CHAPTER 33

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 ファイアウォール向けに ASA を設定する方法について説明します。この章は、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 モニタリングの簡略化

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 の管理者によって行われます。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。

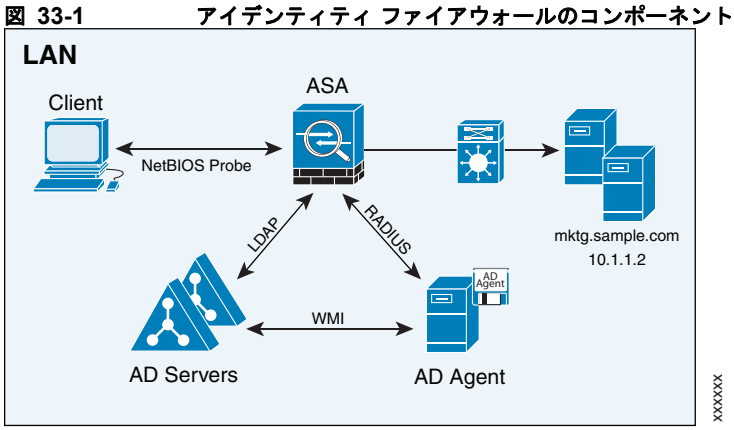
  サポートされているバージョンは、Windows 2003、Windows Server 2008、および Windows Server 2008 R2 サーバです。

- **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 33-1　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**：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 ログオン 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 プロキシ経由で、または VPN を使用して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 MPF 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 アドレスをクエリーする AD エージェントに RADIUS 要求を送信します。 ASA が 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を AD エージェントに転送します。	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オフ 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 デバイスに読み込まれます。

拡張性

- 各 AD エージェントは 100 台の ASA デバイスをサポートします。複数の ASA デバイスが 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 ASA 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。ユーザの総数は、すべてのコンテキストに設定されたユーザの合計です。
- ASA 5505 のアクティブな ASA 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 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 デバイス間での IP アドレスとユーザのマッピング データベースの分散が可能です。

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 33-2 に示すように、冗長性を確保するようにアイデンティティ ファイアウォールのコンポーネントを展開できます。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 1 つの Windows サーバに共存しています。

図 33-2　冗長性のない展開シナリオ
No Redundancy

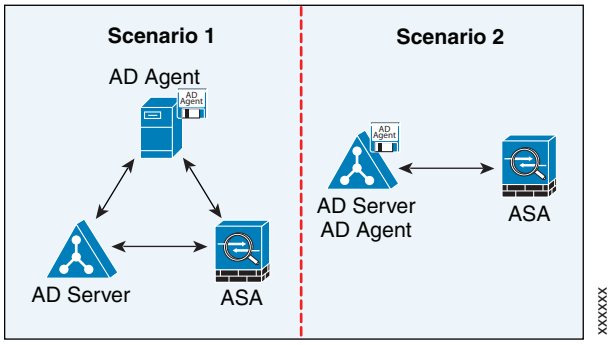


図 33-3 に示すように、冗長性をサポートするようにアイデンティティ ファイアウォールのコンポーネントを展開できます。シナリオ 1 では、複数の Active Directory サーバと、AD エージェントをインストールした 1 台の Windows サーバを配置しています。シナリオ 2 では、複数の Active Directory サーバと、それぞれ AD エージェントがインストールされた複数の Windows サーバを配置しています。

図 33-3　冗長コンポーネントのある展開シナリオ
Redundant

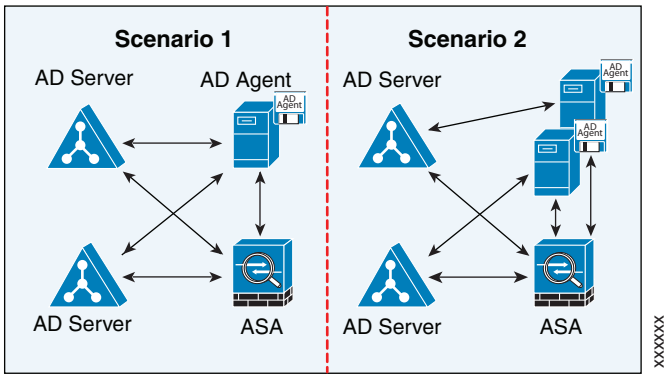


図 33-4 に示すように、すべてのアイデンティティ ファイアウォール コンポーネント（Active Directory サーバ、AD エージェント、およびクライアント）がインストールされ、LAN 上で通信しています。

図 33-4　LAN ベースの展開

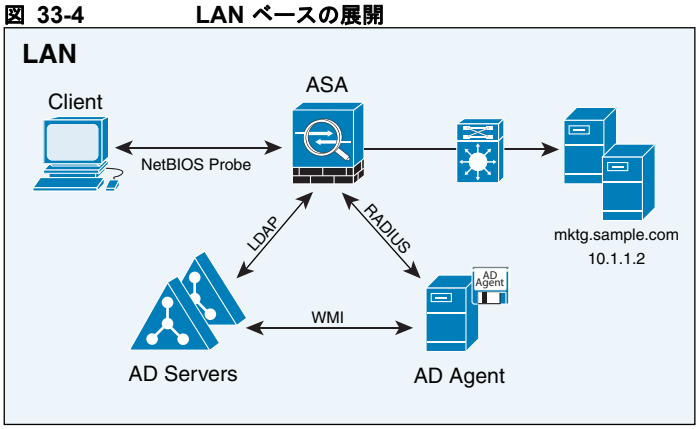


図 33-5 は、WAN を使用してリモート サイトと接続した展開方法を示しています。Active Directory サーバと AD エージェントはメイン サイトの LAN 上に配置されています。クライアントはリモート サイトに配置されており、WAN 経由でアイデンティティ ファイアウォール コンポーネントに接続しています。

図 33-5　WAN ベースの展開

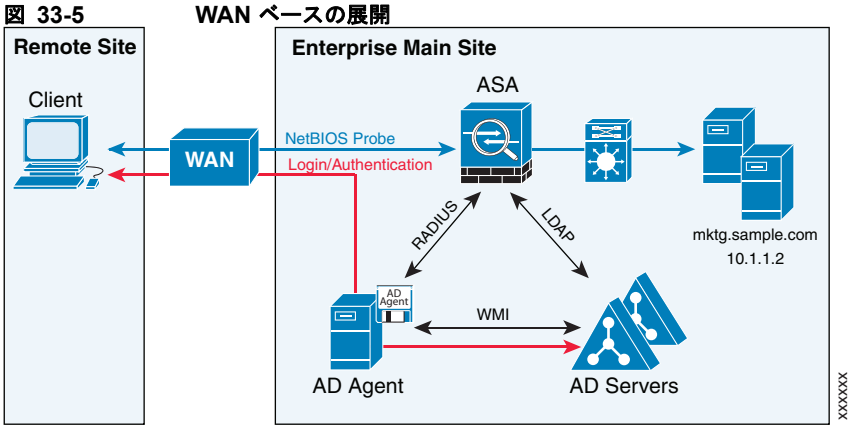


図 33-6 も WAN を使用したリモート サイトにまたがる展開方法を示しています。Active Directory サーバはメイン サイトの LAN にインストールされています。一方、AD エージェントはリモート サイトに配置され、同じサイト内のクライアントからアクセスします。リモート クライアントは、WAN 経由でメイン サイトの Active Directory サーバに接続します。

図 33-6　リモート AD エージェントを使用した WAN ベースの展開

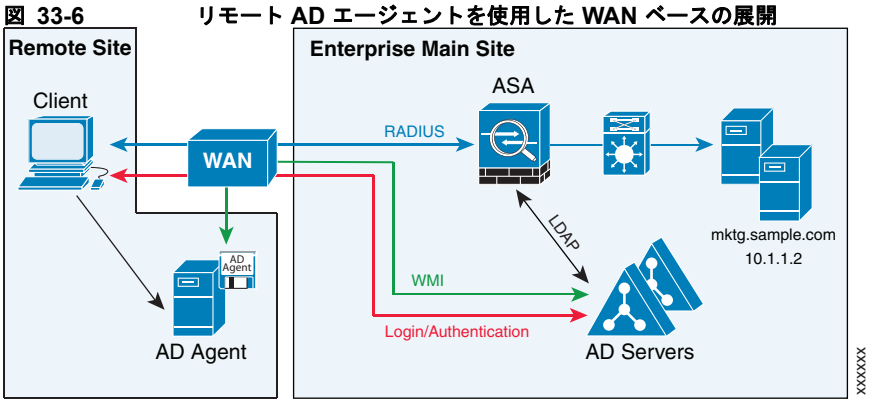
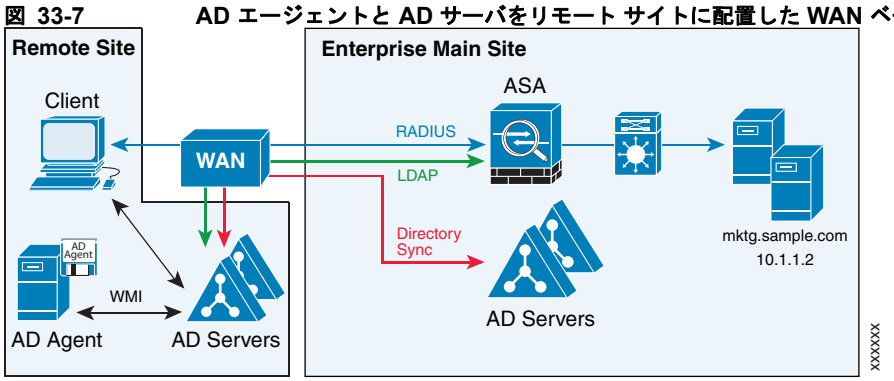


図 33-7 は、リモート サイトを拡張した WAN ベースの展開を示しています。AD エージェントと Active Directory サーバがリモート サイトに配置されています。クライアントは、メイン サイトに配置されているネットワーク リソースにログインする際に、これらのコンポーネントにローカルでアクセスします。リモート Active Directory サーバは、メイン サイトに配置された Active Directory サーバとの間でデータを同期する必要があります。

図 33-7　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 デバイス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
  - group-policy（VPN フィルタを除く）
  - DAP

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するように設定する必要があります。AD エージェントを 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 サーバに次のパッチをインストールする必要があります。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。『*README First for the Cisco Active Directory Agent*』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設定

ここでは、次の項目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」（P.33-9）
- 「Active Directory ドメインの設定」（P.33-10）
- 「Active Directory エージェントの設定」（P.33-12）
- 「アイデンティティ オプションの設定」（P.33-13）
- 「Identity-Based セキュリティ ポリシーの設定」（P.33-20）

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.33-10）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.33-5）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 エージェントの設定」（P.33-12）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.33-5）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.33-13）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.33-20）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。

	コマンド	目的

ステップ 1	`hostname(config)# aaa-server server-tag protocol ldap`
	Example:
	`hostname(config)# aaa-server adserver protocol ldap`
		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。

ステップ 2	`hostname(config-aaa-server-group)# aaa-server server-tag [(interface-name)] host {server-ip | name} [key] [timeout seconds]` **Example:** hostname(config-aaa-server-group)# aaa-server adserver (mgmt) host 172.168.224.6	Active Directory サーバに対し、AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の AAA サーバ パラメータを設定します。

ステップ 3	`hostname(config-aaa-server-host)# ldap-base-dn string`
	Example:
	`hostname(config-aaa-server-host)# ldap-base-dn DC=SAMPLE,DC=com`
		サーバが許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 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	`hostname(config-aaa-server-host)# ldap-scope subtree`	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。

	コマンド	目的
ステップ 5	hostname(config-aaa-server-host)# **ldap-login-password** *string* **Example:** hostname(config-aaa-server-host)# ldap-login-password obscurepassword	LDAP サーバのログイン パスワードを指定します。
ステップ 6	hostname(config-aaa-server-host)# **ldap-login-dn** *string* **Example:** hostname(config-aaa-server-host)#ldap-login-dn SAMPLE\user1	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。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* 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。 従来の ldap-login-dn 形式には、CN=username、OU=Employees、OU=Sample Users があります。DC=sample、DC=com も使用できます。
ステップ 7	hostname(config-aaa-server-host)# **server-type microsoft**	Microsoft Active Directory サーバの LDAP サーバモデルを設定します。
ステップ 8	hostname(config-aaa-server-host)# **ldap-group-base-dn** *string* **Example:** hostname(config-aaa-server-host)# ldap-group-base-dn OU=Sample Groups,DC=SAMPLE,DC=com	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。指定しない場合、ldap-base-dn の値が使用されます。 **ldap-group-base-dn** コマンドの指定は任意です。
ステップ 9	hostname(config-aaa-server-host)# **ldap-over-ssl enable**	ASA が SSL 上で 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 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	hostname(config-aaa-server-host)# **server-port** *port-number* **Examples:** hostname(config-aaa-server-host)# server-port 389 hostname(config-aaa-server-host)# server-port 636	デフォルトでは、ldap-over-ssl がイネーブルになっていない場合、server-port のデフォルトは 389 となります。ldap-over-ssl がイネーブルになっている場合、server-port のデフォルトは 636 となります。
ステップ 11	hostname(config-aaa-server-host)# **group-search-timeout** *seconds* **Examples:** hostname(config-aaa-server-host)# group-search-timeout 300	LDAP クエリー タイムアウトになるまでの時間を設定します。

次の作業

AD エージェントを設定します。「Active Directory エージェントの設定」（P.33-12）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 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。

要件

- 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。

	コマンド	目的
ステップ 1	hostname(config)# **aaa-server** *server-tag* **protocol radius** **Example:** hostname(config)# aaa-server adagent protocol radius	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。
ステップ 2	hostname(config)# **ad-agent-mode**	AD エージェント モードをイネーブルにします。
ステップ 3	hostname(config-aaa-server-group)# **aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*] **Example:** hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101	AD エージェントに対し、AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の AAA サーバ パラメータを設定します。
ステップ 4	hostname(config-aaa-server-host)# **key** *key* **Example:** hostname(config-aaa-server-host)# key mysecret	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。

	コマンド	目的
ステップ 5	hostname(config-aaa-server-host)# **user-identity ad-agent aaa-server** *aaa_server_group_tag* **Examples:** hostname(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent	AD エージェントのサーバ グループを定義します。 *aaa_server_group_tag* 変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 エージェントがダウンしていることを 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 aaa-server 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	hostname(config-aaa-server-host)# **test aaa-server ad-agent**	ASA と AD エージェント サーバとの通信をテストします。

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.33-20）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

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、次の手順を実行します。この機能をイネーブルにするには、[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.33-8）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。

	コマンド	目的
ステップ 1	hostname(config)# **user-identity enable**	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。
ステップ 2	hostname(config)# **user-identity default-domain** *domain_NetBIOS_name* **Example:** hostname(config)# user-identity default-domain SAMPLE	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。 *domain_NetBIOS_name* には、[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、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 経由でログインしたユーザは、VPN が Active Directory で LDAP によって認証される場合を除き、LOCAL ドメインに属するユーザと見なされます。これにより、アイデンティティ ファイアウォールはユーザをそれぞれの Active Directory ドメインに関連付けることができます。

	コマンド	目的
ステップ 3	hostname(config)# **user-identity domain** *domain_nickname* **aaa-server** *aaa_server_group_tag* **Example:** hostname(config)# user-identity domain SAMPLE aaa-server ds	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。 *domain_nickname* には、[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。

	コマンド	目的
ステップ 4	hostname(config)# **user-identity logout-probe netbios local-system probe-time minutes** *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed**|**match-any**|**exact-match**] **Example:** hostname(config)# user-identity logout-probe netbios local-system probe-time minutes 10 retry-interval seconds 10 retry-count 2 user-not-needed	NetBIOS プローブをイネーブルにします。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 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。 NetBIOS プローブ タイマーを 1 ～ 65535 分に設定し、リトライ インターバルを 1 ～ 256 回に設定します。プローブのリトライ回数は、次のように指定してください。 • **match-any**：クライアントからの 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ためには、クライアントで 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ためには、クライアントで 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。

	コマンド	目的
ステップ 5	hostname(config)# **user-identity inactive-user-timer minutes** *minutes* **Example:** hostname(config)# user-identity inactive-user-timer minutes 120	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 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。 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 アドレスの削除を 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。 **（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 6	hostname(config)# **user-identity poll-import-user-group-timer hours** *hours* **Example:** hostname(config)# user-identity poll-import-user-group-timer hours 1	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。 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** の値は 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、次のコマンドを入力します。 **user-identity update import-user** CLI コンフィギュレーション ガイドを参照してください。
ステップ 7	hostname(config)# **user-identity action netbios-response-fail remove-user-ip**	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。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。 **user-identity action remove-user-ip** 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。

	コマンド	目的
ステップ 8	hostname(config)# **user-identity action domain-controller-down** *domain_nickname* **disable-user-identity-rule** **Example:** hostname(config)# user-identity action domain-controller-down SAMPLE disable-user-identity-rule	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。 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	hostname(config)# **user-identity user-not-found enable**	user-not-found トラッキングをイネーブルにします。最後の 1024 個の IP アドレスだけがトラッキングされます。 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 10	hostname(config)# **user-identity action ad-agent-down disable-user-identity-rule**	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。 AD エージェントがダウンし、**user-identity action ad-agent-down** が設定されている場合、ASA はそのドメインのユーザに関連付けられたユーザ アイデンティティ ルール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 11	hostname(config)# **user-identity action mac-address-mismatch remove-user-ip**	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 デバイス 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 action mac-address-mismatch** コマンドが設定されている場合、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。

	コマンド	目的
ステップ 12	hostname(config)# **user-identity ad-agent active-user-database** {**on-demand**|**full-download**} **Example:** hostname(config)# user-identity ad-agent active-user-database full-download	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。 • **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。 • **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。 デフォルトでは、ASA 5505 は on-demand オプションを使用します。それ以外の ASA プラットフォームは full-download オプションを使用します。 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 ダウンロード要求は、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を送信します。 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	hostname(config)# **user-identity ad-agent hello-timer seconds** *seconds* **retry-times** *number* **Example:** hostname(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 タイマーを定義します。 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。 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	hostname(config)# **user-identity ad-agent aaa-server** *aaa_server_group_tag* **Example:** hostname(config)# user-identity ad-agent aaa-server adagent	AD エージェントのサーバ グループを定義します。 *aaa_server_group_tag* には、**aaa-server** コマンドで定義された値を入力します。

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.33-10）を参照してください。

AD エージェントを設定します。「Active Directory エージェントの設定」（P.33-12）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.33-7）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、第 19 章「拡張アクセス コントロール リストの追加」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.17-11）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 6, “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。

```
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   ----> these users will match AAA rule
access-list 100 ex deny any any
access-group 100 in interface inside

access-list 200 ex deny ip user ANY any any -----> skips users who already logged in
access-list 200 ex permit user NONE any any
aaa authenticate match 200 inside user-identity
```

ファイアウォール コンフィギュレーション ガイドの Chapter 7, “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 22, “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）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。

- その他多数 ...

例

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 の 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、Inside 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。

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

AAA ルールとアクセス ルールの例 2

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

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、「permit user NONE」ルールを「access-list 100 ex deny any any」の前に指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。

VPN フィルタの例

一部のトラフィックでアイデンティティ ファイアウォールをバイパスすることが必要となる場合があります。

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 IDFW ルールを適用するには、次の 2 つの方法があります。

- Apply VPN-Filter with bypassing access-list check disabled
- Apply VPN-Filter with bypassing access-list check enabled

設定例 -- VPN への IDFW ルールの適用 - 1

デフォルトでは、「sysopt connection permit-vpn」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 トラフィックに通常のインターフェイスに基づく ACL ルールを適用するには、VPN トラフィックのアクセス リスト バイパスをディセーブルにする必要があります。

この例では、ユーザが outside インターフェイスからログインすると、IDFW ルールにより、アクセス可能なネットワーク リソースが決定されます。VPN ユーザは、すべてドメイン LOCAL 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        >> Control VPN user based on regular IDFW ACLs
```

設定例 -- VPN への IDFW ルールの適用 - 2

デフォルトでは、"sysopt connection permit-vpn" がイネーブルになり、VPN トラフィックのアクセス バイパスもイネーブルになります。VPN-filter を使用することにより、VPN トラフィックに IDFW ルールを適用できます。IDFW ルールを指定した VPN-filter は、CLI ユーザ名と group-policy で定義できます。

この例では、ユーザ idfw がログインすると、10.0.00/24 サブネット内のネットワーク 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。VPN ユーザがすべてドメイン LOCAL 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）IDFW ルールは group-policy に基づく vpn-filter にのみ適用でき、他の group-policy 機能では使用できません。

```
!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         >> Per user VPN-filter control
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           >> Per group VPN-filter control

    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

ここでは、次の項目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できます。

次の **show user-identity** コマンド オプションを使用することにより、AD エージェントのトラブルシューティング情報を取得できます。

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

これらのコマンドは、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を表示します。

- 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 グループをモニタできます。

show user-identity group コマンドを使用することにより、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 グループのトラブルシューティング情報を取得できます。

このコマンドは、ユーザ グループのリストを次の形式で表示します。

*domain**group_name*

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

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をモニタできます。

show user-identity memory コマンドを使用することにより、アイデンティティ ファイアウォールのトラブルシューティング情報を取得できます。

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バイト単位で表示します。

- 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 ログオン 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） Identity Firewall 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** 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。これらのオプションの説明については、「アイデンティティ オプションの設定」（P.33-13）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できます。

次の **show user-identity** コマンド オプションを使用することにより、AD エージェントのトラブルシューティング情報を取得できます。

- **show user-identity user all list**
- **show user-identity user active user** *domain\user-name* **list detail**

これらのコマンドは、ユーザに関する次の情報を表示します。

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）
domain\user_name	アクティブな接続	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。

（注）　最初の 3 つのタブ

コマンド **user-identity action domain-controller-down** *domain_name* **disable-user-identity-rule** が設定されていて、指定されたドメインがダウンした場合、または **user-identity action ad-agent-down disable-user-identity-rule** が設定されていて、AD エージェントがダウンした場合には、ログオンしたすべてのユーザのステータスがディセーブルとなります。

アイデンティティ ファイアウォールの機能履歴

表 33-1 に、この機能のリリース履歴を示します。

表 33-1　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。 **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**、**user**-identity static 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。