ID 認証ファイアウォール ポリシーの管理

ID 認証ファイアウォールポリシーを使用すると、ユーザー ID またはホストの完全修飾ドメイン名に基づいてトラフィックを制御できます。たとえば、すべてのトラフィックを許可または禁止する代わりに、あるユーザーグループに対しては特定のタイプのトラフィックを選択的に許可し、別のユーザーグループに対しては許可しないようにできます。完全修飾ドメイン名を使用すると、特定のサーバーへの HTTP アクセスを禁止し、他の全サーバーへの HTTP トラフィックを許可できます。

アイデンティティ認識は複数の既存のファイアウォール ルールに組み込まれます。固有の ID 認証ファイアウォール ポリシーはありません。この章では、ID認証ファイアウォールポリシーと、ID 認証をサポートするさまざまなポリシーに ID 認証ファイアウォールポリシーを実装する方法について説明します。

この章は次のトピックで構成されています。

- ID 認証ファイアウォールポリシーの概要　（1 ページ）
- ID 認証ファイアウォール ポリシーの設定　（9 ページ）
- アイデンティティ ファイアウォール ポリシーの監視　（35 ページ）

ID 認証ファイアウォールポリシーの概要

従来のファイアウォールポリシーでは、送信元と宛先の IP アドレス、ポート、およびサービスに基づいて決定が行われます。ASA におけるアイデンティティ ファイアウォールは、以下のいずれか、または両方に基づいたより細かな制御を実現します。

- ユーザー ID：送信元 IP アドレス単独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に基づい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。AD エージェントのセットアップおよび設定の詳細については、Cisco.com（http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html）の*Active Directory* エージェントインストール/セットアップガイド [英語] を参照してください。

- FQDN ネットワークオブジェクト：ホストの IP アドレスではなく、完全修飾ドメイン名（FQDN）をルールで使用できるため、ホストのアドレスが変更された場合（DHCP を介してアドレスを取得する場合など）、ルールは引き続き適用されます。

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、送信元または宛先 IP アドレスの代わりに、送信元および FQDN としてユーザーまたはグループを指定できるようにすることで、既存のアクセス制御メカニズムとセキュリティポリシー メカニズムを強化します。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。ユーザーが接続するネットワークの場所に関係なく、ルールがユーザーに適用されます。
- 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 モニタリングの簡略化。

ここでは、次の内容について説明します。

- ユーザー ID の取得　（2 ページ）
- ID 認証ファイアウォール ポリシーの要件　（3 ページ）
- ID 認証サービスを提供するためのファイアウォールの設定　（8 ページ）

ユーザー ID の取得

ファイアウォールポリシーで Active Directory ユーザ名またはユーザグループ名を指定する場合、ASA は最終的にその名前を IP アドレスにマッピングして、パケットを処理する必要があります。ASA はこの情報に次の 2 つのプライマリ ソースを使用します。

- ユーザ グループ メンバーシップ：ルールでユーザグループを指定すると、ASA は設定された Active Directory（AD）サーバーに接続して、グループメンバーシップを取得します。
- ユーザから IP アドレスへのマッピング：標準（VPN 以外）ネットワーク上のネットワーク ドメインにログインするユーザに対して、AD エージェントは、AD サーバーとの通信で、ログイン情報を取得し、ユーザから IP アドレスへのマッピングテーブルを作成します。この情報は ASA に提供されます。

ユーザベースのアイデンティティ ファイアウォール ポリシーを構成する前に、必要な AD サーバーとエージェントをインストールして構成する必要があります。さまざまな導入シナリオの説明については、http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_

guides_list.htmlにある ASDM または CLI の ASA コンフィギュレーション ガイドを参照してください。

ユーザ名は、次のタイプのトラフィックに対して取得され、特に記載がない限り、AD ドメインが含まれます。

- 標準トラフィック。
- IPsec IKEv1 および IKEv2、AnyConnect クライアント、および L2TP VPN を含むリモートアクセス VPN。VPN に LDAP 認証を使用し、VPN とアイデンティティ ファイアウォールのドメインに同じサーバーグループを使用する場合、ユーザは認証に使用されるドメインに関連付けられます。他のすべての承認メカニズムでは、VPNを介して取得されたユーザは、ローカルドメインに存在すると見なされます。ASA は、これらのユーザを AD エージェントに報告します。ADエージェントは、ADエージェントに登録されている他のASAまたはクライアントにそれらのユーザを配布します。

（注） クライアントレス SSL VPN では、ユーザ名は取得されません。

- IPv4カットスループロキシ。IPv6カットスループロキシの場合、ユーザ名は取得されません。認証時にユーザ名にドメイン名が含まれている場合、そのユーザはドメイン名に関連付けられます。それ以外の場合、ドメインは、アイデンティティ オプション ポリシーで設定されているデフォルト メインとなります。カットスルー プロキシの設定 （31 ページ） を参照してください。

ID 認証ファイアウォール ポリシーの要件

ID 認識ファイアウォールポリシーは、すべてのタイプのデバイスおよびオペレーティングシステムでサポートされているわけではありません。次の表では、これらのタイプのポリシーをネットワークに実装するための要件と、いくつかの制限について説明します。

表 *1 : ID* 認証ファイアウォール ポリシーの要件

要件	説明
ファイアウォールデバイス	ASA ソフトウェアバージョン 8.4(2) 以降を実行しているが、8.5(1) を実行している ASA-SM を含まない ASA。単一または複数のコンテキスト構成。 **ヒント** ASA にはオンボード暗号化アクセラレーションが必要です。デバイスに必要な機能があるかどうかを確認するには、デバイスコンソールにログインし、**show version** コマンドを実行します。出力に「暗号化ハードウェアデバイス（Encryption hardware device）」が含まれている必要があります。 1 つの Active Directory エージェントに最大 100 の ASA を登録できます。

要件	説明
Active Directory（AD）	ユーザーとユーザーグループを定義するには、Active Directory を使用する必要があります。ASA は、LDAP プロトコルを実行する AD サーバーから直接ユーザーグループ情報を取得します。他のタイプの LDAP サーバーは使用できません。 サポートされる AD サーバーのタイプと、その設定要件の詳細については、Cisco.com（https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-guides-list.html）の*Active Directory* エージェントのインストールおよびセットアップガイド [英語] を参照してください。 **ヒント** 複数の AD サーバーを設定できますが、それぞれがすべてのドメイン間で一意の IP アドレスを持つ必要があります。他のタイプの LDAP サーバーはサポートされていません。
AD エージェント	ASA と AD サーバー間の仲介として機能するように、オフボックス AD エージェントを設定する必要があります。AD エージェントは、ユーザーと IP アドレスのアクティブなマッピングを保持します。 デフォルトでは、5505 を除き、ASA はブート時またはリロード時にこのリストを取得し、AD エージェントは収集された新しいマッピングを送信します。5505 はアイデンティティ基準を含むトラフィック一致ルールに対応し、必要に応じて AD エージェントを照会します。これはアイデンティティ オプション ポリシーを使用して変更できますが、このデフォルトの動作を使用することをお勧めします。 AD エージェントは RADIUS プロトコルを使用します。 AD エージェントのセットアップおよび設定の詳細については、Cisco.com（http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html）の *Active Directory* エージェントインストール/セットアップガイド [英語] を参照してください。
クライアント システム	デバイスを介してトラフィックを渡すユーザーは、次のクライアントプラットフォームのいずれかを使用する必要があります。 • Windows XP SP3 • Windows Vista • Windows 7 • その他のシステムで、明示的にサポートされるプラットフォームと同じ方法で Active Directory を使用するもの。

要件	説明
IPv6	IPv6 は、次の例外を除いてサポートされています。 • IPv6 上の NetBIOS はサポートされていません。 • ユーザーワークステーションでの複数の IPv6 アドレスはサポートされていません。Windows 64 ビットのシステムでは、通信を開始するときに一時的な IPv6 アドレスを使用する場合があります。ユーザーが 1 つの IPv6 アドレスを使用して AD エージェントに登録し、別のアドレスを使用して通信を開始した場合、ユーザーの ID 認識ファイアウォールルールは適用されず、代わりに 2 番目の IPv6 アドレスに一致するルールが適用されます。 。 これらの一時アドレスの使用を無効にするためのオプションが 2 つあります。 • ネットワーク内のすべてのネットワーキングデバイスのすべてのインターフェイスで、IPv6 ルーティング アドバタイズメントを無効にする。 • 各 Windows マシンでコマンド ウィンドウを開き、次のコマンドを入力してワークステーションをリブートする。 **netsh interface ipv6 set privacy state=disable** **netsh interface ipv6 set global randomizeidentifiers=disabled**

要件	説明
NetBIOS ログアウト プローブ （オプション）	NetBIOS ログアウト プローブをイネーブルにすると、ASA は NetBIOS を使用して、非アクティブ ユーザをデータベースから削除できるように、このユーザをログオフするかどうか判断できます。プローブは、UDP でカプセル化された NetBIOS トラフィックを使用します。したがって、アクセスルールが、ASA、AD エージェント、およびユーザーワークステーション間のネットワーク上で次のトラフィックを確実に許可するようにする必要があります。 • クエリパケット：任意の UDP ソースポートから UDP ポート 137（UDP/137）。 • クエリ応答：UDP/137 ソースから任意の UDP ポート。 さらに、NetBIOS応答パケットにユーザ名が提供されるよう、ワークステーションを設定する必要があります。Windows ワークステーションの場合、メッセンジャーサービスを有効にしてWINSを構成する必要があります。メッセンジャーサービスがオンになっていない場合、ユーザーがログオンしていてもログオンしていなくても、ワークステーションからの応答は同じです。 **ヒント** • NetBIOS ログアウトプローブは、VPN またはカットスルー プロキシ ユーザーでは使用されません。 • ASA には非アクティブ ユーザのタイムアウト設定があります。これは、データベースからユーザを削除するためにも使用されます。このタイマーはすべてのユーザ タイプに適用されます。したがって、データベースから非アクティブ ユーザを削除するために、NetBIOS プローブの実装は不要です。

要件	説明
DNS の設定 （完全修飾ドメイン名の使用に必要）	Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）のネットワーク/ホストオブジェクトをファイアウォールルールに使用する場合は、ドメインネームシステム（DNS）を[DNS]ページの説明のように設定する必要があります。これらの設定により、名前を検索して関連するIPアドレスを判別するために使用される DNS サーバーが識別されます。最終的には、すべての処理がこの IP アドレスに基づいて行われます。 FQDNを使用するようにDNSを設定する場合は、次の点を考慮してください。 • DNS応答はスプーフィングされる可能性があり、ネットワークにセキュリティホールが開く可能性があります。信頼できるDNSサーバーのみを指定します。ネットワーク内のDNSサーバーのみを指定するのが理想的です。 • 一部のホストは、常に変化する複数のIPアドレスを使用する場合があるため、ASA が任意の時点ですべての有効な IP アドレスを持つとは限りません。 • 存続時間の値が短いホスト名では、DNSルックアップを頻繁に行う必要があります。これは、ASAのパフォーマンスに影響を与える可能性があります。 • 複数のホスト名を同じ IP アドレスに解決できます。最終的に、ファイアウォールルールはIPアドレスに基づいて適用されます。つまり、2 つの名前が同じアドレスに割り当てられ、使用中のルールで、これらの名前に別々のサービスが指定されている場合、実際に提供されるサービスは、最初に一致したルールに指定されたものになります。 ルールにすべてのバージョンのFQDNホスト名を指定しなくても済むような、別の方法を検討してください。複数の名前が常に同じホストを指していることがわかっている場合は、最も一般的に使用される名前に対してルールを設定して、その名前のすべての同義語にルールが適用されるようにすることができます。

要件	説明

上限	ユーザー、ユーザーグループ、およびユーザーあたりの IP アドレスの数には制限があります。これらの制限を超えると、追加のトラフィックに対して ID 認識処理が実行されません。
	• IP アドレスの制限：1 人のユーザーを、すべてのドメインで最大 8 つの IP アドレスに関連付けることができます。
	• ユーザーグループの制限：ポリシーは、最大 256 のユーザーグループに適用できます。ユーザーは複数のユーザーグループに属することができます。
	• ユーザの制限：ポリシーは次のユーザ数まで適用できます。この数は、デバイスで定義されているすべてのコンテキストの合計です。
	  • ASA 5505：1024 ユーザー。
	  • その他の ASA 5500 シリーズ：64,000 ユーザー。

ID 認証サービスを提供するためのファイアウォールの設定

ID 認証ファイアウォールサービスをネットワークに提供するには、複数のポリシーを設定して、ファイアウォールでユーザーベースまたは完全修飾ドメイン名（FQDN）ベースのルールを処理できるようにする必要があります。ASA は、ネットワーク内の他のサーバーに依存して、ID 認証ポリシーを実装するために必要なユーザー、ユーザーグループ、および FQDN 名前解決サービスを提供します。

必要な構成は、使用する ID 認証の側面によって異なります。

- ユーザー、ユーザーグループの解決：ファイアウォールルールでアイデンティティ ユーザー グループ オブジェクトを使用するには、いくつかのオブジェクトとポリシーを設定して、ユーザーとユーザーグループの情報を提供する Active Directory サーバーを識別する必要があります。
- FQDN 解決：ファイアウォールルールで FQDN ネットワーク/ホストオブジェクトを使用するには、FQDN を IP アドレスに解決するように DNS サーバーを設定する必要があります。

この手順では、ID 認証ポリシーを実装するプロセス全体について説明します。

はじめる前に

ご使用のネットワークが、ID 認証ファイアウォール ポリシーの要件 （3 ページ）に説明がある要件に適合している必要があります。次の手順では、すでに Active Directory（AD）を使用しており、AD エージェントをインストールして設定し、これらのサービスが正しく動作していることを前提としています。

ステップ 1 AD ユーザーとユーザーグループの解決を有効にします。

a) AD サーバーとエージェントを識別し、サーバーグループの NetBIOS ドメインを設定するために必要なポリシーオブジェクトを作成します。詳細については、Active Directory サーバおよびエージェントの識別 （10 ページ）を参照してください。

b) デフォルト以外の設定が必要な場合はアイデンティティ オプションを変更してください。これらのオプションを使用して NetBIOS ログアウト プローブをイネーブルにし、さまざまなタイマー処理やエラー処理を設定します。詳細については、アイデンティティ オプションの設定 （20 ページ）を参照してください。

c) （AD で定義されたユーザーグループに加えて）ASA で定義されたユーザーグループを作成する場合は、必要なアイデンティティ ユーザー グループ ポリシーオブジェクトを作成します。アイデンティティ ユーザ グループ オブジェクトの作成 （25 ページ）を参照してください。

ステップ 2 FQDN ネットワーク/ホストオブジェクトの解決を有効にします。

a) DefaultDNS グループに DNS サーバを設定します。FQDN を IP アドレスに解決するには、DNS が必要です。DNS の設定手順については、[DNS] ページを参照してください。

b) ネットワーク/ホストオブジェクトの作成の説明に従って、FQDN ネットワーク/ホストオブジェクトを作成します。

ステップ 3 FQDN オブジェクト、ユーザ名、ユーザ グループ名、またはアイデンティティ ユーザ グループ オブジェクトを使用するファイアウォール ルールを設定します。アイデンティティ ベースのファイアウォール ルールの設定 （28 ページ）を参照してください。

ステップ 4 アイデンティティ ファイアウォール システムを監視します。アイデンティティ ファイアウォール ポリシーの監視 （35 ページ） を参照してください。

ID 認証ファイアウォール ポリシーの設定

アイデンティティ認識は複数の既存のファイアウォール ルールに組み込まれます。固有の ID 認証ファイアウォール ポリシーはありません。この項では、アイデンティティ認識をファイアウォール ポリシーに統合するためのさまざまな手順について説明します。

ここでは、次の内容について説明します。

- ID 認証ファイアウォール サービスのイネーブル化 （10 ページ）
- アイデンティティ ユーザ グループ オブジェクトの作成 （25 ページ）
- ポリシーでのアイデンティティ ユーザの選択 （27 ページ）
- アイデンティティ ベースのファイアウォール ルールの設定 （28 ページ）
- カットスルー プロキシの設定 （31 ページ）
- ユーザ統計の収集 （34 ページ）
- アイデンティティ ベースのルールを使用した VPN トラフィックのフィルタリング （35 ページ）

ID 認証ファイアウォール サービスのイネーブル化

アイデンティティ オプション ポリシーを使用して、アイデンティティ認識型ファイアウォールサービスを有効にします。ポリシーを設定するには、次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [アイデンティティオプション（Identity Options）] を選択します。
- （ポリシービュー）ポリシーセレクタから [アイデンティティオプション（ASA）（Identity Options (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ポリシーには次のタブがあります。

- [AD設定（AD Setup）]：ネットワークのユーザおよびユーザグループを定義する Active Directory サーバーと、情報の収集に使用する AD エージェントを設定し、それを ASA に提供します。Active Directory サーバおよびエージェントの識別 （10 ページ）を参照してください。
- [詳細設定（Advanced）]：ユーザアイデンティティ サービスをイネーブルまたはディセーブルにし、エラー処理、NetBIOS ログアウトプローブ、アイドルタイムアウト、および AD エージェント通信設定用の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 （20 ページ） を参照してください。

Active Directory サーバおよびエージェントの識別

[Identity Options] ポリシーの [AD Setup] タブを使用して、ユーザ ID 情報に使用する Active Directory サーバとエージェントを識別します。ユーザ指定（アイデンティティユーザ グループ オブジェクトなど）を含む ID 認証ファイアウォール ポリシーをイネーブルにするには、1 つ以上の AD サーバと AD エージェントを設定する必要があります。

（注） ID 認証ファイアウォールには ASA ソフトウェア 8.4(2+) が必要です。

はじめる前に

設定では AAA サーバ グループ ポリシー オブジェクトを使用します。このオブジェクトには AAA サーバ オブジェクトが組み込まれます。これらのオブジェクトは Policy Object Manager（[Manage] > [Policy Objects]）から作成するか、この手順の実行（設定ウィザードを使用するか、オブジェクト セレクタ ダイアログボックスで [Add Object]（+）ボタンをクリックする）によって作成します。

オブジェクトは、次の要件を満たす必要があります。

- AD サーバ：LDAP プロトコルを使用する必要があります。LDAP サーバ タイプとして Microsoft を選択していると、ユーザ グループの検索のベース ディレクトリを識別し、検索時間を短縮する LDAP グループ ベース DN を指定することもできます。[Auto Detect] を選択した場合、Microsoft AD サーバがアイデンティティ ファイアウォールの設定で使用で

きる LDAP サーバの唯一のタイプであっても、グループ ベース DN は設定できません。Security Manager と Active Directory の通信については、次の制限に従う必要もあります。

- [Enable LDAP over SSL] オプションを選択しない。
- [SASL Kerberos Authentication] オプションを選択しない。シンプルおよび SASL MD5 認証メカニズムのみがサポートされます。ユーザ名とパスワードが平文で送信されるシンプルなメカニズムは、SASL オプションのいずれかを選択していない場合に使用されます。

- AD エージェント：RADIUS プロトコルを使用する必要があります。AAA サーバー グループ オブジェクトで、[AD エージェントモード（AD Agent Mode）] オプションを選択します。

このポリシーを設定する前に、AD エージェントをインストールおよび設定しておく必要があります。サーバ グループには AD エージェントを最大 2 つ設定できます。2 番目のエージェントは、最初のエージェントがクエリーへの応答を停止した場合にのみ使用されます。この 2 つのエージェント以降に定義されたエージェントはすべて無視されます。

http://www.cisco.com/go/asa から AD エージェントソフトウェアを入手します。AD エージェントのセットアップおよび設定の詳細については、Cisco.com の『*Installation and Setup Guide for the Active Directory Agent*』を参照してください。

関連項目

- ID 認証ファイアウォール ポリシーの要件 （3 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて
- AAA サーバ オブジェクトの作成
- [AAA Server] ダイアログボックス - LDAP 設定
- AAA サーバ グループ オブジェクトの作成
- アイデンティティ オプションの設定 （20 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [アイデンティティオプション（Identity Options）] を選択します。[AD Setup] タブを選択します。
- （ポリシー ビュー）ポリシーセレクタから [アイデンティティオプション（ASA）（Identity Options (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。[AD Setup] タブを選択します。

ステップ 2 AD Setup のガイドを利用する場合は、[アイデンティティの設定（Configure Identity）] ボタンをクリックして Identity Configuration ウィザードを開始してください。このウィザードによって、ドメイン用の AD サーバと、AD エージェントを設定するプロセスが実行され、必要な AAA サーバおよび AAA サーバ グループ オブジェクトを作成できます。

ウィザードでは次の手順を実行します。

- AD サーバ設定：ドメイン用の AD サーバを設定します。 Identity Configuration ウィザードの Active Directory Settings （14 ページ）を参照してください。
- AD エージェント設定：ASA 用の AD エージェントを設定します。 Identity Configuration ウィザードの Active Directory エージェント （17 ページ）を参照してください。
- プレビュー：作成されるオブジェクトを表示します。 Identity Configuration ウィザードの Preview （19 ページ）を参照してください。

ヒント このウィザードを複数回使用すると、さまざまな NetBIOS ドメインを設定できます。ただし、このウィザードでは常に AD エージェント情報の入力を求められます。AD エージェントにはドメイン単位に別個のグループを設定するのではなく、単一グループを設定するため、すでに行った AD エージェントの設定が選択によって上書きされます。そのため、ウィザードを実行するたびに、必ず AD エージェントに同じ AAA サーバーグループを選択してください。

ステップ 3 ウィザードを使用しない場合は、AD サーバを設定します。AD サーバは、ID 認証ファイアウォール ポリシーで使用する AD ユーザ グループについてのユーザ メンバーシップ情報を取得するために使用されます。

テーブルにはネットワーク用の AD サーバがリストされます。個々の NetBIOS ドメイン名にエントリを追加する必要があります。各行には AAA サーバ グループが定義され、ドメインに対応する AD LDAP サーバの識別と、AD サーバ グループが使用できない場合に、ドメインの ID 認証ファイアウォール ルールをアクティブにするかどうかの判断に使用されます。

次を実行できます。

- エントリを追加するには、[行の追加（Add Row）]（+）ボタンをクリックし、[AD ドメインサーバーの追加（Add AD Domain Server）] ダイアログボックスに入力します。 [Domain AD Server] ダイアログボックス （13 ページ）を参照してください。
- エントリを編集するには、エントリを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- エントリを削除するには、エントリを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

ステップ 4 ウィザードを使用しない場合は、AD エージェントを設定します。AD エージェントはユーザのログオン/ログアウトと IP アドレス マッピングを AD サーバから入手します。次に、ASA は AD エージェントから情報を取得します。

[Active Directoryエージェントグループ（Active Directory Agent Group）] で、AD エージェントのリストを定義する AAA サーバー グループ オブジェクトの名前を入力します。あるいは [選択（Select）] をクリックしてオブジェクトを選択するか、グループオブジェクトを新しく作成します。

ステップ 5 [デフォルトドメイン（Default Domain）] で、デバイスのデフォルトドメインとして設定するドメインを選択します。ドメインをデフォルト ドメインとして選択する前に、そのドメインを AD サーバに追加する必要があります。

デフォルトは LOCAL です。これは、デバイスに定義されたユーザ グループまたはアイデンティティ サービス用に設定された AD サーバ以外の方法を使用して認証を行う VPN ユーザに適用されます。この設定はカットスルー プロキシを設定する場合にも使用されます（カットスルー プロキシの設定 （31 ページ）を参照）。

ステップ 6 [保存（Save）] をクリックして変更を保存します。

管理設定の [Identity Settings] ページを、ドメインから AD サーバへのマッピングを使用して更新するかどうかの問い合わせがあります。ID設定によって、ファイアウォール ポリシーまたはアイデンティティ ユーザ グループ オブジェクトでユーザまたはユーザ オブジェクトを指定する際に、どのサーバを使用して [Find] 機能を使用するかが決まります。ID 管理設定は、ASA の設定には影響を与えません。

[Domain AD Server] ダイアログボックス

NetBIOS ドメインに Active Directory サーバを定義するには、[Add Domain AD Server] または [Edit Domain AD Server] ダイアログボックスを使用します。NetBIOS ドメインにユーザ グループのファイアウォール ルールを設定すると、ユーザ メンバーシップはドメインに定義した AD サーバを照会することによって決まります。

ナビゲーション パス

次のいずれかを実行します。

- [Identity Options] ページの [AD Setup] タブで、ドメイン テーブルの [Add] または [Edit] ボタンをクリックします。 Active Directory サーバおよびエージェントの識別 （10 ページ）を参照してください。
- ID 設定の Security Manager 管理ページで、設定テーブルの [Add] または [Edit] ボタンをクリックします。これらの設定は、ファイアウォール ルールまたはアイデンティティ ユーザ グループ オブジェクトの設定で、[Find] を使用してユーザ名またはユーザ グループ名を検索する際に、どのサーバを使用するかを決定します。[Identity Settings] ページを参照してください。

フィールド リファレンス

表 2 : [Domain AD Server] ダイアログボックス

要素	説明
ドメイン	この AD サーバ グループの NetBIOS ドメイン。ドメイン名は最大 32 文字まで指定できます。通常はすべて大文字です。たとえば、ユーザ指定が DOMAIN\user1 の場合、DOMAIN は NetBIOS ドメイン名になります。

要素	説明
AD Server Group	AAA サーバ グループ ポリシー オブジェクトの名前。この名前によって、このドメインの AD サーバが指定されます。オブジェクトで LDAP プロトコルを使用する必要があります。 [選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。
Disable Rules When Server Is Down （アイデンティティ オプション ポリシーのみ）	ドメイン コントローラが停止している場合、このドメインのすべての ID 認証ファイアウォール ルールをディセーブルにするかどうかを指定します。このオプションを選択した場合、ドメインのすべてのユーザは、サーバが使用可能になるまでディセーブルとマークされます。
Update Administrative Settings （アイデンティティ オプション ポリシーのみ）	ドメインとサーバのマッピングを [Security Manager Administration] の [Identity Settings] ページに追加するかどうかを指定します。この管理ページによって、ファイアウォール ポリシーまたはアイデンティティ ユーザ グループ オブジェクトに、ユーザまたはユーザ グループを追加する場合、これらの検索時にどの AD サーバを照会するかが決定されます。詳細については、[Identity Settings] ページを参照してください。

Identity Configuration ウィザードの Active Directory Settings

NetBIOS ドメインの Active Directory（AD）サーバを識別するには、Identity Configuration ウィザードの [Active Directory Settings] ページを使用します。これらの設定は、ユーザ ID 対応のファイアウォール ポリシーをドメイン内のユーザでイネーブルにするために必要です。

ナビゲーション パス

次のいずれかを実行します。

- [アイデンティティオプション（Identity Options）] ページの [ADセットアップ（AD Setup）] タブで [アイデンティティの設定（Configure Identity）] ボタンをクリックします。 Active Directory サーバおよびエージェントの識別 （10 ページ）を参照してください。
- アイデンティティ オプションのポリシーがまだ設定されていない場合は、[User] フィールドの [Select] ボタンをクリックし、アイデンティティを設定するかどうかの質問には [Yes] をクリックすると、AAA ルール ポリシー、アクセス ルール ポリシー、またはインスペクション ルール ポリシーからこのウィザードを開始できます。

フィールド リファレンス

表 3 : Identity Configuration ウィザードの Active Directory Settings

要素	説明
NetBIOS ドメイン（NetBIOS Domain）	この AD サーバ グループの NetBIOS ドメイン。ドメイン名は最大 32 文字まで指定できます。通常はすべて大文字です。たとえば、ユーザ指定が DOMAIN\user1 の場合、DOMAIN は NetBIOS ドメイン名になります。
Select Existing AD Server Group	必要な AD サーバを識別する AAA サーバ グループ ポリシー オブジェクトがすでに存在している場合はこのオプションを選択します。オブジェクトで LDAP プロトコルを使用する必要があります。 [グループ名（Group Name）] フィールドの横にある [選択（Select）] をクリックし、オブジェクトを選択します。
Create New AD Server Group	AAA サーバ グループ ポリシー オブジェクトがまだ存在していないか、ウィザードでオブジェクトを新たに作成する場合にこのオプションを選択します。 オブジェクトに含まれるグループおよびサーバを識別するように、残りのオプションを設定します。
[Create AD Server Group] プロパティ	
グループ名（Group Name） （ウィザードでグループを作成する場合）	作成する AAA サーバ グループ オブジェクトの名前。名前には最大 16 文字を使用できます。
AD Server Name/IP	次のいずれかです。 • AD サーバを定義する既存の AAA サーバ オブジェクトの名前。[選択（Select）] をクリックして、リストからオブジェクトを選択します。 オブジェクトを選択すると、残りのプロパティを設定できなくなります。 • AD サーバの IP アドレス。

要素	説明
ユーザー名	認証済みバインディングに使用されるLDAP階層内のユーザまたはディレクトリ オブジェクトの名前（最大 128 文字）。認証済みバインディングは、一部の LDAP サーバ（Microsoft Active Directory サーバなど）によって、他の LDAP 操作の実行前に要求されます。このフィールドには、デバイスの認証特性が記述されます。これらの特性は、管理者特権を持つユーザーの特性に対応している必要があります。 この文字列では、大文字と小文字が区別されます。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。 通常は、DOMAIN\Administrator などのユーザ名です。従来型のフォーマット（cn=Administrator、OU=Employees、DN=example、DN=com など）を使用してもかまいません。
パスワード 確認（Confirm）	LDAPサーバにアクセスするための、大文字と小文字が区別される英数字のパスワード（最大 64 文字）。スペースは使用できません。
インターフェイス	すべての発信パケットに対して、そのIPアドレスが使用されるインターフェイス（送信元インターフェイスと呼ばれます）。インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。 **ヒント** • インターフェイスの名前を入力する場合、この AAA オブジェクトを使用するポリシーが、この名前のインターフェイスを含むデバイスに割り当てられるようにします。 • インターフェイス ロールの名前を入力する場合、ロールが複数のインターフェイスではなく、1つのインターフェイスを表すようにします。 • AAA サーバ グループ内の AAA サーバに対して定義できる送信元インターフェイスは 1 つだけです。複数のサーバを指定する場合は、すべて同じインターフェイスにする必要があります。
Add Another AD Server	サーバを別に作成する場合にのみ、このボタンをクリックしてください。 このボタンをクリックすると、サーバ フィールドの情報が保存されてフィールドがクリアされ、次のサーバの情報を追加できるようになります。サーバは、シングルコンテキスト モードでは16台まで、マルチコンテキスト モードでは 4 台まで追加できます。

Identity Configuration ウィザードの Active Directory エージェント

NetBIOS ドメインの Active Directory（AD）エージェントを識別するには、Identity Configuration ウィザードの [Active Directory Agent Settings] ページを使用します。これらの設定は、ユーザ ID 対応のファイアウォール ポリシーをドメイン内のユーザでイネーブルにするために必要です。

ヒント ASA に単一の AD エージェント グループを設定できます。NetBIOS ドメインごとにに別のグループを設定しないでください。したがって、アイデンティティ オプションのポリシーに正しい AD エージェント グループをすでに設定している場合は、このウィザードページで同じグループを選択してください。ポリシーで定義されているグループがこのページで選択した内容に置き換えられます。

ナビゲーション パス

次のいずれかを実行します。

- [アイデンティティオプション（Identity Options）]ページの [ADセットアップ（AD Setup）] タブで [アイデンティティの設定（Configure Identity）] ボタンをクリックし、次のページに進みます。[Identity Settings] ページを参照してください。
- アイデンティティ オプションのポリシーがまだ設定されていない場合は、[User] フィールドの [Select] ボタンをクリックし、アイデンティティを設定するかどうかの質問には [Yes] をクリックすると、AAA ルール ポリシー、アクセス ルール ポリシー、またはインスペクション ルール ポリシーからこのウィザードを開始できます。

フィールド リファレンス

表 4 : Identity Configuration ウィザードの Active Directory Agent Settings

要素	説明
Select Existing AD Agent Group	必要な AD エージェントを識別する AAA サーバ グループ ポリシー オブジェクトがすでに存在している場合はこのオプションを選択します。このオブジェクトは RADIUS プロトコルを使用し、[ADエージェントモード（AD Agent Mode）] オプションを選択している必要があります。 [グループ名（Group Name）] フィールドの横にある [選択（Select）] をクリックし、オブジェクトを選択します。
Create New AD Agent Group	AAA サーバ グループ ポリシー オブジェクトがまだ存在していないか、ウィザードでオブジェクトを新たに作成する場合にこのオプションを選択します。 オブジェクトに含まれるグループおよびサーバを識別するように、残りのオプションを設定します。

要素	説明
[Create AD Agent Group] プロパティ	
グループ名（Group Name） （ウィザードでグループを作成する場合）	作成する AAA サーバ グループ オブジェクトの名前。名前には最大 16 文字を使用できます。
AD Agent Name/IP	次のいずれかです。 • AD エージェントを定義する既存の AAA サーバ オブジェクトの名前。[選択（Select）] をクリックして、リストからオブジェクトを選択します。 オブジェクトを選択すると、残りのプロパティを設定できなくなります。 • AD エージェントの IP アドレス。
秘密キー（Secret Key） 確認（Confirm）	ネットワーク デバイス（クライアント）と AAA サーバ間でデータを暗号化するために使用される共有秘密キー。キーでは、127 文字以下の英数字で、大文字と小文字を区別します。特殊文字も使用可能です。 このフィールドで定義したキーは、RADIUS サーバのキーと一致している必要があります。確認フィールドでもう一度キーを入力します。 キーを定義しない場合、AAA サーバとその AAA クライアント間のすべてのトラフィックは暗号化されずに送信されます。
インターフェイス	すべての発信パケットに対して、そのIPアドレスが使用されるインターフェイス（送信元インターフェイスと呼ばれます）。インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは[選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。 **ヒント** • インターフェイスの名前を入力する場合、この AAA オブジェクトを使用するポリシーが、この名前のインターフェイスを含むデバイスに割り当てられるようにします。 • インターフェイス ロールの名前を入力する場合、ロールが複数のインターフェイスではなく、1 つのインターフェイスを表すようにします。 • AAA サーバ グループ内の AAA サーバに対して定義できる送信元インターフェイスは 1 つだけです。複数のサーバを指定する場合は、すべて同じインターフェイスにする必要があります。

要素	説明
Add Secondary AD Agent	エージェントを別に作成する場合にのみ、このボタンをクリックしてください。このエージェントは、最初のエージェントが使用できなくなった場合に使用されます。 このボタンをクリックすると、エージェント フィールドの情報が保存されてプレビュー ページに追加され、フィールドがクリアされて 2 番目のエージェントの情報を追加できるようになります。

Identity Configuration ウィザードの Preview

Identity Configuration ウィザードに入力した情報を確認するには、このウィザードの [Preview] ページを使用します。

プレビューには NetBIOS ドメインの Active Directory 設定に作成または使用されるオブジェクトの情報がまとめられています。

- AD サーバ グループには、このドメインで使用される AD サーバの AAA サーバ グループ オブジェクト名が示されます。テーブルには各 AD サーバを定義する AAA サーバ オブジェクトが示されます。
- AD エージェントには、AD エージェントの AAA サーバ グループ オブジェクト名が示されます。プライマリ エージェントとセカンダリ エージェントには、エージェントを定義する AAA サーバ オブジェクトが示されます。

ウィザードで作成されるオブジェクトの場合、名前は AAA サーバーオブジェクト用に自動的に生成され、**ldap_** または **radius_** がプレフィックスとしてサーバーの IP アドレスに追加されます。

変更する場合、[戻る（Back）] をクリックします。変更しない場合は、[終了（Finish）] をクリックして設定を保存します。

ヒント　ウィザードを完了すると、新たに作成されたオブジェクトのプロパティを編集して、ウィザードがデフォルト設定として残した設定値を設定できます。

ナビゲーション パス

次のいずれかを実行します。

- [アイデンティティオプション（Identity Options）] ページの [ADセットアップ（AD Setup）] タブで [アイデンティティの設定（Configure Identity）] ボタンをクリックし、次のページに進みます。 Active Directory サーバおよびエージェントの識別 （10 ページ）を参照してください。
- アイデンティティ オプションのポリシーがまだ設定されていない場合は、[User] フィールドの [Select] ボタンをクリックし、アイデンティティを設定するかどうかの質問には [Yes]

をクリックすると、AAA ルール ポリシー、アクセス ルール ポリシー、またはインスペクション ルール ポリシーからこのウィザードを開始できます。

アイデンティティ オプションの設定

アイデンティティ オプション ポリシーの [Advanced] タブを使用して、ユーザ ID サービスをイネーブルまたはディセーブルにし、エラー処理、NetBIOS ログアウト プローブ、アイドル タイムアウト、および AD エージェント通信設定用のオプションを設定します。このタブに含まれるオプションにはデフォルト値があるため、実際のネットワーク用に設定を微調整する必要がある場合にのみ、値を変更します。

ナビゲーション パス

- （デバイス ビュー）ASA デバイスを選択し、ポリシー セレクタから [アイデンティティ オプション（Identity Options）] を選択します。[Advanced] タブを選択します。
- （ポリシー ビュー）ポリシー セレクタから [アイデンティティ オプション（ASA）（Identity Options (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。[Advanced] タブを選択します。

関連項目

- Active Directory サーバおよびエージェントの識別 （10 ページ）
- ID 認証ファイアウォール ポリシーの要件 （3 ページ）

フィールド リファレンス

表 5 : アイデンティティ オプションの *[Advanced]* タブ

要素	説明
Enable User Identity	[AD設定（AD Setup）] タブに AD エージェントと AD サーバーが設定されている場合、これらからユーザ ID 情報を入手するためにデバイスをイネーブルにするかどうかを指定します。デフォルトではイネーブルになっています。 このオプションを変更して展開すると、この変更には新しい設定に基づいた次の効果があります。 • ディセーブル：ユーザ マッピング データベースに対する IP アドレス全体が消去され、有効なユーザ固有のルールがないすべてのユーザが解放されます。ADエージェントおよびサーバは更新に対するクエリーを受信しなくなり、有効なユーザ ID ベースのすべてのルールは、トラフィックに影響を与えなくなります。 • イネーブル：有効なユーザがADエージェントとの通信を介して段階的に再作成されます。VPNユーザの再認証が必要な場合があります。AD エージェントと AD サーバへのクエリーが再開されます。
エラー状態	
Disable Rules When Active Directory Agent Is Down	AD エージェントへの接続が使用できない場合に、ユーザ ID を含むすべてのルールをディセーブルにするかどうかを指定します。このオプションを選択すると、ユーザから IP アドレスへのマッピングはすべてディセーブルとマークされ、ユーザの詳細情報を含むルールがすべてトラフィックに適用されなくなります。デフォルトでは、このオプションはディセーブルです。
Remove User IP When NetBIOS Probe Fails	ユーザの NetBIOS プローブが何らかの理由で失敗した（プローブがネットワーク内でブロックされているか、ユーザが活動していないためにプローブに失敗した）場合に、ユーザの IP アドレスマッピングをデータベースから削除するかどうかを指定します。ユーザはワークステーションにログインし直す必要があります。NetBIOS ログアウト プローブをこのページでイネーブルにした場合にのみ、このオプションに効果があります。デフォルトでは、このオプションはディセーブルです。

要素	説明
[ユーザのMACアドレスが不整合の場合にユーザIPを削除する（Remove User IP When User's MAC Address is Inconsistent）]	ユーザがマッピングされたIPアドレスからの要求ごとに、そのMedia Access Control（MAC; メディア アクセス コントロール）アドレスと前のパケットの MAC アドレスとを確認するかどうかを指定します。 このオプションを選択し、MAC アドレスがパケット間で変化した場合、ユーザと IP アドレスのマッピングはデータベースから削除され、後続のパケットはドロップされます。ユーザは Active Directory への再認証が必要です。MACの不一致によってユーザとIPのマッピングが削除された場合は、ADエージェントに通知されます。デフォルトでは、このオプションは有効になっています。 MAC の確認は、ASA に直接接続されたネットワーク上の IP アドレスからのパケットだけに対して行われます。VPN ユーザは確認されません。
Track User Not Found	「ユーザが見つからない」トラッキングをイネーブルにするかどうかを指定します。デフォルトでは、このオプションはディセーブルです。
NetBIOS ログアウト プローブ	
Enable (NetBIOS Logout Probe)	NetBIOS ログアウト プローブをイネーブルにするかどうかを指定します。 このプローブを使用すると、ユーザがネットワークからログアウトしたかどうかを事前に判断できます。これにより、アイドル タイムアウトがこの目的で使用される唯一のメカニズムである場合よりも、デバイスによるユーザから IP アドレスへのマッピングの削除が迅速にできるようになります。デフォルトでは、プローブはディセーブルになっていて、ユーザは Idle Timeout の値よりも長い期間アイドルになっている場合にのみ削除されます。 ユーザが検査されるのは、ユーザの状態がアクティブで、1つ以上の有効なルールで使用されている場合に限ります。VPN ユーザとカットスルー プロキシ ユーザは検査されません。NetBIOS ログアウト プローブによってユーザと IP のマッピングが削除された場合は、AD エージェントに通知されます。 以下のオプションの設定の詳細については、ID認証ファイアウォール ポリシーの要件 （3 ページ）を参照してください。
Probe Timer	ユーザがアイドルであるかどうかにかかわらず、有効なユーザに NetBIOS プローブを送信する頻度。デフォルトは 15 分で、指定できる範囲は 1 ～ 65535 分です。

要素	説明
再試行間隔（Retry Interval）	IP アドレスからの応答がない場合にプローブを再試行する頻度と、プローブを再試行する回数。デフォルトは 3 秒と再試行回数 3 回です。範囲は 1 ～ 65535 秒と、再試行回数 1 ～ 256 回です。 最後の再試行から応答がない場合に [NetBIOSプローブが失敗した場合にユーザIPを削除する（Remove User IP When NetBIOS Probe Fails）] オプションを選択すると、ユーザから IP アドレスへのマッピングが削除されます。このオプションを選択しないと、アドレスは次のインターバルで確認されます。
ユーザー名	NetBIOS 応答があった場合に、戻されたユーザ名に基づいて応答を処理する方法を指定します。 • [いずれかが一致（Match Any）]（デフォルト）：応答内の任意のユーザ名が、IP アドレスのデータベース内のユーザ名と一致します。応答に複数の名前があり（複数のユーザがワークステーションにログインしている）、応答内のユーザがデータベース内のユーザと一致する場合、プローブは成功したと見なされ、そのマッピングが保持されます。 • [ユーザ不要（User Not Needed）]：NetBIOS 応答内のユーザ名は無視されます。クエリの応答だけで、ユーザから IP アドレスへのマッピングを保持することができます。このオプションは、Messenger サービスがワークステーションでオンになっていない場合に有効です。この場合、NetBIOS の応答にはユーザ名は含まれません。このオプションは、複数のユーザーがワークステーションにログインする場合にも役立ちます。 • [完全一致（Exact Match）]：NetBIOS 応答内には 1 つのユーザ名のみが含まれ、ユーザから IP アドレスへのマッピングデータベース内のユーザ名と完全に一致する必要があります。ユーザが複数含まれていたり、ユーザ名が一致しなかったりすると、マッピングはデータベースから削除され、IP アドレスは非アクティブとしてマークされます。
Users	
アイドル タイムアウト	データベース内のユーザから IP アドレスへのマッピングを削除する前に、ユーザがアイドル状態でいられる期間を分単位で指定します。マッピングが削除されると、ユーザはマッピングを更新するためにログインし直す必要があります（Ctrl+Alt+Delete を使用してワークステーションをロックし、もう一度ログインするなど）。デフォルトは 60 分で、指定できる範囲は 1 ～ 65535 分です。 このオプションの選択を解除すると、アイドル タイムアウトの確認をディセーブルにすることができます。この場合、ユーザから IP へのマッピングはアイドル状態のため削除されません。 VPN ユーザとカットスルー プロキシ ユーザはこのタイマーの対象となりません。アイドル タイムアウトによってユーザと IP アドレスのマッピングが削除された場合は、AD エージェントに通知されません。

要素	説明
Active Directory Agent	
Hello タイマー（Hello Timer）	Hello パケットを AD エージェントに送信する頻度。ASA は hello パケットを使用して、ASA レプリケーション ステータスとドメイン ステータスを入手します。ASA が最後の再試行後に応答を受け取らなかった場合、AD エージェントはダウンしていると見なされ、ASA はバックアップの AD エージェントに切り替えられます（エージェントを設定している場合）。 デフォルトでは、hello パケットは 30 秒おきに送信され、応答がない場合は最大 5 回まで再試行が行われます。範囲は 10 ～ 65535 秒と、再試行回数 1 ～ 65535 回です。
Poll Groups Timer	ファイアウォール ルールに指定したユーザ メンバーシップのリストを入手するために Active Directory サーバがクエリーを送信する間隔を指定します。ASA は、グループを使用している場合に限り、グループ内のメンバーシップについてサーバに対してクエリーを実行します。AD サーバに定義されたすべてのグループに対するクエリーは実行しません。デフォルトは 8 時間で、指定できる範囲は 1 ～ 65535 時間です。 **ヒント** グループ メンバーシップが変更された場合、その変更は、このタイマーの期限が切れて、ASA が更新情報を AD サーバにポーリングするまでルール処理に反映されません。したがって、ASA でグループ メンバーシップを更新する必要性と、ポーリングの量を削減しようとする要求とのバランスをとりながら、ネットワーク内のグループ メンバーシップに対する変更頻度に基づいてタイマーを設定する必要があります。

要素	説明
Retrieve User Information	ASA がユーザと IP アドレスのマッピングを AD エージェントから取得する方法を指定します。 • [フルダウンロード（Full Download）]（ASA 5505 以外のデバイスのデフォルト）：ブート時に、ASA はユーザから IP アドレスへの完全マッピングデータベースを AD エージェントから取得し、ユーザがネットワークにログインおよびログアウトしたときに差分更新を入手します。 このオプションは、ネットワークにあるユーザが 1024 よりも少ない場合にのみ、5505 で使用されます。5505 ではユーザから IP へのマッピングの数が 1024 以内に制限されているためです。5505 では、デフォルトのオンデマンド設定は、ごく少数のユーザがデバイス経由でトラフィックを通過させる場合にのみ適用されます。 • [オンデマンド（On Demand）]（ASA 5505 デバイスのデフォルト）：ASA は、新しいパケットが接続を必要とし、マッピングが存在しない場合にのみ、ユーザから IP へのマッピングについて、AD エージェントに対してクエリを実行します。このオプションではメモリがあまり使用されませんが、マッピングの取得で遅延が生じる可能性があります。パケットは、当初従来型の送信元 IP アドレスと宛先 IP アドレス、およびサービス情報を基に評価され、誤ったアクションが生じる可能性があります。企業の環境か悪意のある攻撃により、大量のユーザが同時にログインした場合、遅延が増大する可能性があります。

アイデンティティ ユーザ グループ オブジェクトの作成

アイデンティティ ユーザ グループ オブジェクトを作成すると、個々のユーザ、ユーザ グループ、またはユーザとグループの組み合わせを識別できます。これらのユーザとグループは、Active Directory（AD）に定義されている必要があります。他のタイプのユーザは定義できません。

ヒント アイデンティティ ユーザ グループは ASA で定義されます。AD に定義済みのグループを複製するために、これらのグループを作成する必要はありません。AD グループはファイアウォール ルール内に直接指定できます。アイデンティティ ユーザ グループ オブジェクトは、それ以外では AD に存在しないユーザとユーザ グループの集合を定義するためのみに必要です。

事前に定義されているアイデンティティ ユーザ グループは 2 種類あります。これらのグループは、カットスルー プロキシの設定 （31 ページ）で説明されているカットスルー プロキシの設定で使用されます。

- all-auth-users：認証済みユーザと関連付けられているすべての IP アドレスと一致します。

- all-unauth-users：認証済みユーザーと関連付けられていない IP アドレスのみを照合します。

ヒント

- これらのオブジェクトの使用は、ASA 8.4(2+) のみでサポートされます。
- これらのオブジェクトを使用できるようにするには、ASA にアイデンティティ オプションのポリシーを設定する必要があります。
- このオブジェクトタイプを使用するポリシーまたはオブジェクトを定義するときに、アイデンティティ ユーザ グループを作成できます。詳細については、ポリシーでのアイデンティティ ユーザの選択 （27 ページ）を参照してください。

関連項目

- アイデンティティ ベースのファイアウォール ルールの設定 （28 ページ）
- ID 認証ファイアウォール ポリシーの要件 （3 ページ）
- [Identity Settings] ページ
- ポリシー オブジェクトの作成

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Managerを参照）。

ステップ 2 オブジェクトタイプセレクタから [アイデンティティユーザーグループ（Identity User Group）] を選択します。

ステップ 3 作業領域を右クリックして [新規オブジェクト（New Object）] を選択し、[アイデンティティユーザーグループの追加（Identity User Group）] ダイアログボックスを開きます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 [グループ内のメンバー（Members in Group）] リストにアイテムを追加したり、このリストからアイテムを削除したりして、オブジェクトに定義されているユーザーとユーザーグループを識別します。

リストに入力するには、次のいずれかの組み合わせを実行します。

- [利用可能なアイデンティティユーザーグループ（Available Identity User Group）] で、既存のオブジェクトを選択し、リスト間の [追加>>（Add >>）] ボタンをクリックします。
- [ユーザー/ユーザーグループの検索（Search User/User Group）] で、ID 設定の管理オプションでドメインに対して設定されている Active Directory サーバーからユーザーまたはユーザーグループを選択します。ユーザまたはユーザ グループを選択する前に設定を行っておく必要があります。この設定でSecurity Manager が使用する AD サーバを認識します。

ユーザまたはユーザ グループを検索するには、NetBIOS ドメインを選択し、ユーザまたはユーザ グループを検索しているかどうかを指定して、検索文字列を入力します。次に、[検索（Search）] をクリックして一致する文字列を検索します。検索文字列が名前内の任意の場所（名前、ミドルネームのイニシャル、姓）、

ユーザ ID、CN、（ユーザ グループの場合）ユーザ グループ名に含まれている場合、名前は一致していると見なされます。

ユーザーまたはグループを追加するには、リストで選択し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。

- [カンマで区切られたアイデンティティユーザーまたはユーザーグループの入力（Type in comma separated identity user or user group）] に有効な名前を入力し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。複数の名前はカンマで区切ります。これらは、メンバー リストに別々の行として追加されます。

次の形式を使用して、名前を入力できます。

- 個別のユーザ：NETBIOS_DOMAIN\user
- ユーザ グループ（\ を二重にします）：NETBIOS_DOMAIN\\user_group

ドメイン名が含まれていない場合、Security Manager Administration の [Identity Settings] ページで選択したオプションに基づいてドメイン名が付加されます。名前の前に \ または \\ を付けると、[Identity Settings] ページで定義されたデフォルト ドメインが自動的に追加されます。

- オブジェクトから項目を削除するには、[メンバー（Members）] リストで項目を選択し、リスト間にある [<<削除（<< Remove）] ボタンをクリックします。

ステップ 6 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用を参照してください。

ステップ 7 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可を参照してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

ポリシーでのアイデンティティ ユーザの選択

アイデンティティ ユーザの指定を許可するポリシーまたはポリシー オブジェクトで、[User] フィールドの横にある [Select] ボタンをクリックして、アイデンティティ ユーザ グループ オブジェクトを選択して情報入力するか、直接情報を入力できます。

[アイデンティティユーザーグループセレクタ（Identity User Group Selector）] ダイアログボックスで [グループ内のメンバー（Members in Group）] リストに入力することにより、[ユーザー（User）] フィールドの内容を定義できます。リストに入力するには、次のいずれかの組み合わせを実行します。

- [利用可能なアイデンティティユーザーグループ（Available Identity User Group）] で、既存のオブジェクトを選択し、リスト間の [追加>>（Add >>）] ボタンをクリックします。目的のオブジェクトが存在しない場合は、リストの下にある [追加（Add）]（+）ボタンをクリックして新しいオブジェクトを作成できます。オブジェクトを選択し [編集（Edit）]（鉛筆）ボタンをクリックして、オブジェクトを変更するか、内容を確認できます。

事前に定義されているアイデンティティ ユーザ グループは 2 種類あります。これらのグループは、カットスルー プロキシの設定 （31 ページ）で説明されているカットスルー プロキシの設定で使用されます。

- all-auth-users：認証済みユーザと関連付けられているすべての IP アドレスと一致します。
- all-unauth-users：認証済みユーザーと関連付けられていない IP アドレスのみを照合します。
- [ユーザー/ユーザーグループの検索（Search User/User Group）] で、ID 設定の管理オプションでドメインに対して設定されている Active Directory サーバーからユーザーまたはユーザーグループを選択します。ユーザまたはユーザ グループを選択する前に設定を行っておく必要があります。この設定で Security Manager が使用する AD サーバを認識します。

ユーザまたはユーザ グループを検索するには、NetBIOS ドメインを選択し、ユーザまたはユーザ グループを検索しているかどうかを指定して、検索文字列を入力します。次に、[検索（Search）] をクリックして一致する文字列を検索します。検索文字列が名前内の任意の場所（名前、ミドルネームのイニシャル、姓）、ユーザ ID、CN、（ユーザ グループの場合）ユーザ グループ名に含まれている場合、名前は一致していると見なされます。

ユーザーまたはグループを追加するには、リストで選択し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。

- [カンマで区切られたアイデンティティユーザーまたはユーザーグループの入力（Type in comma separated identity user or user group）] に有効な名前を入力し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。複数の名前はカンマで区切ります。これらは、メンバー リストに別々の行として追加されます。

次の形式を使用して、名前を入力できます。

- 個別のユーザ：NETBIOS_DOMAIN\user
- ユーザ グループ（\ を二重にします）：NETBIOS_DOMAIN\\user_group

ドメイン名が含まれていない場合、[Identity Settings] ページで説明しているように、[Security Manager Administration] の [Identity Settings] ページで選択したオプションに基づいてドメイン名が付加されます。名前の前に \ または \\ を付けると、[Identity Settings] ページで定義されたデフォルト ドメインが自動的に追加されます。

- オブジェクトから項目を削除するには、[メンバー（Members）] リストで項目を選択し、リスト間にある [<<削除（<< Remove）] ボタンをクリックします。

アイデンティティ ベースのファイアウォール ルールの設定

アイデンティティ認識は、ファイアウォール サービスを提供するために使用される ACL 内のアクセス コントロール エントリまたはルールと統合されます。この機能は ACL と統合されるため、アイデンティティ ベースのルールをファイアウォール ポリシーに追加する方法は、すべてのタイプのファイアウォール ポリシーで同じになります。この項では、アイデンティティ

ベースのルールを既存のポリシーに取り込む一般的な方法を説明し、アイデンティティ ベースのルールを許可するポリシーごとの設定について、詳細な情報を提供します。

アイデンティティ ベースのルールを追加する際のガイドライン

アイデンティティ ベースのルールを追加する際の一般的なガイドラインと推奨事項は以下のとおりです。

- FQDN（完全修飾ドメイン名）のネットワーク/ホスト オブジェクトは、送信元フィールドと宛先フィールドの両方に使用できます。これらのオブジェクトの設定の詳細については、ネットワーク/ホストオブジェクトの作成を参照してください。
- Active Directory（AD）ユーザ名またはユーザ グループ名を指定するユーザ、ユーザ グループ、アイデンティティ ユーザ グループ オブジェクトは、別個のフィールド [User] で定義されます。1 つ以上のユーザー名、ユーザーグループ名、またはアイデンティティ ユーザー グループ オブジェクトを使用してルールを設定した場合、指定により送信元アドレスの設定のみが変更されます。宛先フィールドに指定されたアドレスには適用されません。これらのアイデンティティ ユーザ グループ オブジェクトの設定の詳細については、アイデンティティ ユーザ グループ オブジェクトの作成 （25 ページ）を参照してください。

ルールを主に、指定したユーザまたはユーザ グループに基づいて動作するようにする場合でも、送信元アドレスはルール内に設定する必要があります。送信元指定とユーザ指定は、その組み合わせでルールの有効範囲をコントロールします。送信元フィールドの値に基づいて、ルールは次のように動作します。

- **Source = any**：ルールをユーザー指定にのみ基づいて適用する場合、送信元として「any」を使用します。これらのルールは、ユーザがトラフィックを送信するワークステーションの IP アドレスに関係なくユーザ指定と一致します。
- **Source = その他**：送信元アドレスとして「any」以外を指定した場合は、ユーザーが送信元アドレス指定と一致する IP アドレスからトラフィックを送信した場合にのみ、ルールが適用されます。送信元のネットワークに基づいてさまざまなサービスを提供する場合は、この方法を使用します。

たとえば、内部に信頼されたネットワークがある場合、特定のユーザ グループ内のユーザには、そこから機密性の高い宛先へのアクセスを許可しても、そのユーザが信頼されるネットワークの外部にいる場合はアクセスを拒否することができます。この場合は、信頼されたネットワークを送信元、信頼されたユーザ グループをユーザ、機密性の高いサーバを宛先として指定した許可ルールを作成します。また、送信元と宛先だけを指定した特定の拒否ルールを作成したり、デフォルトのすべて拒否ルールによって、一致しないトラフィックをキャプチャすることもできます。

- ユーザ アイデンティティの影響をまったく受けないトラフィック クラスがあるかどうか確認します。たとえば、DNS トラフィックはすべてのユーザに許可されます。こうしたタイプのルールをアイデンティティ ベースのルールよりも上位に配置すると、デバイスがアイデンティティ ベースのルールの評価を必要とする前にトラフィックの照合を迅速に許可することができます。

- ルールのトラブルシューティング時は、最終的に IP アドレスに基づいてルールが適用されることに注意してください。FQDN ルールの照合は DNS 検索に基づいて行われます。ホストの IP アドレスは、正常に終了した検索と、検索が次に更新されるときとで変化することがあります。ユーザについては、IP アドレスのマッピングはネットワークに設定された AD エージェントから取得されるか、ASA 自身によって行われる認証によって取得されます。
- FQDN 指定とユーザ指定は完全に独立したものです。それぞれを個別に使用できます。

アイデンティティ ベースのルールを許可するファイアウォール ポリシー

アイデンティティベースのルールは ASA 8.4.2 以降だけで可能です。以下のポリシーにより、アイデンティティ ベースのルールを設定できます。

- AAA ルール：[ファイアウォール（Firewall）] > [AAA ルール（AAA Rules）] を選択します。ASA、PIX、および FWSM デバイスの AAA ルールの設定を参照してください。

ヒント AAA ルールは、カットスルー プロキシの設定に使用できます。このプロキシにより、IP アドレスのマッピングが無効になり、ネットワーク アクセスが拒否されたユーザが、マッピングの問題を解決するために ASA に直接認証処理を行うことができるようになります。カットスルー プロキシの設定 （31 ページ）を参照してください。

- アクセスルール：[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] を選択します。アクセス ルールの設定を参照してください。
- インスペクションルール：[ファイアウォール（Firewall）] > [インスペクションルール（Inspection Rules）] を選択します。インスペクション ルールの設定を参照してください。
- 拡張 ACL ポリシー オブジェクトを使用するポリシー：複数のファイアウォール ポリシーが拡張 ACL ポリシー オブジェクトを使用して、ルール テーブルを直接ポリシーに取り込む代わりにトラフィック照合基準を定義できます。FQDN オブジェクトまたはユーザ指定を組み込むために拡張 ACL ポリシー オブジェクトを設定できます（拡張アクセス コントロール リスト オブジェクトの作成を参照）。これらのアイデンティティ ベースの拡張 ACL オブジェクトは、次のポリシーで使用できます。
  - ボットネット トラフィック フィルタ ルール：[ファイアウォール（Firewall）] > [ボットネット トラフィック フィルタ ルール（Botnet Traffic Filter Rules）] を選択します。ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化を参照してください。アイデンティティ ベースの ACL は、イネーブル ルールおよびドロップ ルールのトラフィック分類として使用できます。
  - IPS ルール、QoS ルール、および接続ルール（サービスポリシールール）：[プラットフォーム（Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、QoS、および接続ルール（IPS, QoS, and Connection Rules）] を選択します。[サービスポリシールール（Service Policy Rules）] ページを参照してください。

このポリシーのトラフィック照合基準は、トラフィック フロー ポリシー オブジェクトに組み込まれる拡張 ACL ポリシー オブジェクトに基づいて行われます。アイデンティティ ベースのトラフィック分類を組み込むトラフィック フロー オブジェクトに、ACL を指定するオプションをいずれか選択する必要があります。アイデンティティ ベースの ACL はすべてのサービス タイプに使用できます。詳細については、トラフィック フロー オブジェクトの設定を参照してください。

このポリシーで使用できるサービスの 1 つであるユーザ統計は、アイデンティティ ベースのファイアウォールユーザのアカウンティング情報の収集用に特別に設計されたものです。ユーザ統計の収集 （34 ページ）を参照してください。

- リモート アクセス グループ ポリシーでの VPN フィルタ：VPN フィルタ ACL が VPN トラフィックに適用されます。VPN フィルタは、リモート アクセス接続ポリシーで使用する ASA グループ ポリシー オブジェクトの [Connection Settings] ページに設定できます。ASA グループ ポリシーの接続設定およびアイデンティティ ベースのルールを使用した VPN トラフィックのフィルタリング （35 ページ）を参照してください。

アイデンティティ ベースのルールまたはオブジェクトを許可しないポリシー

ポリシーには、ネットワーク/ホスト オブジェクトまたは拡張 ACL オブジェクトを指定できるタイプがありますが、このタイプのオブジェクトやアイデンティティ ユーザ グループ オブジェクトを使用する FQDN ネットワーク/ホスト オブジェクトまたは ACL を許可しないポリシーもあります。こうしたタイプのオブジェクトを使用できない例を、いくつか次に示します。

- ルート マップを含むルーティング ポリシー。
- Network Address Translation（NAT; ネットワーク アドレス変換）。
- WCCP（Web キャッシュ コントロール プロトコル）。
- VPN 設定のクリプト マップ。
- リモート アクセス VPN 設定のダイナミック アクセス ポリシー。

カットスルー プロキシの設定

ID 認証ファイアウォール ポリシーを使用する場合、ユーザから IP アドレスへのマッピングは、さまざまな機能、主にネットワーク内の AD エージェントから取得されます。マッピングは定期的に更新されますが、ユーザから IP アドレスへのマッピングが同期されていないために、ファイアウォール ルールによって正規のユーザがブロックされる場合があります。

この状態に備えるためカットスルー プロキシを設定できます。カットスルー プロキシを使用すると、ユーザがブロックされても ASA に直接サインオンできます。ASA は、ユーザの現在の IP アドレスを正しく反映するようにユーザから IP へのマッピングを更新します。HTTP パケット/HTTPS パケットを受信して認証するインターフェイスを含むすべてのコンテキストに新しいマッピングが転送されます。

AAA ルールはカットスルー プロキシの設定に使用できます。設定の選択項目は、1 つ以上の NetBIOS ドメインがネットワーク内にあるかどうかに基づき、2 種類が用意されています。

- 単一ドメイン：認証用に通常の AAA ルールを設定し、このドメインに対して Active Directory サーバを識別する LDAP サーバ グループを指定します。送信元には「any」を使用し、宛先には ASA の IP アドレスを使用します。サービスには HTTP と HTTPS を含めることができます。次に、サーバーへの認証を必要とする場合、ユーザーは次の標準認証 URL のいずれかを入力します。interface_ip はインターフェイスの IP アドレスで、対話型認証テーブルでプロトコルにデフォルト以外のポートを指定した場合、port はポート番号（任意）です。**http://***interface_ip* [**:***port*]**/netaccess/connstatus.html** or **https://***interface_ip* [**:***port*]**/netaccess/connstatus.html**。

ヒント　ユーザから IP へのマッピングは、選択した AD サーバ グループに設定されたドメインと同じドメインの下に置かれます。別の方法を認証に使用した場合、マッピングは LOCAL ドメインの下に置かれます。

- 複数ドメイン：特定の AAA サーバ グループではなくユーザ ID オプションを使用する 2 種類の認証ルールを設定します。次の手順で、このステップについて説明します。この設定は単一ドメイン ネットワークでも機能します。単一ドメインの場合と同じ URL を使用して ASA への認証を行います。

ユーザ ID オプションを使用する場合、認証は次のように処理されます。

- ユーザがログイン クレデンシャルに DOMAIN\username 形式でドメインを組み込んでいると、ASA はそのドメインを使用して、アイデンティティ オプションのポリシー内のドメイン マッピングに基づいてどの AD サーバを認証に使用するか決定します。AAA サーバがドメインにマップされていない場合、認証の試行は拒否されます。
- ログイン クレデンシャルに識別可能なドメイン名が含まれていない場合（\ 文字がユーザ名ストリングに含まれていない場合）、ASA はアイデンティティ オプションのポリシーで選択されたデフォルトのドメインに割り当てられている AD サーバを使用します。AAA サーバがデフォルトのドメインにマップされていない場合、認証の試行は拒否されます。

ヒント　カットスルー プロキシは IPv4 アドレスでのみ機能します。IPv6 はサポートされていません。

関連項目

- ID 認証ファイアウォール ポリシーの要件　（3 ページ）
- ID 認証サービスを提供するためのファイアウォールの設定　（8 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定
- ユーザの認証方法について

ステップ 1 Active Directory サーバおよびエージェントの識別 （10 ページ）の説明のとおり、すべての NetBIOS ドメインと、そのネットワーク用の AD サーバ グループ、および AD エージェント グループを指定するようにアイデンティティ オプション ポリシーを設定します。

ステップ 2 次のいずれかを実行して、[AAA Rules] ページを開きます。

- （デバイスビュー）：ポリシーセレクタから **[ファイアウォール（Firewall）] > [AAAルール（AAA Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）]>[AAAルール（AAA Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 3 [行の追加（Add Row）] ボタンを使用して次のルールを作成します。[Add AAA Rules] ダイアログボックスの詳細については、[Add AAA Rule]/[Edit AAA Rule] ダイアログボックスを参照してください。

ヒント 次のルールに示すものよりも詳細な送信元指定、宛先指定、サービス指定を使用できます。

ルール 1：認証済みユーザに再認証を強制しない。

- [認証アクション（Authentication Action）] オプションおよび [ユーザーID（User-Identity）] オプションを選択します。
- Action = Deny。AAA 認証ルールの場合、「deny」ではユーザーは認証を要求されませんが、ユーザーのトラフィックがドロップされるわけではありません。
- Sources = any。
- Users = all-auth-users。

ユーザーの場合、**all-auth-users** は、Active Directory で認証済みで、IP マッピングが存在するユーザーを意味します。

- Destination = any。
- Services = IP。
- AAA Server Group =（選択なし）。
- Interface =（選択、通常はインターフェイス内）。

ルール 2：まだ認証されていないユーザを認証する。

- [認証アクション（Authentication Action）] オプションおよび [ユーザーID（User-Identity）] オプションを選択します。
- Action = Permit。このアクションには認証と照合を行うユーザが必要です。
- User = all-unauth-users。

この場合、**all-unauth-users** は Active Directory で認証されていないすべてのユーザーを意味します。

- その他のオプションは最初のルールと同じです。

ユーザ統計の収集

アイデンティティ ベースのファイアウォール ポリシーに関するユーザ統計のアカウンティング情報を収集できます。これらの統計情報は、ユーザ名またはユーザ グループ メンバーシップに基づいてファイアウォール ポリシーが適用されるユーザに対して保持されます。

関連項目

- ID 認証ファイアウォール ポリシーの要件 （3 ページ）
- ID 認証サービスを提供するためのファイアウォールの設定 （8 ページ）
- [サービスポリシールール（Service Policy Rules）] ページ
- トラフィック フロー オブジェクトの設定

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [プラットフォーム（Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、QoS、および接続ルール（IPS, QoS, and Connection Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、QoS、および接続ルール（IPS, QoS, and Connection Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを追加する行を選択して、テーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックし、Insert Service Policy Rule ウィザードを開始します。

ステップ 3 ウィザードのステップ 1 で、ルールをグローバルにするか、特定のインターフェイスまたはインターフェイス ロールに適用するかを選択します。ユーザのトラフィックがどのインターフェイスを通過するかに関係なく、ユーザの統計を収集する場合は [Global] を選択します。

[次へ（Next）] をクリックします。

ステップ 4 ステップ 2 で、統計情報の収集対象となるトラフィックを定義するトラフィック クラスを選択します。すべてのトラフィックで統計情報を収集する場合は、class-default を選択します。対象がすべてのトラフィックではない場合は、[Traffic Class] を使用してトラフィック照合属性を定義するトラフィック フロー オブジェクトを選択します。

[次へ（Next）] をクリックします。

ステップ 5 ステップ 3 で、[ユーザー統計（User Statistics）] タブを選択します。

- [ユーザー統計アカウンティングの有効化（Enable user statistics accounting）] を選択します。

- 収集する情報のタイプを選択します。
  - **Account for sent drop count**
  - **Account for sent packet, sent drop and received packet count**

ステップ 6 [終了（Finish）] をクリックしてルールを保存します。

アイデンティティベースのルールを使用したVPNトラフィックのフィルタリング

ASA 上のリモート アクセス VPN をサポートしている場合、ユーザ依存のアクセスを設定します。アイデンティティ ベースのルールは、リモート ユーザ アクセスの検証後、トラフィックをフィルタリングするために使用することもできます。

VPN 用のアイデンティティ ベースのルールを作成する前に、VPN ユーザ名のルールについて理解し、このルールが正しいドメイン名を使用していることを確認する必要があります。

- 認可に Active Directory LDAP サーバ グループを使用していて、ドメイン グループ/サーバ グループをアイデンティティ オプションのポリシーに設定した場合、ユーザ名はNetBIOS ドメインに関連付けられます。
- 他の許可メカニズムの場合、VPN ユーザのドメイン名は LOCAL になります。

これらのことを考慮して、アイデンティティ ベースの ACL ルールで VPN 上のトラフィックをフィルタリングするために使用できる方法は次の 2 種類です。

- ASA グループ ポリシー オブジェクトに VPN フィルタを適用します。このフィルタはグループ内のすべてのユーザに適用されます。VPN フィルタは、リモート アクセス接続ポリシーで使用する ASA グループ ポリシー オブジェクトの [Connection Settings] ページに設定できます。ASA グループ ポリシーの接続設定を参照してください。
- デフォルトでは、VPN トラフィックがインターフェイス アクセス ルールをバイパスします。この動作は、すべての VPN トラフィックがインターフェイス アクセス ルールも経由するように変更できます。この方法を採用した場合、インターフェイス ルールは VPN トラフィックに依存することに注意してください。VPN トラフィックがインターフェイス アクセス ルールを経由するようにするには、RA VPNグローバル設定ポリシーの [ISAKMP/IPsec] タブで [Sysopt上でのIPsecの有効化（Enable IPsec over Sysopt）] オプションの選択を解除してください。VPN グローバル ISAKMP/IPsec 設定 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 ポリシーの監視

Event Viewer を使用して、他のタイプのポリシーやイベントと同じ方法で ID 認証ファイアウォール ポリシーを監視できます。次に、アイデンティティ ポリシーを効率的に監視するた

めのヒントをいくつか示します。Event Viewer 使用の一般情報については、イベントの表示を参照してください。

- アイデンティティ ファイアウォールに特に関連した syslog メッセージのグループは 746001 ～ 746019 です。これらのメッセージの説明については、http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html で、ご使用の ASA ソフトウェアバージョンの Syslog メッセージ [英語] を参照してください。

特に重要なのは、次のメッセージです。

- **746004 と 746011**：これらの syslog は、ユーザーグループまたはユーザーへの参照数がサポートされる数を超えたことを示します。ポリシーの変更を検討する必要があります。これらの制約事項の詳細については、ID 認証ファイアウォール ポリシーの要件 （3 ページ）を参照してください。
- **746003**：IP アドレスへのユーザーグループまたはユーザーマッピングのダウンロードに失敗しました。メッセージには、失敗の理由についての説明があります。
- **746005**：AD エージェントに到達できませんでした。このエージェントが正しく機能し、ASA とエージェントの間にネットワーク パスが存在することを確認してください。
- **746010**：メッセージに示された理由によって、インポートしたユーザーまたはユーザーグループへの更新が失敗しました。
- **746016**：メッセージに示された理由によって、完全修飾ドメイン名（FQDN）への DNS 探索が失敗しました。
- 複数の既存の syslog メッセージにユーザ名または FQDN 情報が含まれるようになりました。Event Viewer には [Destination User Identity] 情報と [FQDN and Source User Identity] 情報を表示する 2 つのカラムがあります。更新されたメッセージは次のとおりです。
  - 302005、302006、302013、302014、302016 ～ 302018、302020、302021。
  - 305005、305006、305009 ～ 305013。
  - 304001 ～ 304002 には ID 情報が含まれていますが解析されません。
- [Event Type] にフィルタを作成し、[Identity Firewall Events] フォルダを選択することで、すべてのアイデンティティ関連の syslog メッセージをフィルタリングできます。
- Event Viewer からの Security Manager ポリシーの検索の説明のとおり、イベントで Go to Policy コマンドを使用する場合は、ID 情報が検索基準に含まれます。ID 情報は、106100 には含まれていないことに注意してください。そのためこのメッセージのポリシー検索は、ユーザ ID の影響を受けません。

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。