa-server ad-agent

例：

```
ciscoasa(config-aaa-server-host)# test aaa-server ad-agent
```

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 アイデンティティ ファイアウォール機能をイネーブルにします。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。

user-identity enable

例：

```
ciscoasa(config)# user-identity enable
```

ステップ 2 アイデンティティ ファイアウォールのデフォルト ドメインを指定します。

user-identity default-domain *domain_NetBIOS_name*

例：

```
ciscoasa(config)# user-identity default-domain SAMPLE
```

domain_NetBIOS_name 用引数。[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「 」（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、名前全体を引用符で囲みます。ドメイン名では、大文字と小文字が区別されません。

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。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。

（注） 指定するデフォルト 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 アイデンティティと IP アドレスのマッピング エントリを 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。

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に対して LOCAL ドメインを使用します。Web ポータル（カットスルー プロキシ）経由でログインしたユーザは、認証された Active Directory ドメインに属すると見なされます。VPN が Active Directory で LDAP により認証されていない限り、VPN 経由でログインしたユーザは、ローカル ドメインに属すると見なされます。この場合は、アイデンティティ ファイアウォールは、Active Directory ドメインとユーザを関連付けることができます。

ステップ 3 AAA サーバでユーザ グループ クエリーのインポート用に定義された LDAP パラメータをドメイン名に関連付けます。

user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*

例：

```
ciscoasa(config)# user-identity domain SAMPLE aaa-server ds
```

domain_nickname 用引数。[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「 」（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。

ステップ 4 NetBIOS プローブをイネーブルにします。

user-identity logout-probe netbios local-system probe-time minutes *minutes***retry-interval seconds** *seconds***retry-count** *times* **user-not-needed** [**user-not-needed** | **match-any** | **exact-match**]

例：

```
ciscoasa(config)# user-identity logout-probe netbios
local-system probe-time minutes 10 retry-interval seconds 10
retry-count 2 user-not-needed
```

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 クライアント IP アドレスのプローブによって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。デフォルトでは、NetBIOS プローブはディセーブルになっています。NetBIOS パケットを最小限に抑えるために、ASA は、ユーザが指定された分数を超えて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。

- **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。
- **User-not-needed**：ASA がクライアントから 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。

アイデンティティ ファイアウォールは、少なくとも 1 つのセキュリティ ポリシーに存在するアクティブ状態のユーザアイデンティティに対してのみNetBIOSプローブを実行します。ASAは、ユーザがカットスルー プロキシ経由または VPN を使用してログインするクライアントについては、NetBIOS プローブを実行しません。

ステップ 5 ユーザがアイドル状態であると見なされるまでの時間を指定します。これは、ASAが指定された時間にわたりユーザの IP アドレスからトラフィックを受信しなかった場合を意味します。

user-identity inactive-user-timer minutes *minutes*

例：

```
ciscoasa(config)# user-identity inactive-user-timer minutes 120
```

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 キャッシュ内のユーザ アイデンティティと IP アドレスのマッピング データベースから削除されます。ASA は、この IP アドレスを 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。このコマンドを指定すると、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。

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 6 ASAがActive Directoryサーバにユーザ グループ情報を問い合わせるまでの時間を指定します。

user-identity poll-import-user-group-timer hours *hours*

例：

```
ciscoasa(config)# user-identity poll-import-user-group-timer hours1
```

Active Directory グループでユーザが追加または削除されると、ASA はグループ インポート タイマーの実行後に更新されたユーザ グループを受け取ります。デフォルトでは、**poll-import user-group-timer hours** 値は 8 時間です。

ユーザ グループ情報をただちに更新する場合は、**user-identity update import-user** コマンドを入力します。

ステップ 7 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を指定します。

user-identity action netbios-response-fail remove-user-ip

例：

```
ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip
```

このような状況には、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などがあります。

このコマンドを設定すると、ASA はそのクライアントのユーザ アイデンティティと IP アドレスのマッピングを削除します。

デフォルトでは、このコマンドはディセーブルです。

ステップ 8 Active Directory ドメイン コントローラが応答しないためにドメインがダウンしている場合のアクションを指定します。

user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**

例：

```
ciscoasa(config)# user-identity action domain-controller-down SAMPLE
disable-user-identity-rule
```

ドメインがダウンし、**disable-user-identity-rule** キーワードが設定されている場合、ASA はそのドメインのユーザ アイデンティティと IP アドレスのマッピングをディセーブルにします。さらに、**show user-identity user** コマンドによって表示される出力では、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。

デフォルトでは、このコマンドはディセーブルです。

ステップ 9 user-not-found トラッキングをイネーブルにします。デフォルトでは、このコマンドはディセーブルです。

user-identity user-not-found enable

例：

```
ciscoasa(config)# user-identity user-not-found enable
```

最後の 1024 個の IP アドレスだけがトラッキングされます。

ステップ 10 AD エージェントが応答していない場合のアクションを指定します。

user-identity action ad-agent-down disable-user-identity-rule

例：

```
ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule
```

AD エージェントがダウンしており、このコマンドが設定されている場合、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、**show user-identity user** コマンドによって表示される出力では、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。

デフォルトでは、このコマンドはディセーブルです。

ステップ 11 ユーザの MAC アドレスが、そのアドレスに現在マッピングされている ASA IP アドレスと一致しないことが明らかになった場合のアクションを指定します。

user-identity actionmac-address-mismatch remove-user-ip

例：

```
ciscoasa(config)# user-identity actionmac-address-mismatch remove-user-ip
```

このコマンドを設定すると、ASA はそのクライアントのユーザ アイデンティティと IP アドレスのマッピングを削除します。

デフォルトでは、このコマンドが指定されている場合、ASA は **remove-user-ip** キーワードを使用します。

ステップ 12 ASA が 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情報を取得する方法を定義します。

user-identity ad-agent active-user-database {**on-demand** | **full-download**}

例：

```
ciscoasa(config)# user-identity ad-agent active-user-database full-download
```

デフォルトでは、ASA は **full-download** オプションを使用します。

- **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 マッピング情報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。フル ダウンロードはイベント ドリブンです。つまり、2 回目以降のデータベース ダウンロード要求があった場合、ユーザ アイデンティティと IP アドレス マッピング データベースの更新内容だけが送信されます。
- **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。

ASA が変更要求を AD エージェントに登録すると、AD エージェントは新しいイベントを ASA に送信します。

ステップ 13 ASA と AD エージェントとの間の Hello タイマーを定義します。

user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

例：

```
ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3
```

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。

デフォルトでは、Hello タイマーは間隔が 30 秒、リトライ回数が 5 回に設定されます。

ステップ 14 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 をイネーブルにできます。

user-identity ad-agent event-timestamp-check

例：

```
ciscoasa(config)# user-identity ad-agent event-timestamp-check
```

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 15 AD エージェントのサーバ グループを定義します。

user-identity ad-agent aaa-server *aaa_server_group_tag*

例：

```
ciscoasa(config)# user-identity ad-agent aaa-server ad-agent
```

aaa_server_group_tag 引数には、**aaa-server** コマンドで定義された値を入力します。

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 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 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、レガシー機能ガイド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。
- 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。

ユーザ統計情報の収集

モジュラ ポリシー フレームワークによるユーザの統計情報の収集とアイデンティティ ファイアウォールの一致ルックアップ アクションをアクティブにするには、次の手順を実行します。

手順

モジュラ ポリシー フレームワークによるユーザ統計情報の収集と、アイデンティティ ファイアウォールの一致ルックアップ アクションをアクティブにします。

user-statistics [**accounting** | **scanning**]

例：

```
ciscoasa(config)# class-map c-identity-example-1
ciscoasa(config-cmap)# match access-list identity-example-1
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-mapp-identity-example-1
ciscoasa(config-pmap)# class c-identity-example-1
ciscoasa(config-pmap)# user-statistics accounting
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy p-identity-example-1 interface outside
```

accounting キーワードは、ASA が送信パケット カウント、送信ドロップ カウント、受信パケット カウントを収集することを指定します。**scanning** キーワードは、ASA が送信ドロップ カウントだけを収集することを指定します。

ユーザ統計情報を収集するようポリシー マップを設定すると、ASA は選択したユーザの詳細な統計情報を収集します。**user-statistics** コマンドを **accounting** または **scanning** キーワードなしで指定すると、ASA はアカウティング統計とスキャニング統計の両方を収集します。

アイデンティティ ファイアウォールの例

ここでは、アイデンティティ ファイアウォールの例を示します。

AAA ルールとアクセス ルールの例 1

次の例は、ユーザが ASA を介してログインすることを可能にする典型的なカットスルー プロキシ設定を示します。この例は次の条件に基づいています。

- ASA IP アドレスは 172.1.1.118 です。
- Active Directory ドメイン コントローラの IP アドレスは 71.1.2.93 です。
- エンドユーザ クライアントは、IP アドレスが 172.1.1.118 であり、HTTPS を使用して Web ポータル経由でログインします。
- ユーザは、LDAP を介して Active Directory ドメイン コントローラにより認証されます。
- ASA は、内部インターフェイスを使用して企業ネットワーク上の Active Directory ドメイン コントローラに接続します。

```
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255
eq http
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255
eq https
ciscoasa(config)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 171.1.2.93
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-dn
cn=kao,OU=Employees,OU=CiscoUsers,DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-login-password *****
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
ciscoasa(config-aaa-server-host)# aaa authentication match AUTH inside LDAP
ciscoasa(config)#
ciscoasa(config)# http server enable
ciscoasa(config)# http 0.0.0.0 0.0.0.0 inside
ciscoasa(config)#
ciscoasa(config)# auth-prompt prompt Enter Your Authentication
ciscoasa(config)# auth-prompt accept You are Good
ciscoasa(config)# auth-prompt reject Goodbye
```

AAA ルールとアクセス ルールの例 2

この例には、次のガイドラインが適用されます。

- **access-list** コマンドでは、未認証の着信ユーザが AAA カットスルー プロキシをトリガーできるように、**access-list 100 ex deny any any** コマンドを入力する前に permit user NONE ルールを設定する必要があります。
- **auth access-list** コマンドでは、permit user NONE ルールにより、未認証のユーザだけがカットスルー プロキシをトリガーします。これらを最後の行に指定することが理想的です。

```
ciscoasa(config)# access-list listenerAuth extended permit tcp any any
ciscoasa(config)# aaa authentication match listenerAuth inside ldap
ciscoasa(config)# aaa authentication listener http inside port 8888
ciscoasa(config)# access-list 100 ex permit ip user SAMPLE\user1 any any
ciscoasa(config)# access-list 100 ex deny ip user SAMPLE\user2 any any
ciscoasa(config)# access-list 100 ex permit ip user NONE any any
ciscoasa(config)# access-list 100 ex deny any any
ciscoasa(config)# access-group 100 in interface inside
ciscoasa(config)# aaa authenticate match 200 inside user-identity
```

VPN フィルタの例

ASA は、VPN 認証または Web ポータル（カットスルー プロキシ）によってログインしたユーザを AD エージェントに報告し、AD エージェントがユーザ情報を登録されているすべての ASA デバイスに配布します。具体的には、認証されたユーザの IP とユーザのマッピングが、HTTP/HTTPS パケットを受信して認証する入力インターフェイスを含むすべての ASA コンテキストに転送されます。ASA は、VPN 経由でログインするユーザを LOCAL ドメインに属するユーザと見なします。

VPN ユーザにアイデンティティ ファイアウォールのルールを適用するには 2 種類の方法があります。

- インターフェイス アクセス ルール（アイデンティティ ファイアウォール ルールが含まれている場合があります）が VPN ユーザに適用されていることを確認します。
- インターフェイス アクセス リストをバイパスしますが、VPN トラフィックに VPN フィルタを適用します。VPN フィルタには、アイデンティティ ファイアウォール ルールを含めることができます。

次のトピックに例を示します。

インターフェイス アクセス ルールを VPN トラフィックに適用する例

デフォルトでは **sysopt connection permit-vpn** コマンドがイネーブルになり、VPN トラフィックはアクセス リスト チェックの対象外となります。VPN トラフィックにインターフェイスに基づく ACL ルールを適用するには、VPN トラフィック アクセス リストのバイパスを無効にする必要があります。

この例では、ユーザが外部インターフェイスからログインすると、アイデンティティ ファイアウォール ルールはアクセス可能なネットワーク リソースを制御します。すべての VPN ユーザは LOCAL ドメインに保存されます。したがって、LOCAL ユーザまたは LOCAL ユーザを含むオブジェクト グループへのルールの適用のみが意味を持ちます。

```
 ! Apply VPN-Filter with bypassing access-list check disabled
no sysopt connection permit-vpn
access-list v1 extended deny ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended permit ip user LOCAL\idfw any 20.0.0.0 255.255.255.0
access-group v1 in interface outside
```

ユーザ仕様による VPN フィルタの適用例

デフォルトでは **sysopt connection permit-vpn** コマンドがイネーブルになり、VPN トラフィックはアクセス リスト チェックの対象外となります。VPN フィルタを使用して、VPN トラフィックにアイデンティティ ファイアウォール ルールを適用できます。ユーザ名とグループ ポリシーのアイデンティティ ファイアウォール ルールを使用して VPN フィルタを定義できます。

この例では、ユーザ idfw がログインすると、ユーザは、10.0.00/24 サブネットのネットワーク リソースにアクセスできます。これに対し、ユーザ user1 がログインした場合は、10.0.00/24 サブネット内のネットワーク リソースへのアクセスは拒否されます。すべての VPN ユーザが LOCAL ドメインに保存されることに注意してください。したがって、LOCAL ユーザまたは LOCAL ユーザを含むオブジェクト グループへのルールの適用のみが意味を持ちます。

（注） VPN フィルタ ACL でユーザ仕様を使用できますが、ユーザ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に戻るものには適用されません。たとえば、サーバへの ping を特定のユーザ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、サーバがユーザに ping を実行することは許可されません。

```
! Apply VPN-Filter with bypassing access-list check enabled
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v2 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
username user1 password QkBIIYVi6IFLEsYv encrypted privilege 0
username user1 attributes
    vpn-group-policy group1 vpn-filter value v2
username idfw password eEm2dmjMaopcGozT encrypted
username idfw attributes
    vpn-group-policy testgroup vpn-filter value v1
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
group-policy group1 internal
group-policy group1 attributes
    vpn-filter value v1
    vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
```

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、次のコマンドを参照してください。

- **show user-identity ad-agent**

  このコマンドは、AD エージェントおよびドメインのステータスを表示します。

- **show user-identity ad-agent statistics**

  このコマンドは、ADエージェントの統計情報を表示します。

- **show user-identity memory**

  このコマンドは、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を表示します。

- **show user-identity user all list**

  このコマンドは、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 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します。

- **show user-identity user active user** *domainuser-name***list detail**

  このコマンドは、アクティブ ユーザに関する追加情報を表示します。

- **show user-identity group**

  このコマンドは、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 グループのリストを表示します。

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。 **user-identity enable**、**user-identity default-domain**、**user-identity domain**、**user-identity logout-probe**、**user-identity inactive-user-timer**、**user-identity poll-import-user-group-timer**、**user-identity action netbios-response-fail**、**user-identity user-not-found**、**user-identity action ad-agent-down**、**user-identity action mac-address-mismatch**、**user-identity action domain-controller-down**、**user-identity ad-agent active-user-database**、**user-identity ad-agent hello-timer**、**user-identity ad-agent aaa-server**、**user-identity update import-user**、**dns domain-lookup**、**dns poll-timer**、**dns expire-entry-timer**、**object-group user,** **show user-identity**、**show dns**、**clear configure user-identity**、**clear dns**、**debug user-identity** の各コマンドが導入または変更されました。