ASA 8.X 以降： ASDM GUI を使用したアクセス リストの追加または変更の設定例

目次

概要

このドキュメントでは、アクセス コントロール リストで Cisco Adaptive Security Device Manager (ASDM) を使用する方法について説明します。 また、新しいアクセス リストの作成、既存のアクセス リストの編集方法、およびアクセス リストのその他の機能について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- バージョン 8.2.X の Cisco 適応型セキュリティ アプライアンス (ASA)

- Cisco Adaptive Security Device Manager（ASDM）バージョン 6.3.X

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

アクセス リストは、主にファイアウォールを介したトラフィック フローの制御に使用されます。 アクセス リストを使用して、特定のタイプのトラフィックを許可または拒否できます。 すべてのアクセス リストには、特定の送信元から特定の宛先へのトラフィック フローを制御する多くのアクセス リスト エントリ（ACE）の数が含まれます。 通常、このアクセス リストはインターフェイスにバインドされ、検索するフローの方向を示します。 アクセス リストは、大きく 2 種類に分けられます。

1. 着信アクセス リスト
2. 発信アクセス リスト

着信アクセス リストは、インターフェイスに入るトラフィックに適用されます。発信アクセス リストは、インターフェイスから出るトラフィックに適用されます。 着信/発信表記は、セキュリティが高いインターフェイスと低いインターフェイスとの間のトラフィックの移動ではなく、そのインターフェイスのトラフィックの方向を示します。

TCP 接続と UDP 接続では、リターン トラフィックを許可するアクセス リストは必要ありません。これは、セキュリティ アプライアンスによって、確立された双方向接続のすべてのリターン トラフィックが許可されるためです。 ICMP などのコネクションレス プロトコルの場合、セキュリティ アプライアンスにより、単方向セッションが確立されます。そのため、送信元と宛先のインターフェイスにアクセス リストを適用して両方向の ICMP を許可するか、ICMP インスペクション エンジンを有効にする必要があります。 ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

ASDM バージョン 6.3.X 以降では、設定できるアクセス リストは、次の 2 種類があります。

1. インターフェイス アクセス ルール
2. グローバル アクセス ルール

注: アクセス ルールは、個々のアクセス リスト エントリ（ACE）を参照します。

インターフェイス アクセスルールは、作成時に任意のインターフェイスにバインドされます。 インターフェイスにバインドしない場合、作成できません。 これは、コマンド ラインの例とは異なります。 CLI の場合、**access list** コマンドを使用してアクセス リストを作成してから、**access-group** コマンドを使用してアクセス リストをインターフェイスにバインドします。 ASDM 6.3 以降では、アクセス リストの作成とインターフェイスへのバインドが 1 つのタスクとして実行されます。 これは、特定のインターフェイスを介するトラフィックだけに適用されます。

グローバル アクセス ルールは、任意のインターフェイスにバインドされません。 これらは、ASDM の [ACL Manager] タブを介して設定でき、グローバル入力トラフィックに適用されます。 実装は、発信元、宛先およびプロトコル タイプに基づいたマッチングがある場合に行われます。

これらのルールは、各インターフェイスで複製されないので、メモリ領域の節約になります。

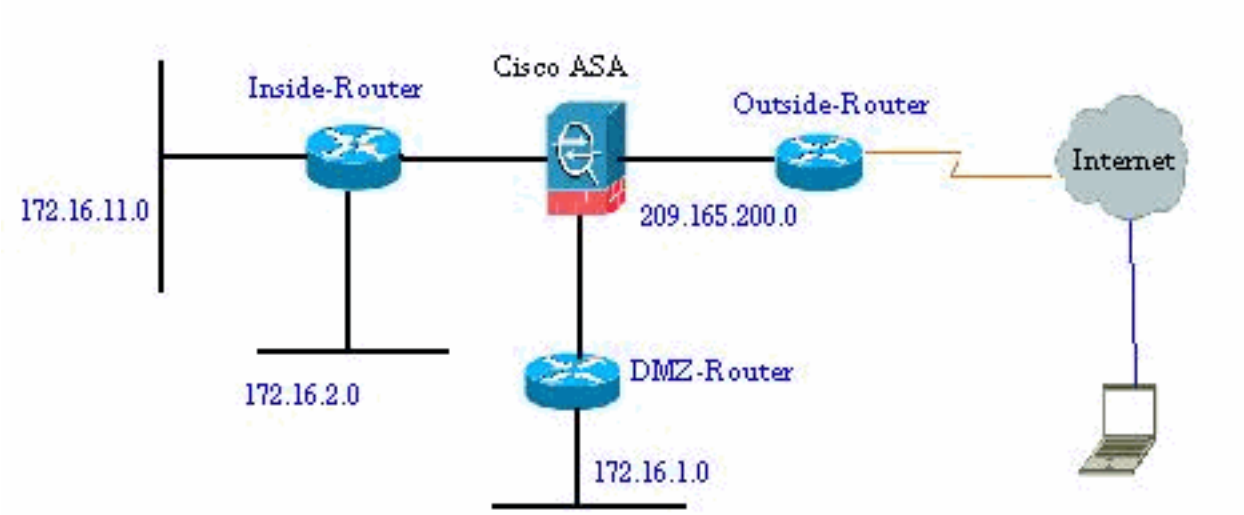
これら両方のルールが実装される場合、通常、グローバル アクセス ルールより、インターフェイス アクセス ルールが優先されます。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

ネットワーク図

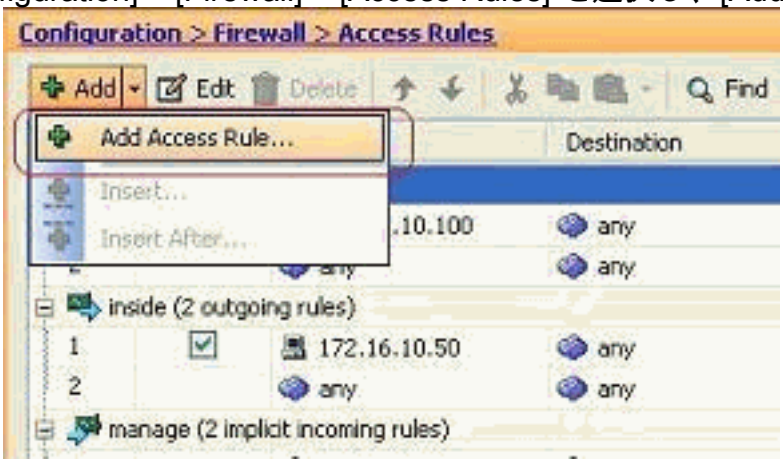
このドキュメントでは、次のネットワーク構成を使用しています。



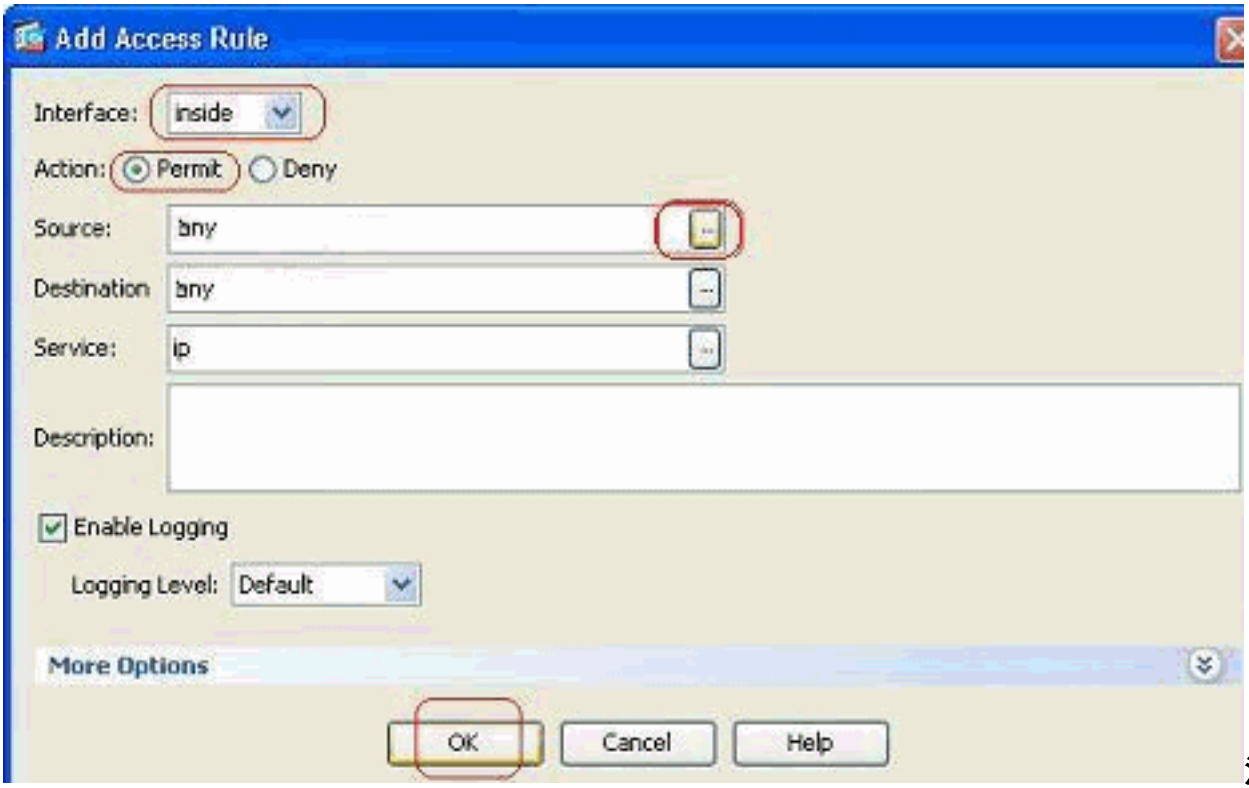
新規アクセス リストの追加

ASDM で新しいアクセス リストを作成するには、次の手順を実行します。

1. Choose [Configuration] > [Firewall] > [Access Rules] を選択し、[Add Access Rule] ボタンを選択します。

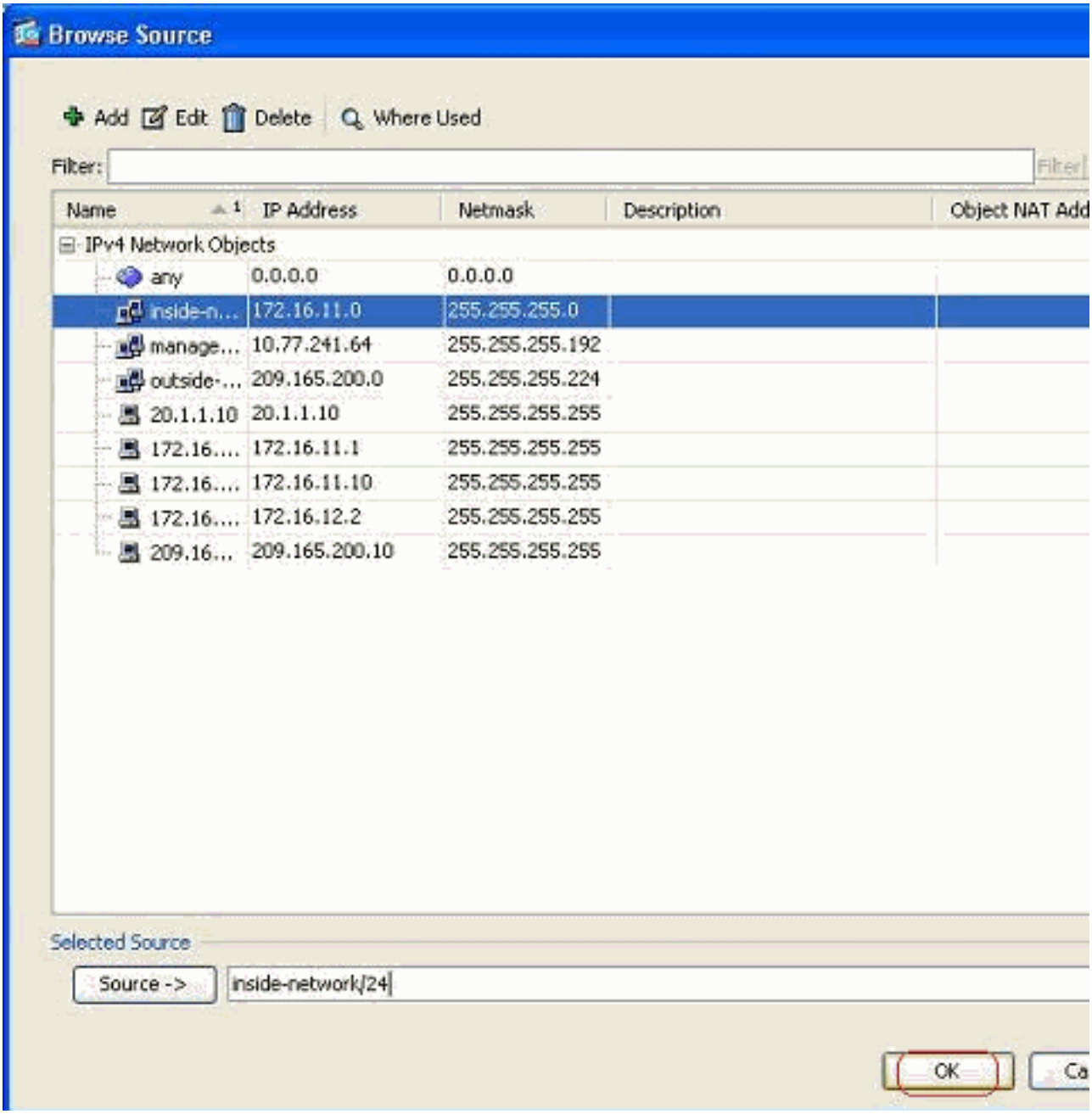


2. このアクセス リストをバインドする必要があるインターフェイス、およびトラフィックで実行するアクション（許可や拒否）を選択します。 それからソースネットワークを選択するために Detailsbutton をクリックして下さい。

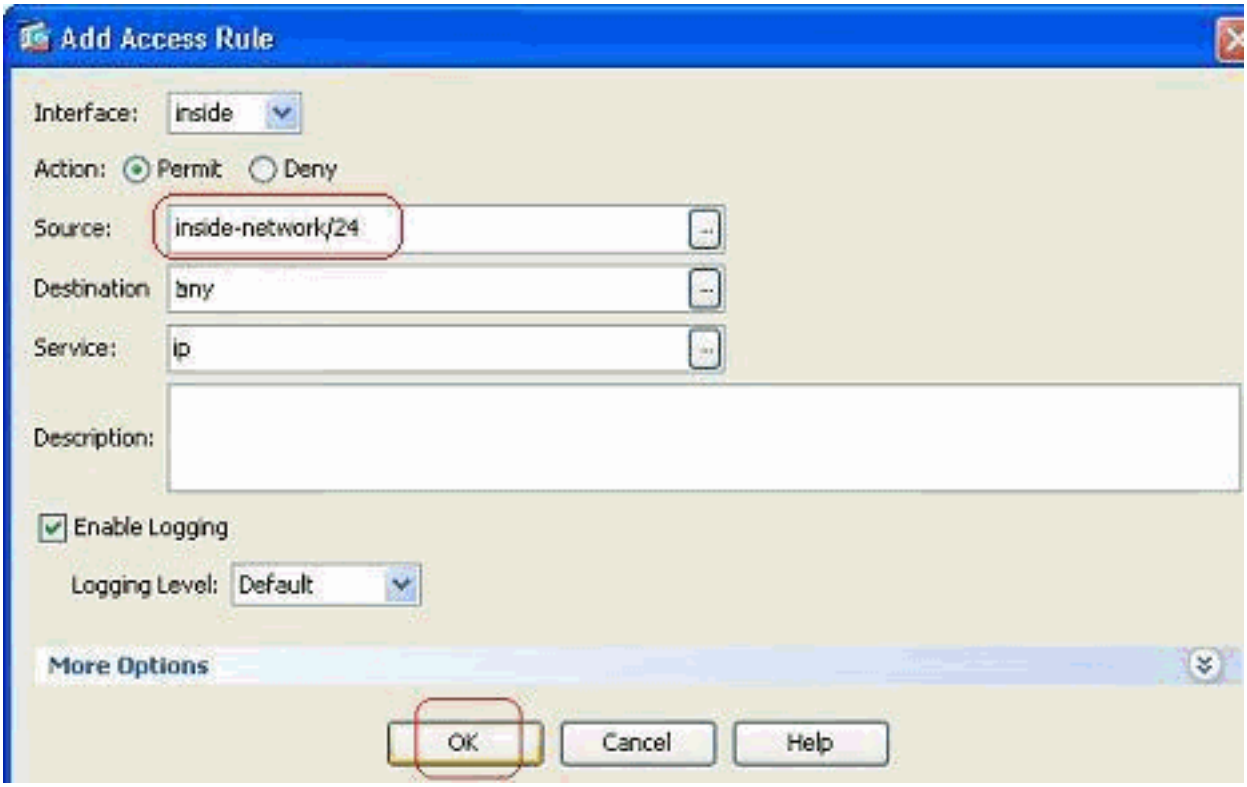


注: 次に、このウィンドウに表示されるフィールドを簡単に説明します。[Interface]：このアクセス リストがバインドされるインターフェイスを決定します。[Action]：新しいルールのアクション タイプを決定します。 次の 2 つのオプションを使用できます。 [Permit] は一致するすべてのトラックを許可します。[Deny] は一致するすべてのトラフィックをブロックします。[Source]：トラフィックの送信元を指定します。 これは、ファイアウォールまたはネットワーク オブジェクト グループの単一 IP アドレスか、ネットワークか、インターフェイス IP アドレスのいずれかとすることができます。 これらは [Details] ボタンで選択できます。[Destination]：トラフィックの宛先を指定します。 これは、ファイアウォールまたはネットワーク オブジェクト グループの単一 IP アドレスか、ネットワークか、インターフェイス IP アドレスのいずれかとすることができます。 これらは [Details] ボタンで選択できます。[Service]：このアクセス リストが適用されるトラフィックのプロトコルまたはサービスを決定します。 また、さまざまなプロトコルのセットを含むサービス グループを定義することもできます。

3. [Details] ボタンをクリックしたら、既存のネットワーク オブジェクトを含む新しいウィンドウが表示されます。 [inside-network] を選択して、[OK] をクリックします。



4. [Add Access Rule] ウィンドウに戻ります。 [Destination] フィールドに **any** と入力します。 [OK] をクリックして、アクセス ルールの設定を完了します。

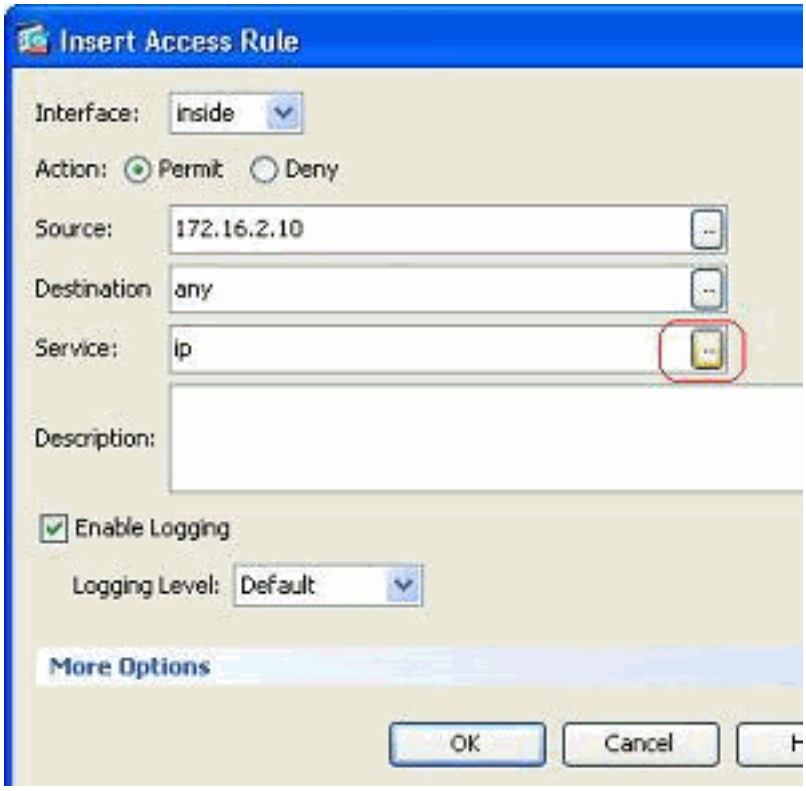


アクセス ルールを既存のアクセス ルールの前に追加する：

既存のアクセス ルールの前にアクセス ルールを追加するには、次の手順を実行します。

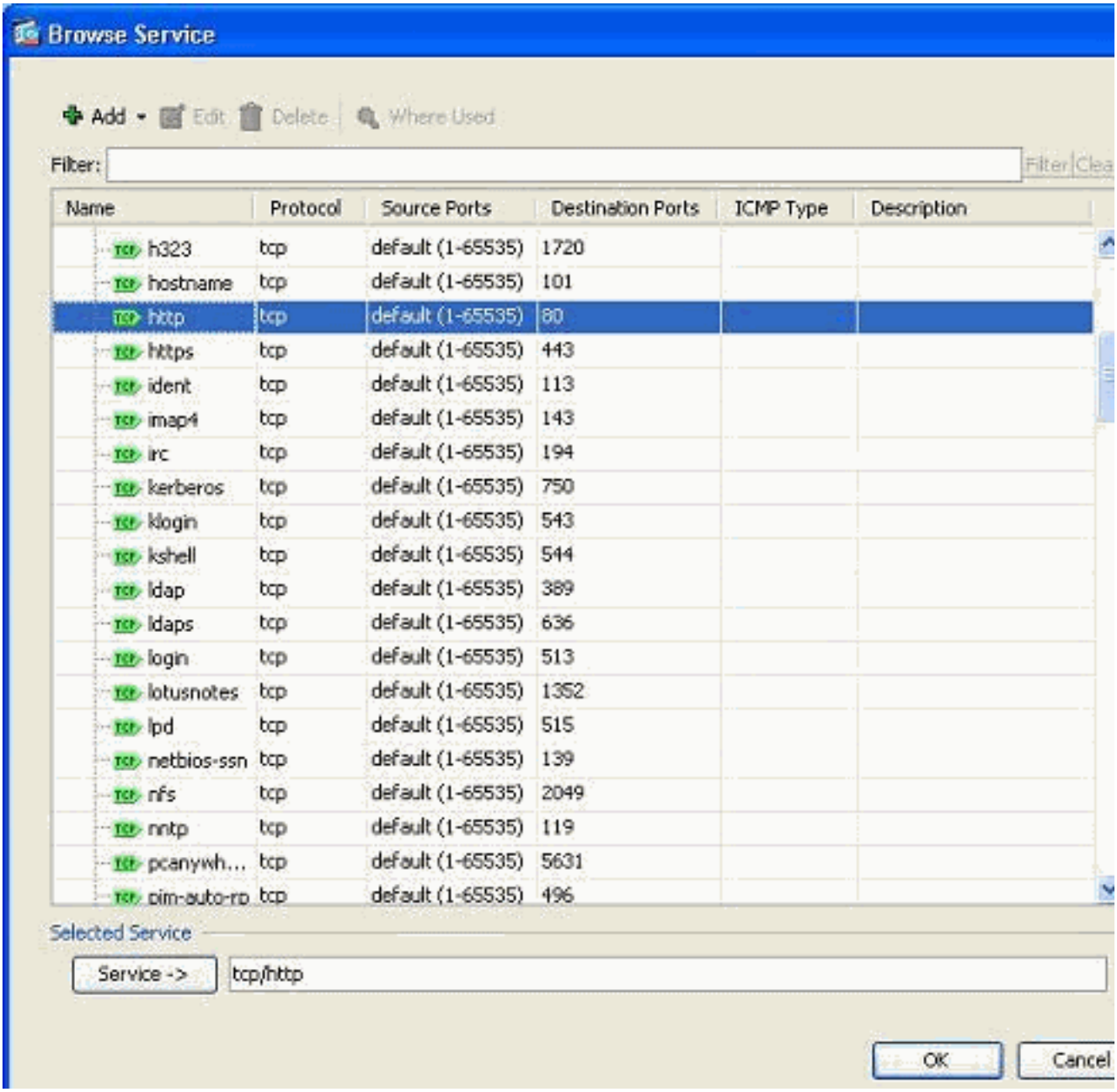
1. 既存のアクセス リスト エントリを選択して、[Add] ドロップダウン メニューから [Insert] をクリックします。 

2. 送信元と宛先を選択し、[Service] フィールドの [Details] ボタンをクリックして、[Protocol]

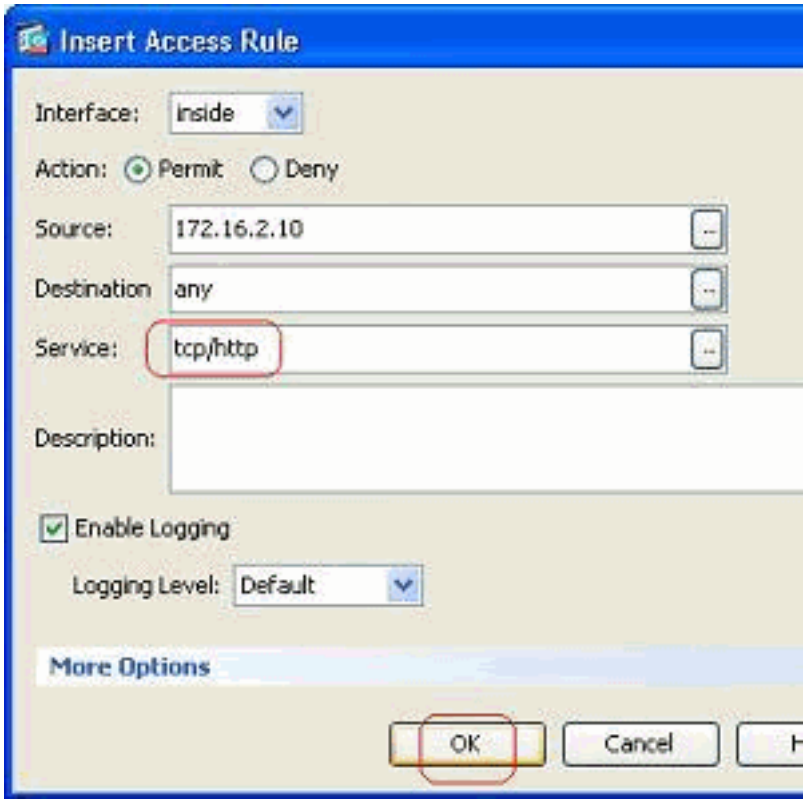


を選択します。

3. [HTTP] プロトコルを選択して、[OK] をクリックします。

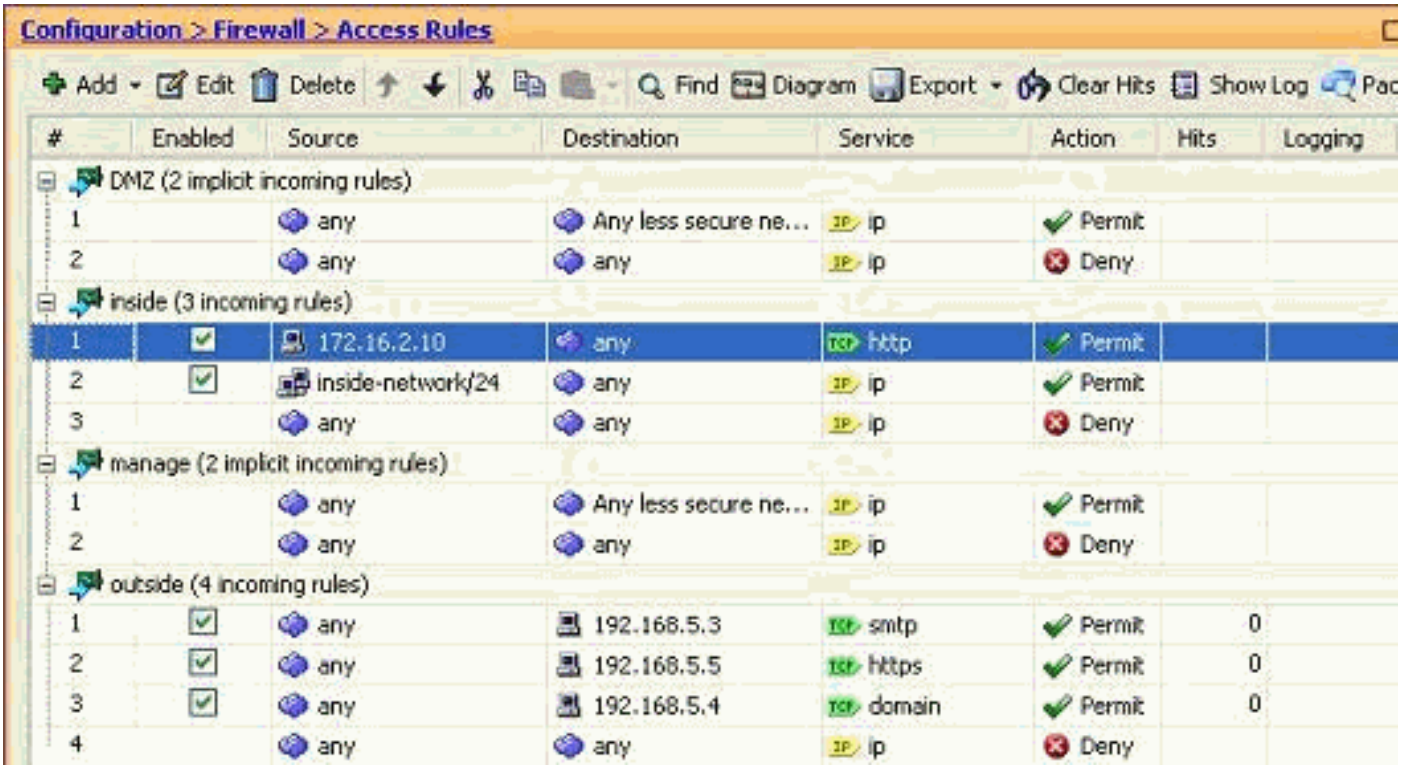


4. [Insert Access Rule] ウィンドウに戻ります。 [Service] フィールドに、選択プロトコルとして [tcp/http] が表示されます。 [OK] をクリックして、新しいアクセス リスト エントリの設



定を完了します。

新しいアクセス ルールが、Inside-Network の既存のエントリの前に表示されます。

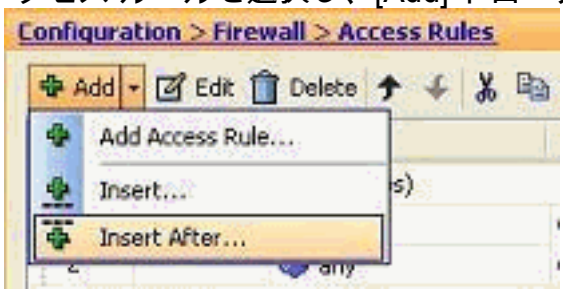


注: アクセス ルールの順序は非常に重要です。 各パケットのフィルタリング処理中、ASA は、パケットがアクセス ルール条件に一致するか順序通りに検証し、一致した場合、そのアクセス ルールのアクセスを実装します。 アクセス ルールに一致すると、他のアクセス ルールとの検証は行われません。

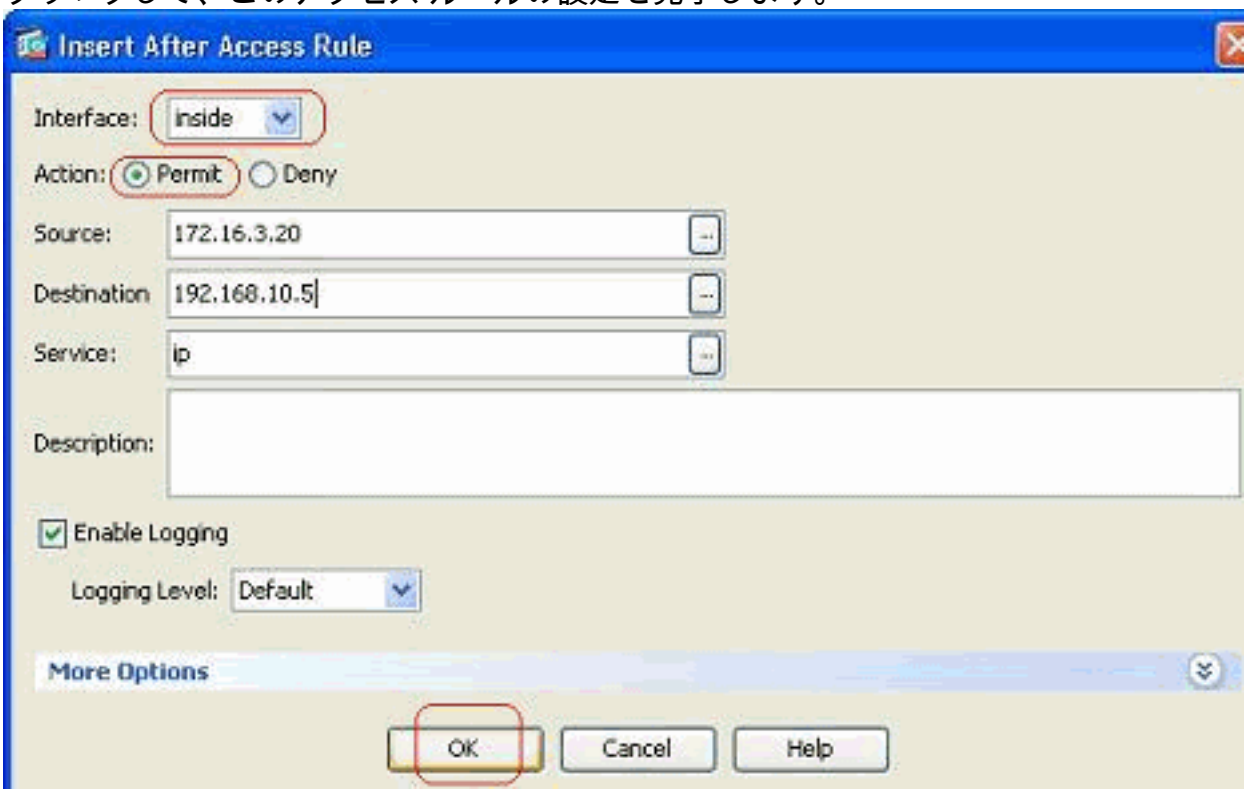
アクセス ルールを既存のアクセス ルールの後に追加する：

既存のアクセス ルールの後にアクセス ルールを作成するには、次の手順を実行します。

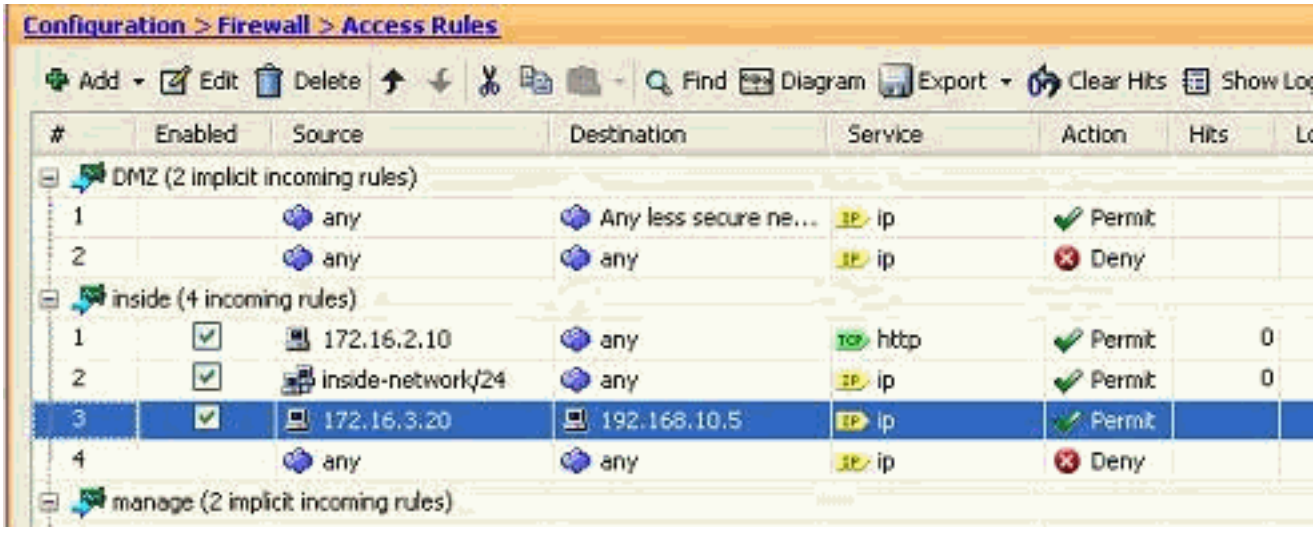
1. 新しいアクセス ルールを追加するアクセス ルールを選択し、[Add] ドロップダウン メニューから [Insert After] を選択します。



2. [Interface]、[Action]、[Source]、[Destination] および [Service] フィールドを指定し、[OK] をクリックして、このアクセス ルールの設定を完了します。



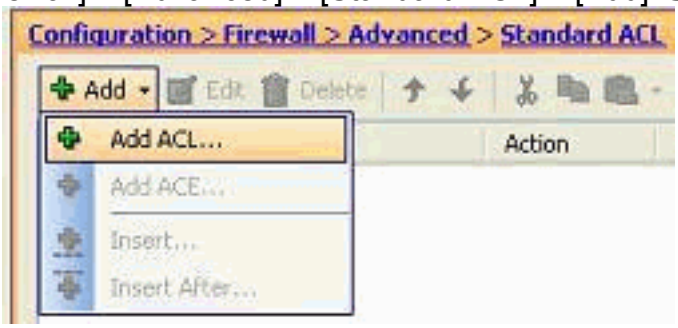
すでに設定されているアクセス ルールの後に、新しく設定したアクセス ルールが追加されていることを確認できます。



標準アクセス リストの作成

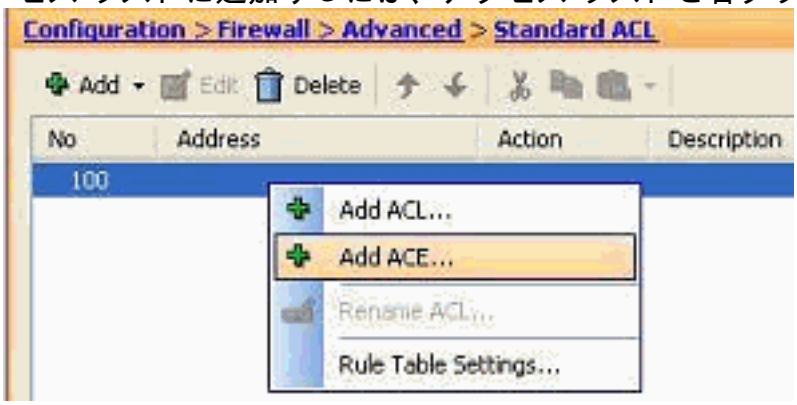
ASDM GUI で標準アクセス リストを作成するには、次の手順を実行します。

1. [Configuration] > [Firewall] > [Advanced] > [Standard ACL] > [Add] を選択して、[Add ACL] をクリックします。

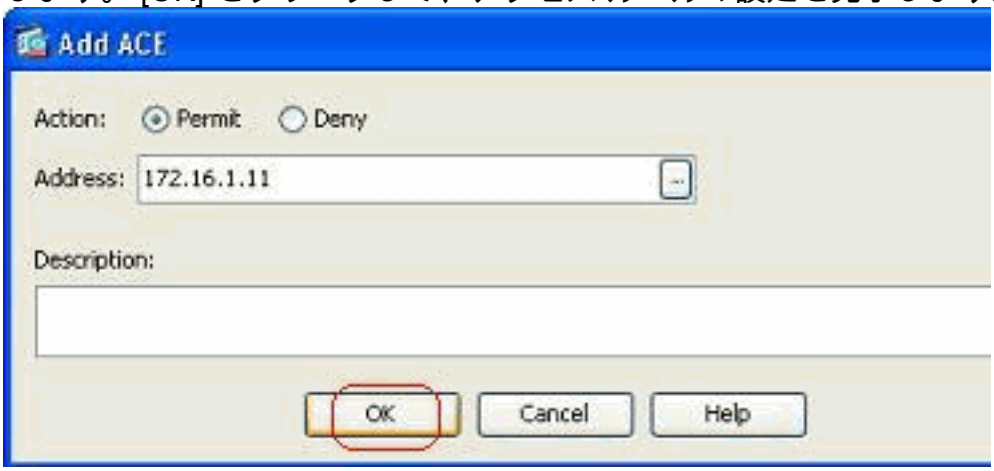


2. 標準アクセス リストで許可される範囲の数値を指定して、[OK] をクリックします。

3. アクセス ルールをこのアクセス リストに追加するには、アクセス リストを右クリックして [Add ACE] を選択します。



4. [Action] を選択して、[Source address] を指定します。 必要に応じて、[Description] も指定します。 [OK] をクリックして、アクセス ルールの設定を完了します。

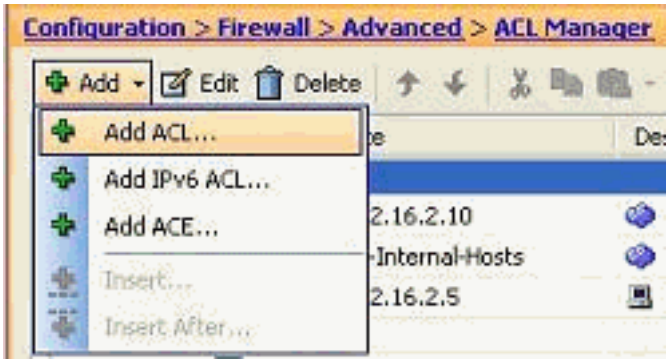


グローバル アクセス ルールの作成

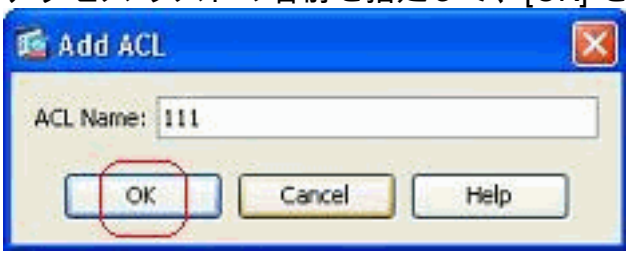
グローバル アクセス ルールを含む拡張アクセス リストを作成するには、次の手順を実行します。

1. [Configuration] > [Firewall] > [Advanced] > [ACL Manager] > [Add] を選択して、[Add ACL] ボ

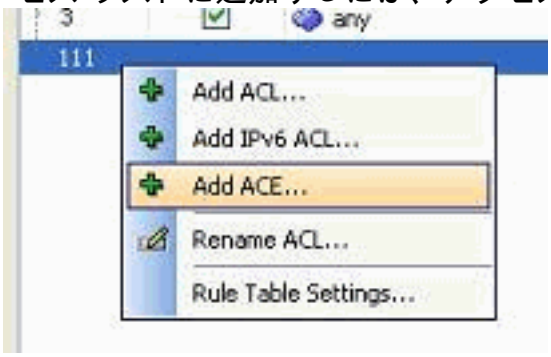
タンをクリックします。



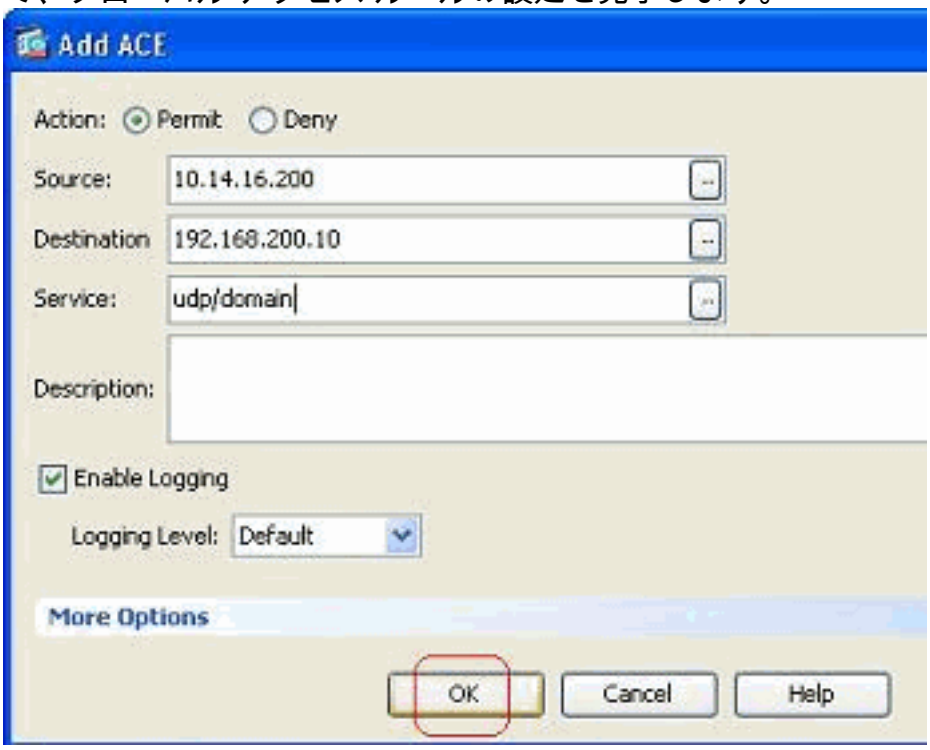
2. アクセス リストの名前を指定して、[OK] をクリックします。



3. アクセス ルールをこのアクセス リストに追加するには、アクセス リストを右クリックして [Add ACE] を選択します。



4. [Action]、[Source]、[Destination] および [Service] フィールドを完了し、[OK] をクリックして、グローバル アクセス ルールの設定を完了します。



次のように、グローバル アクセス ルールを表示できます。

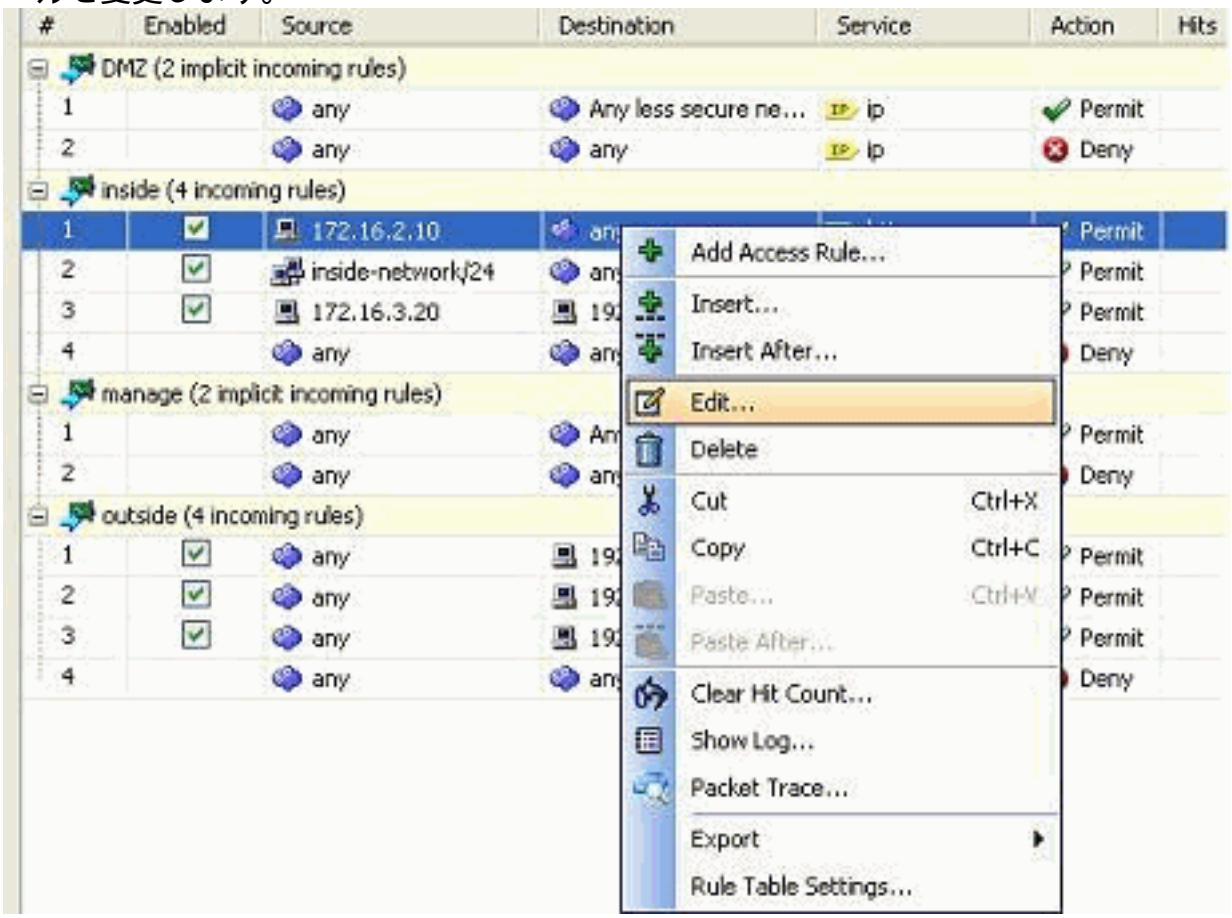
既存のアクセス リストの編集

このセクションでは、既存のアクセスの編集方法について説明します。

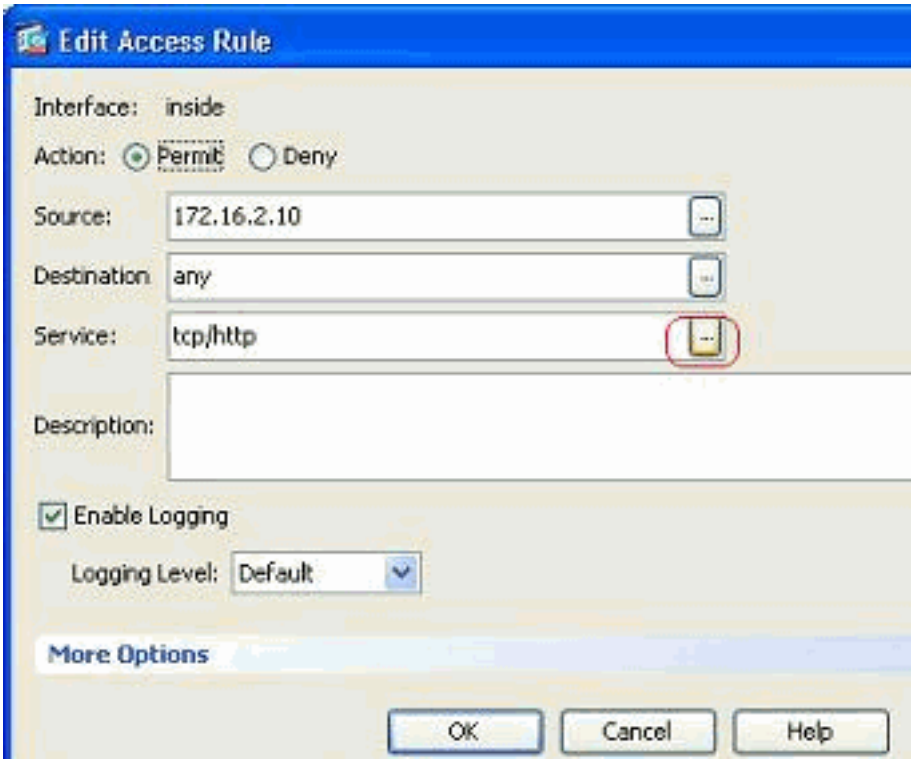
[Protocol] フィールドを編集して、サービス グループを作成する：

新しいサービス グループを作成するには、次の手順を実行します。

1. 変更する必要があるアクセス ルールを右クリックし、[Edit] を選択して、特定のアクセス ルールを変更します。

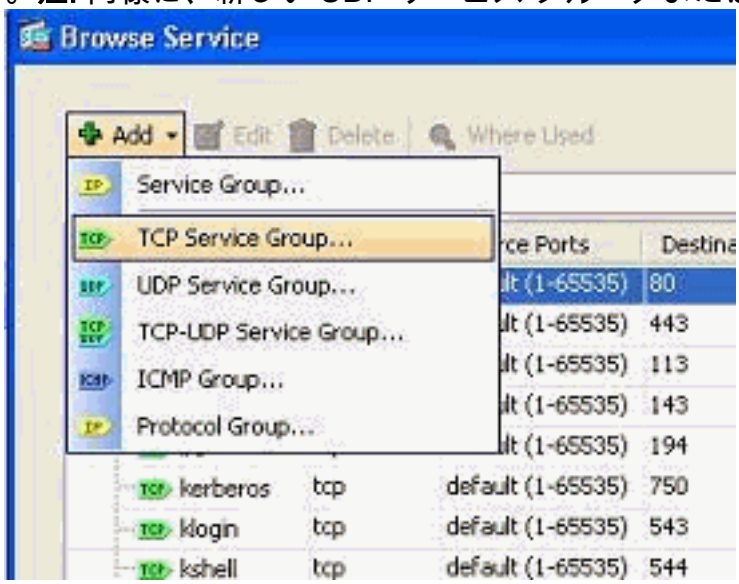


2. [Details] ボタンをクリックして、このアクセス ルールに関連付けられているプロトコルを変



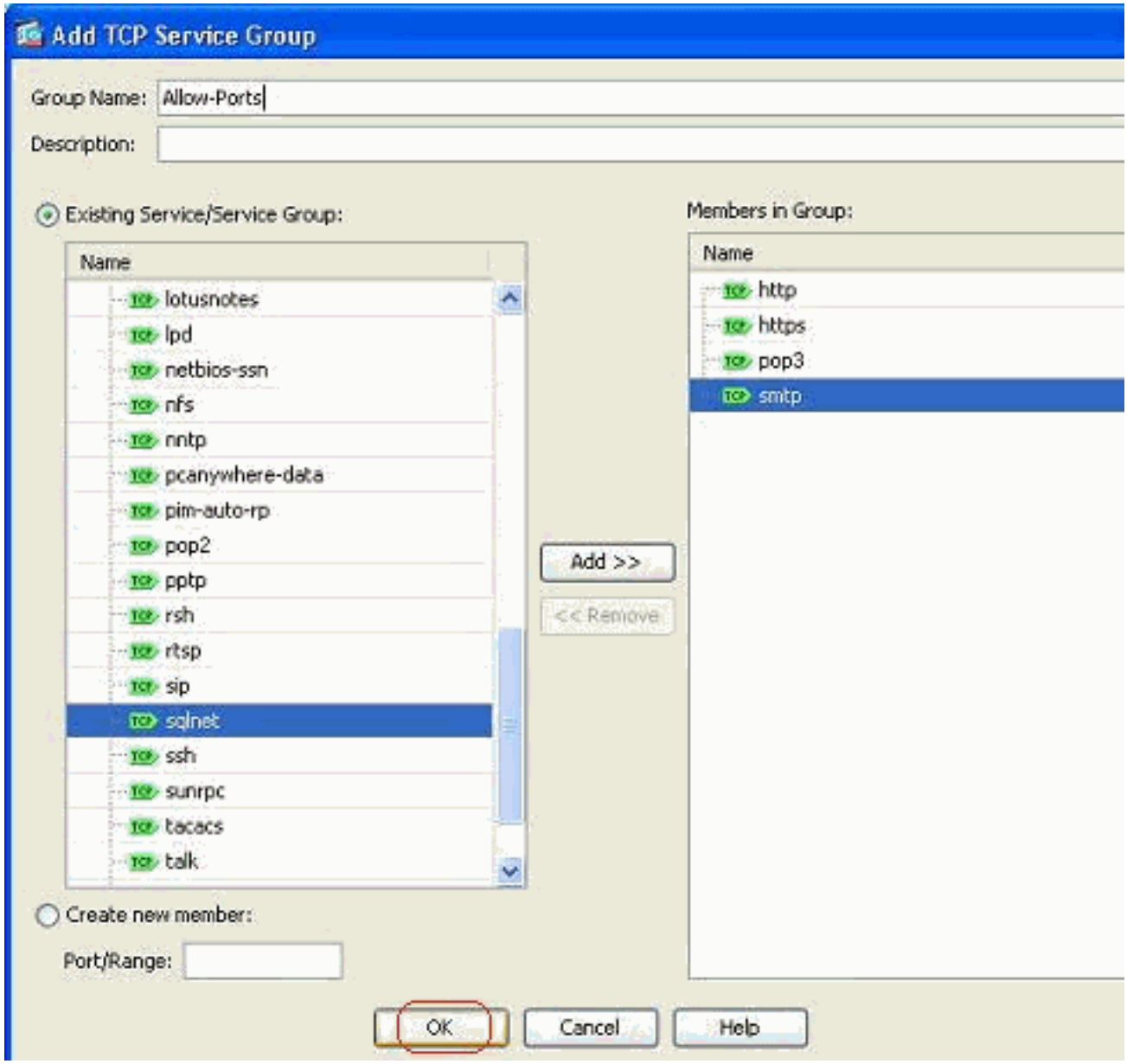
更します。

3. 必要に応じて、HTTP 以外の任意のプロトコルを選択できます。 選択するプロトコルが 1 つだけの場合、サービス グループを作成する必要はありません。 サービス グループは、マッチングする隣接しない複数のプロトコルをこのアクセス ルールで特定する必要がある場合に役に立ちます。[Add] > [TCP service group] を選択して、新しい TCP サービス グループを作成します。**注:** 同様に、新しい UDP サービス グループまたは ICMP グループなどを

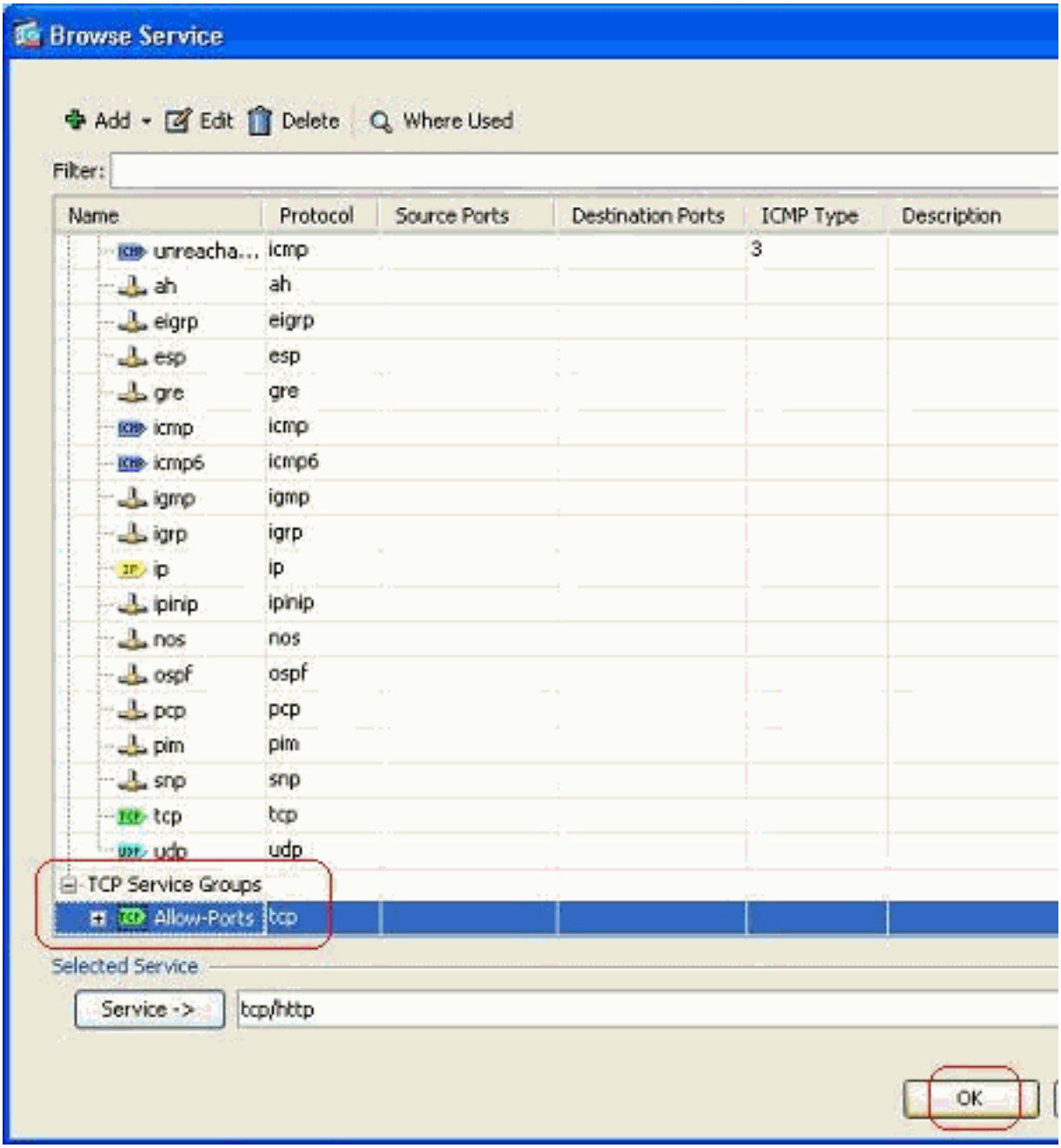


作成できます。

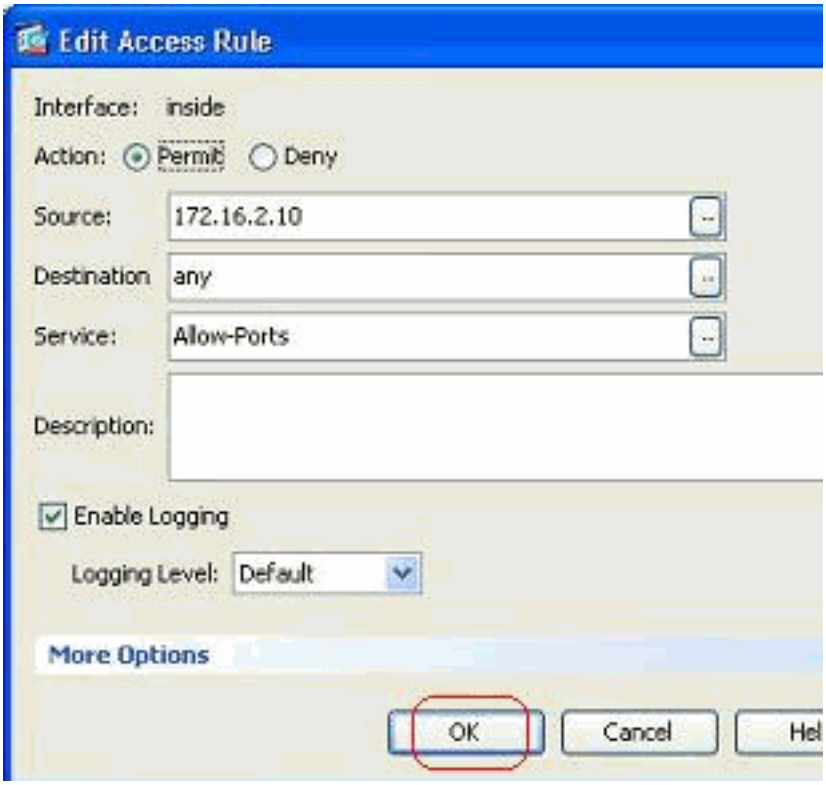
4. このサービス グループの名前を指定し、左側のメニューからプロトコルを選択し、[Add] をクリックして、右側の [Members in Group] メニューに移動します。 必要に応じて、複数のプロトコルをサービス グループのメンバとして追加できます。 これらのプロトコルは 1 つずつ追加されます。 すべてのメンバが追加されたら、[OK] をクリックします。



5. 新しく作成したサービス グループは、[TCP service groups] タブの下に表示されます。 [OK] ボタンをクリックして、[Edit Access Rule] ウィンドウに戻ります。

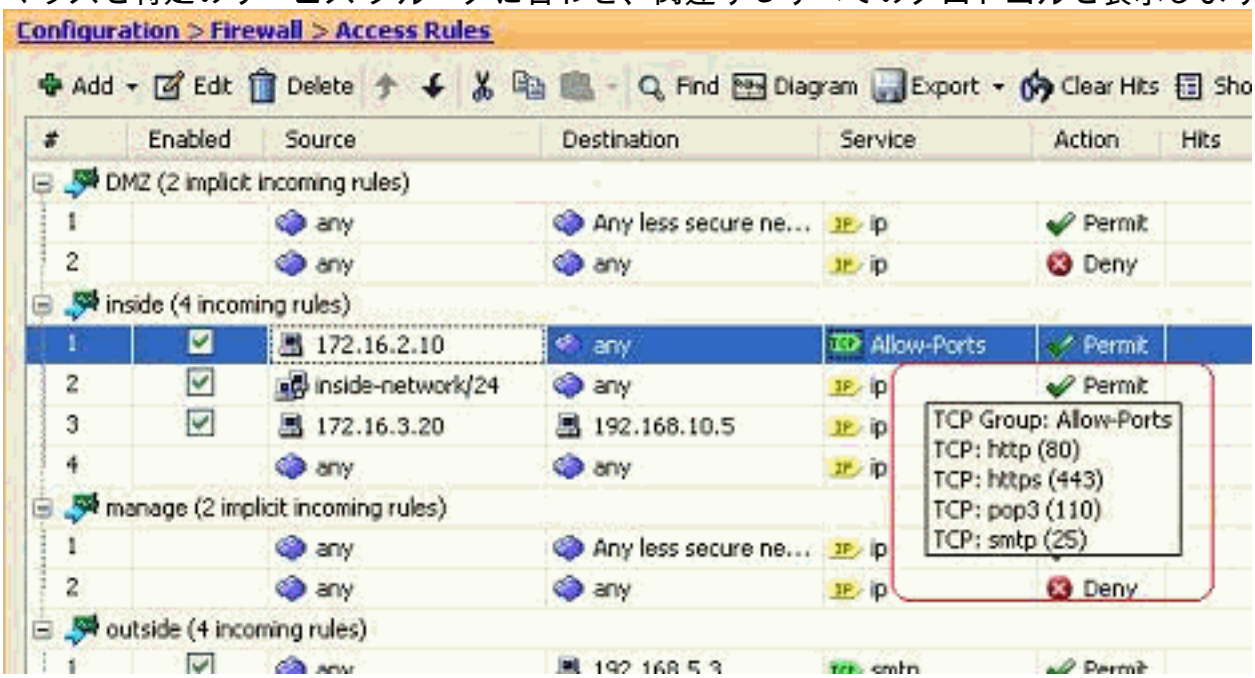


6. 新しく作成したサービス グループが [Service] フィールドに追加されます。 [OK] をクリッ



クして編集を完了します。

7. マウスを特定のサービス グループに合わせ、関連するすべてのプロトコルを表示します。

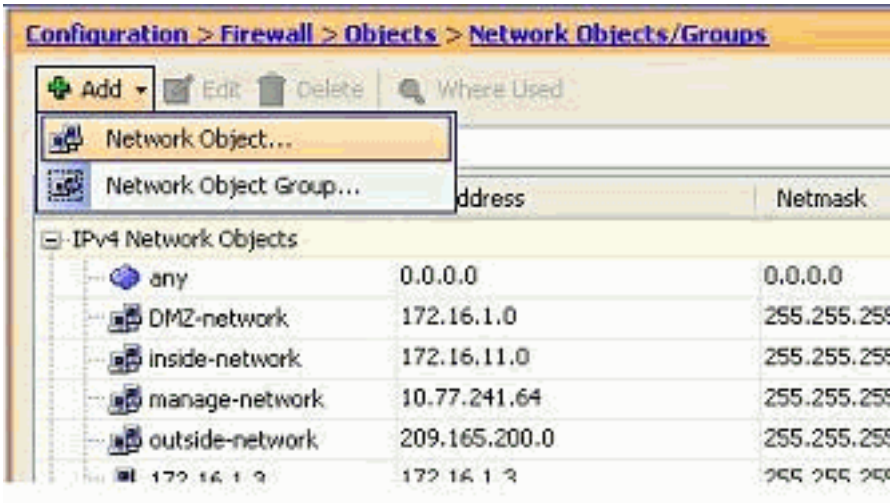


[Source]/[Destination] フィールドを編集して、ネットワーク オブジェクト グループを作成する：

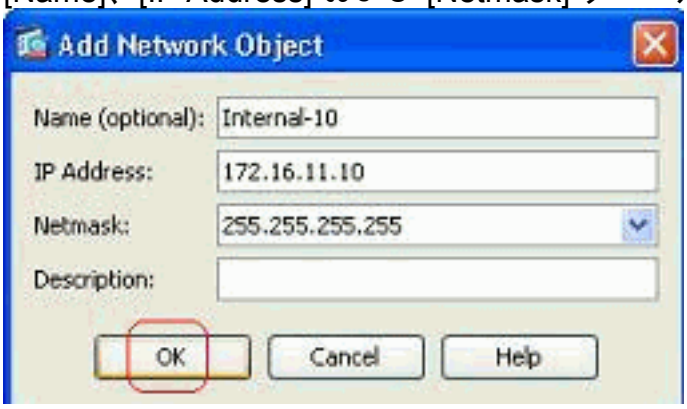
オブジェクト グループを使用すると、アクセス リストの作成およびメンテナンスが簡単になります。 類似オブジェクトをグループにまとめると、オブジェクトごとに ACE を入力する代わりに、ACE でオブジェクト グループを使用できるようになります。 オブジェクト グループを作成する前に、オブジェクトを作成する必要があります。 ASDM 用語では、オブジェクトは、ネットワーク オブジェクトと呼ばれ、オブジェクト グループは、ネットワーク オブジェクト グループと呼ばれます。

次の手順を実行します。

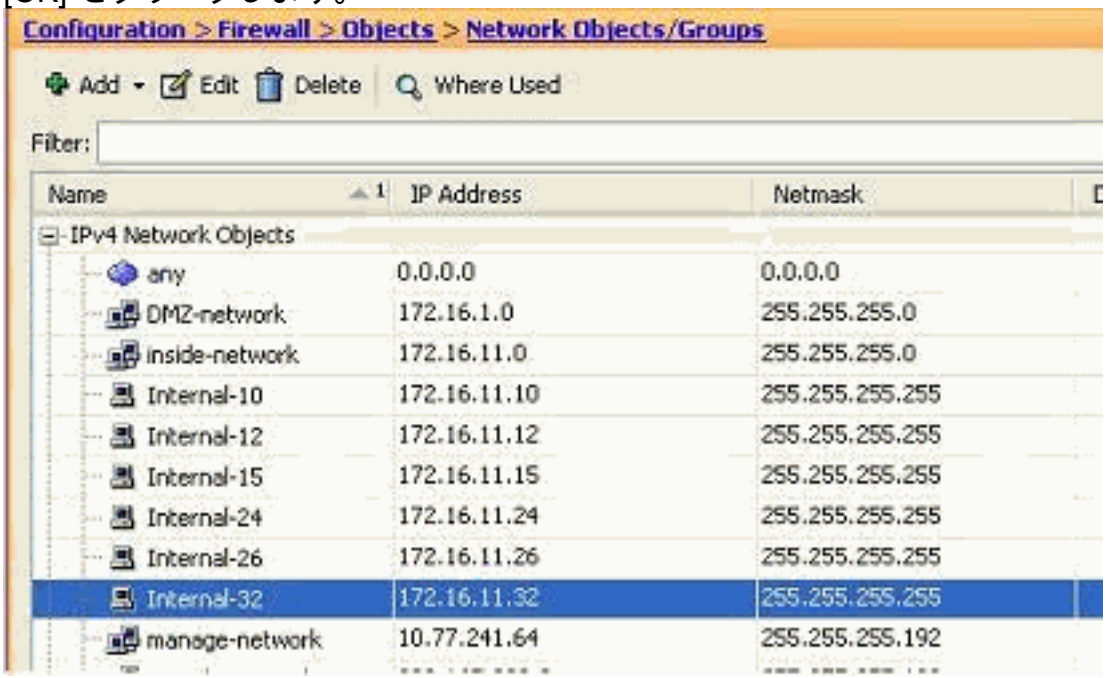
1. [Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] > [Add] を選択し、[Network Object] をクリックして、新しいネットワーク オブジェクトを作成します。



2. [Name]、[IP Address] および [Netmask] フィールドに入力して、[OK] をクリックします。

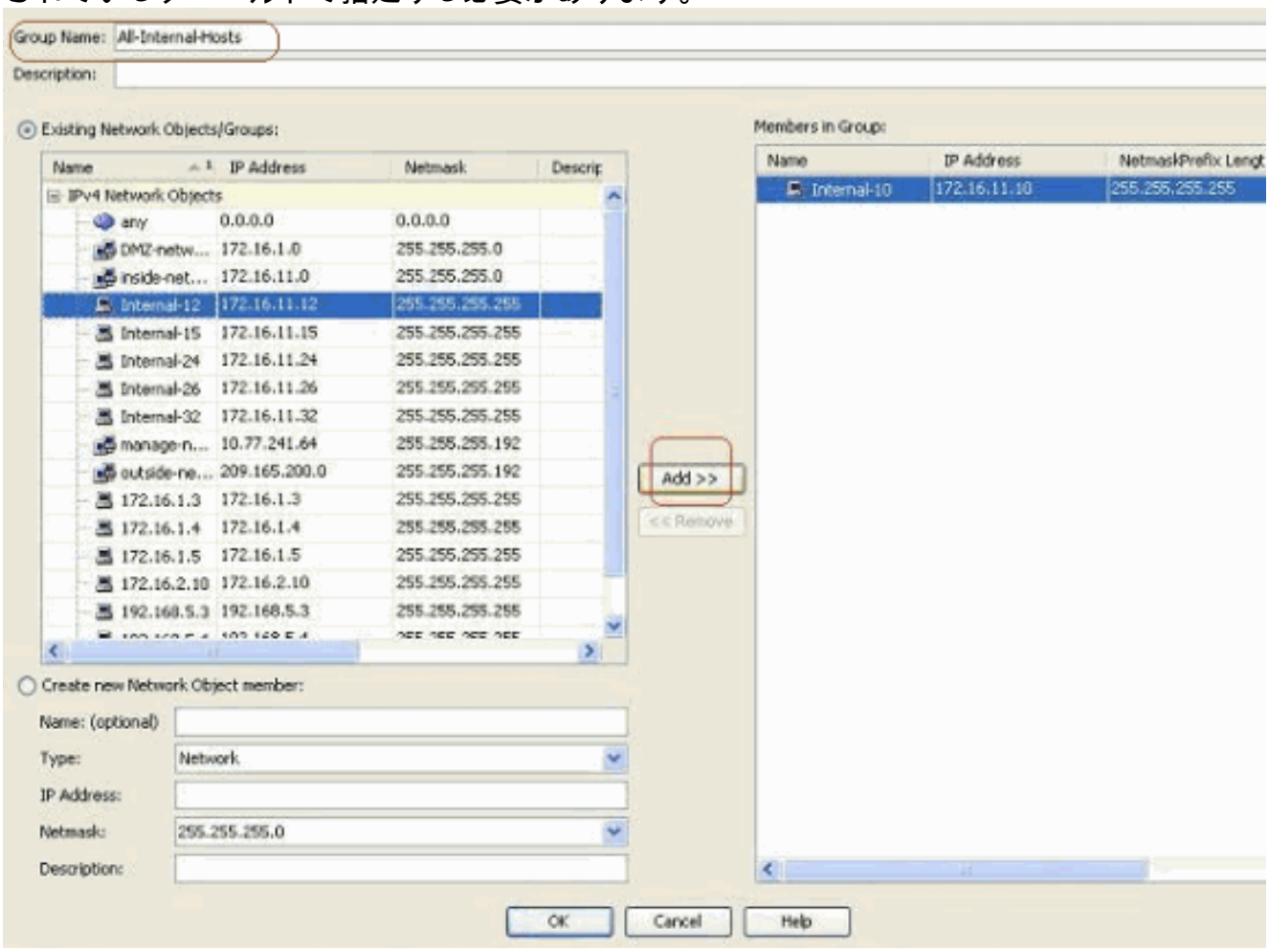


3. 新しく作成したネットワーク オブジェクトが、オブジェクトのリストに表示されます。[OK] をクリックします。

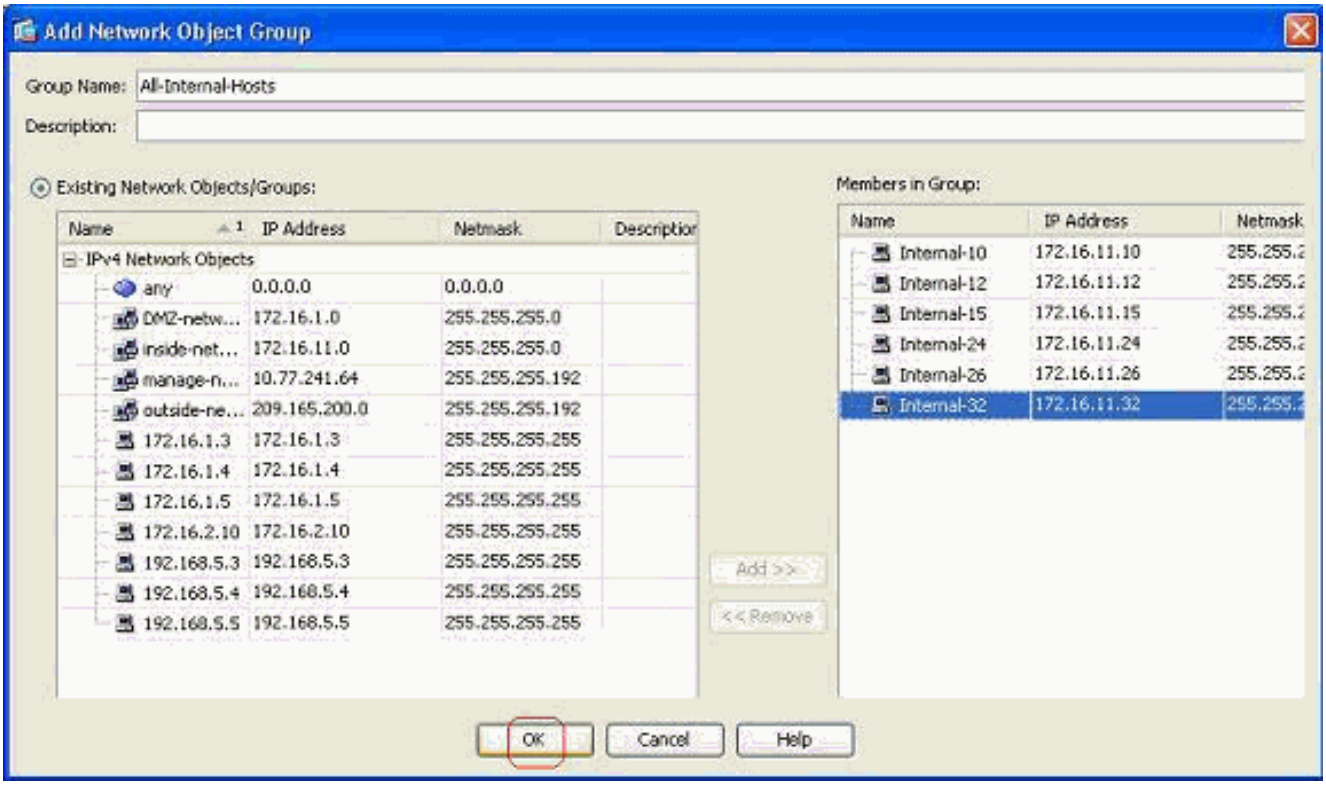


4. [Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] > [Add] を選択し、[Network Object Group] をクリックして、新しいネットワーク オブジェクトを作成します。

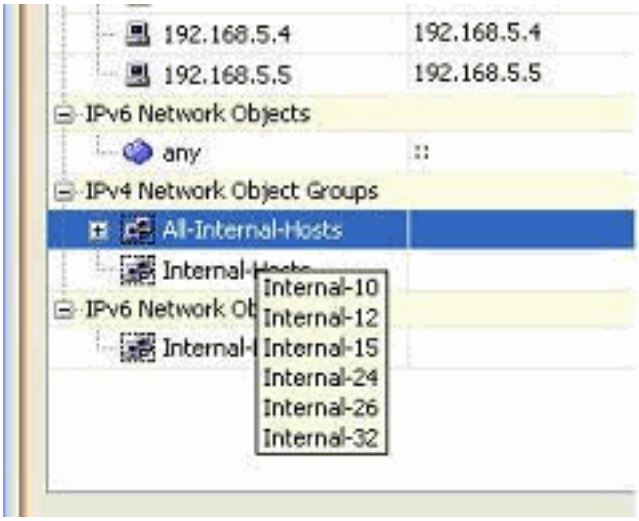
5. すべてのネットワーク オブジェクトの使用可能リストは、ウィンドウの左ペインに表示されます。 個々のネットワーク オブジェクトを選択し、[Add] ボタンをクリックして、新しく作成したネットワーク オブジェクト グループのメンバにします。 グループ名は、割り当てられているフィールドで指定する必要があります。



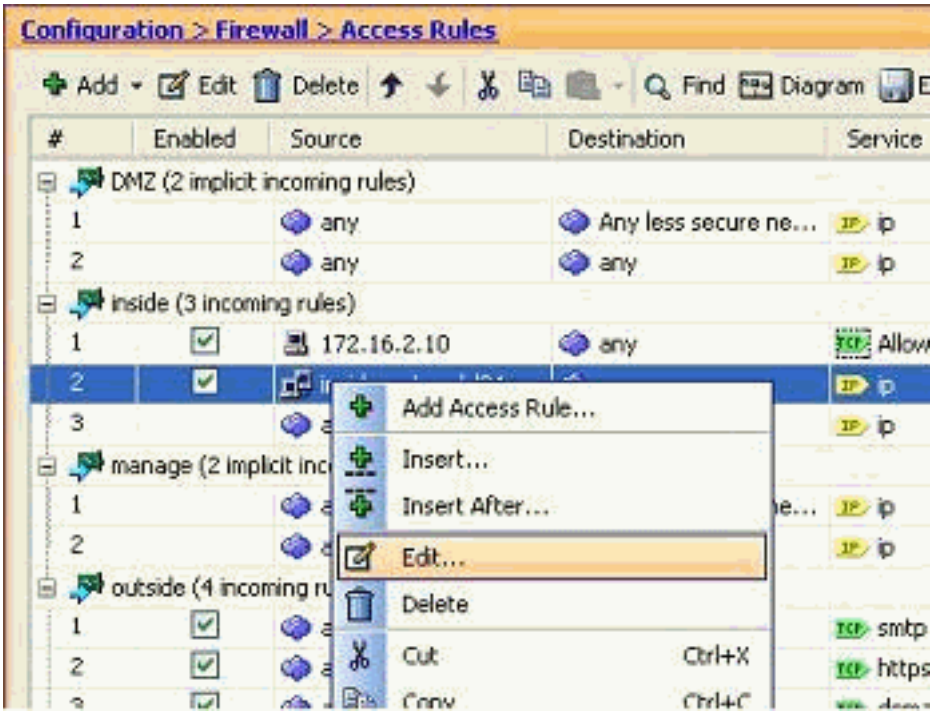
6. すべてのメンバをグループに追加したら、[OK] をクリックします。



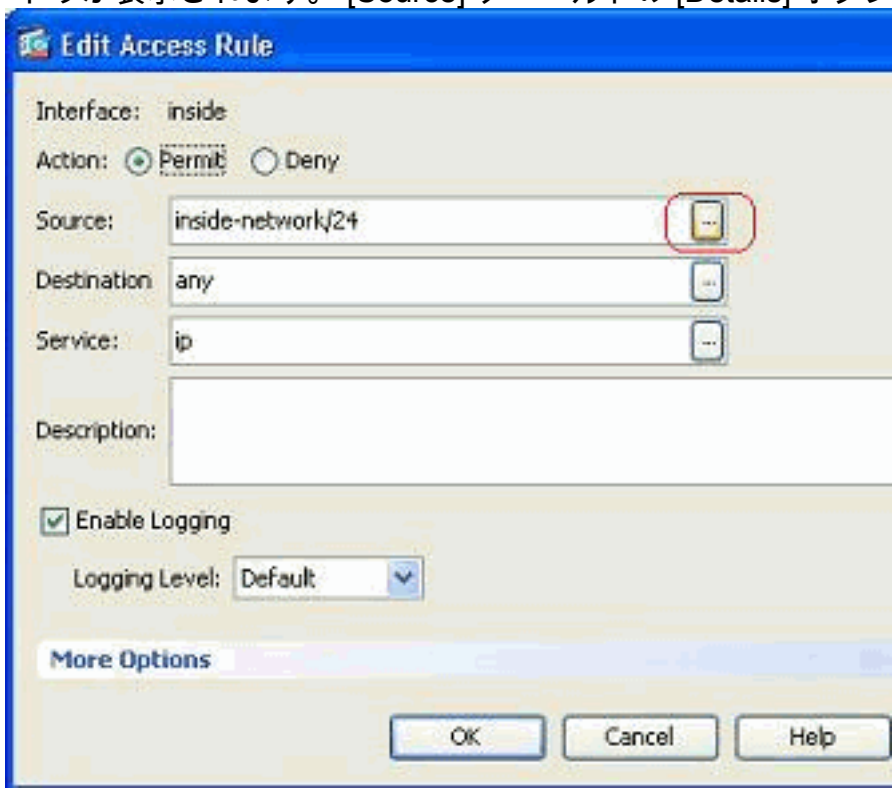
これで、ネットワーク オブジェクト グループを表示できます。



7. ネットワーク グループ オブジェクトで既存のアクセス リストの任意の送信元または宛先フィールドを変更するには、特定のアクセス ルールを右クリックして、[Edit] を選択します。

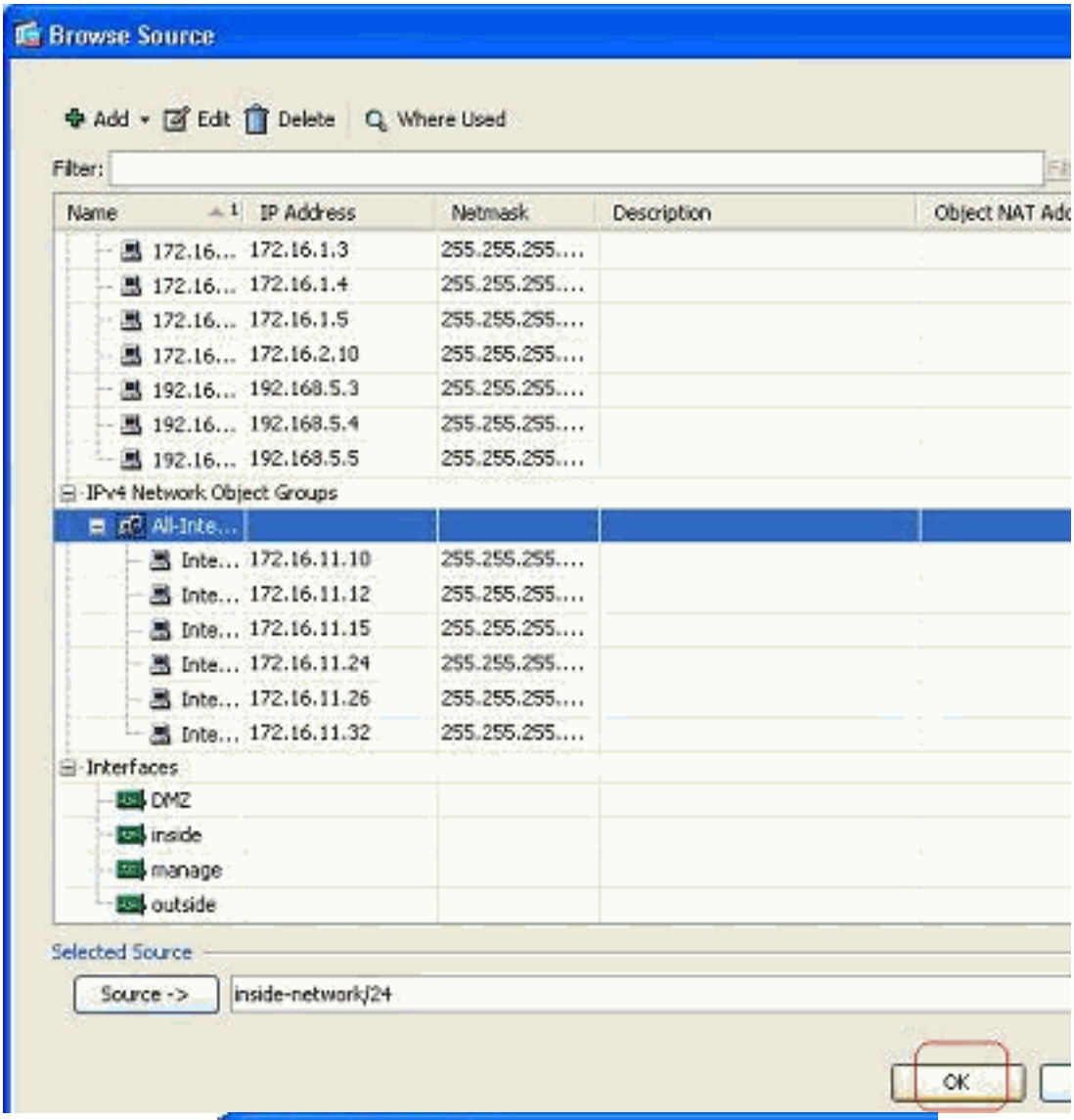


8. [Edit Access Rule] ウィンドウが表示されます。 [Source] フィールドの [Details] ボタンをクリックして変更します。

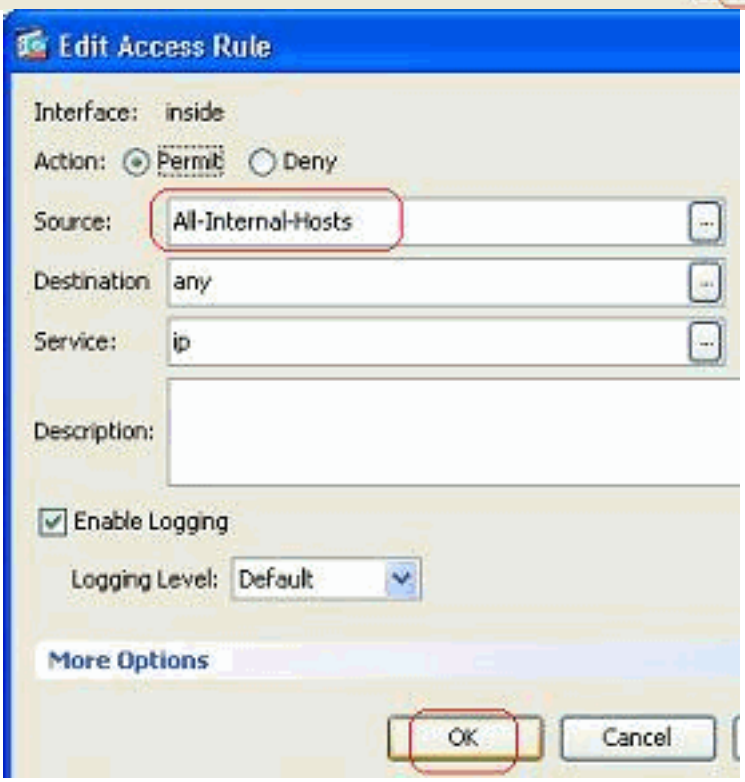


9. [All-Internal-Hosts] ネットワーク オブジェクト グループを選択して、[OK] ボタンをクリッ

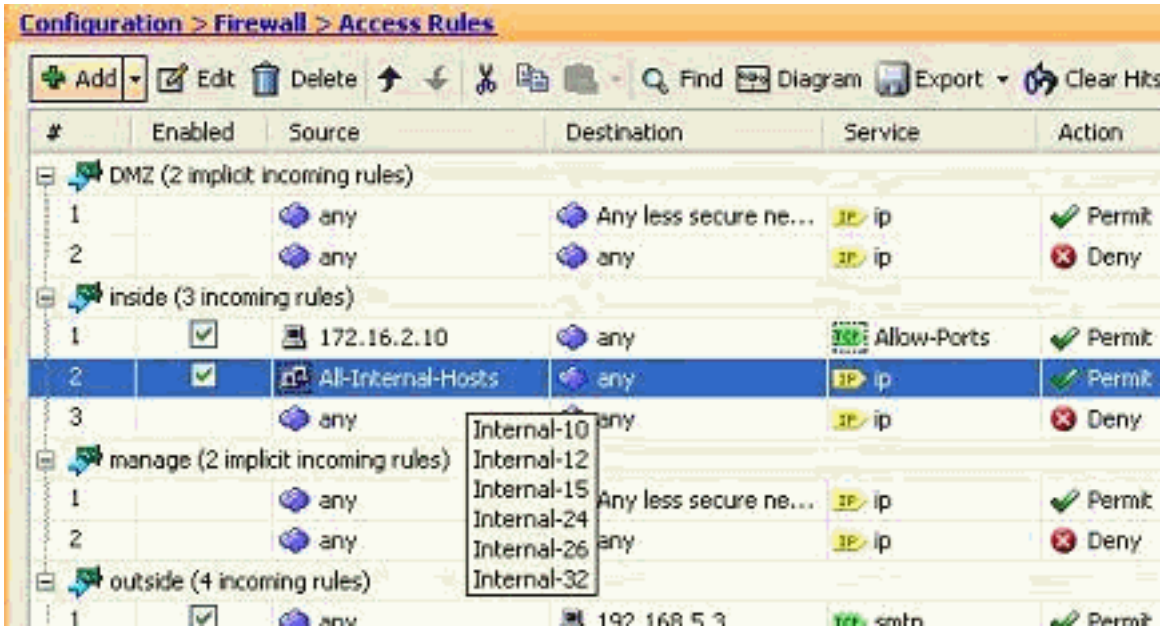
クします。



10. [OK] をクリックします。



11. アクセス ルールの [Source] フィールドにマウスを合わせ、グループのメンバを表示します

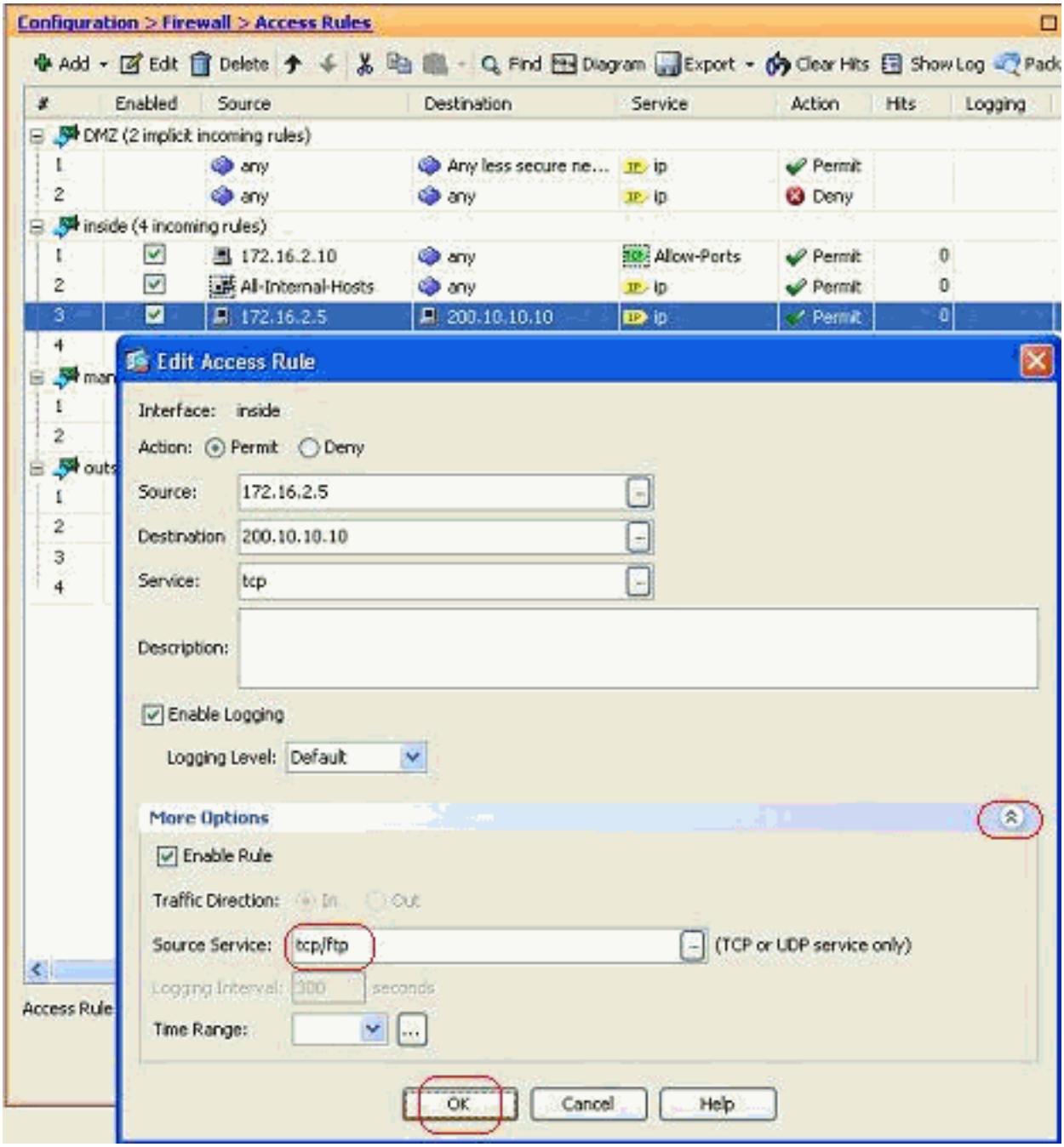


。

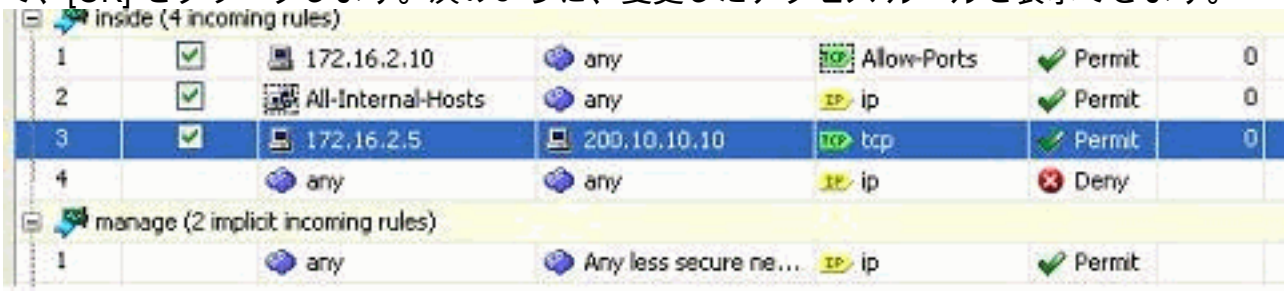
送信元ポートを編集する：

アクセス ルールの送信元ポートを変更するには、次の手順を実行します。

1. 既存のアクセス ルールの送信元ポートを変更するには、右クリックして、[Edit] を選択します。[Edit Access Rule] ウィンドウが表示されます。



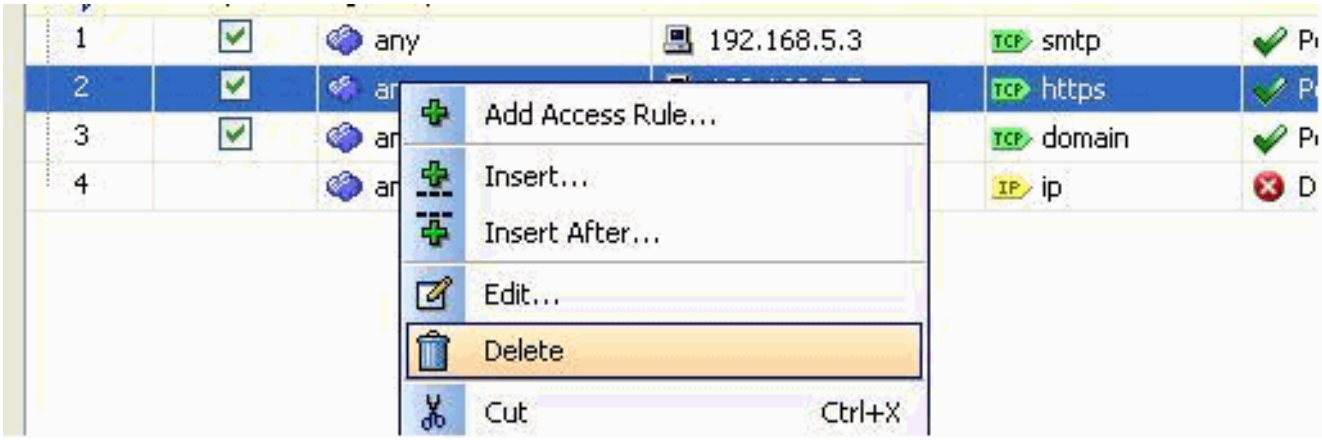
2. [More Options] ドロップダウン ボタンをクリックし、[Source Service] フィールドを変更して、[OK] をクリックします。次のように、変更したアクセス ルールを表示できます。



アクセス リストの削除

アクセス リストを削除するには、次の手順を実行します。

1. 既存のアクセス リストを削除する前に、アクセス リスト エントリ（アクセス ルール）を削除する必要があります。 すべてのアクセス ルールを削除しないと、アクセス リストを削除できません。削除するアクセス ルールを右クリックして、[Delete] を選択します。



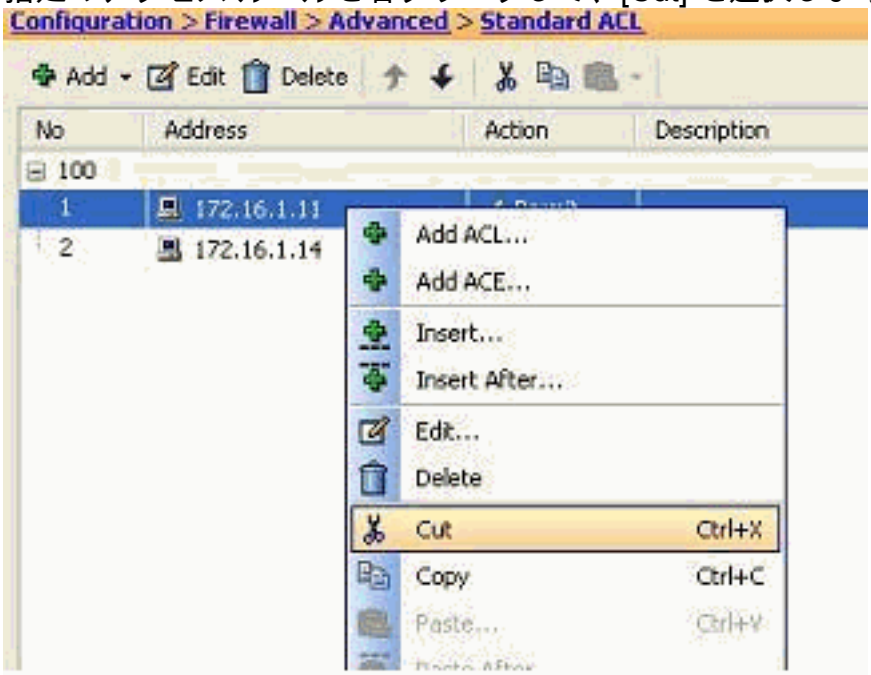
2. 既存のすべてのアクセス ルールで同じ削除操作を実行し、アクセス リストを選択して、[Delete] を選択して削除します。

アクセス ルールのエクスポート

ASDM アクセス ルールでは、アクセス リストと個々のインターフェイスがバインドされますが、ACL Manager では、すべての拡張アクセス リストが追跡されます。 ACL Manager により作成されるアクセス ルールは、インターフェイスにバインドされません。 これらのアクセス リストは、通常、インターフェイスとは関連のない NAT-Exempt、VPN-Filter およびその他の同様機能のために使用されます。 ACL Manager には、[Configuration] > [Firewall] > [Access Rules] セクションのすべてのエントリが含まれます。 また、ACL Manager には、インターフェイスとは関連のないグローバル アクセス ルールも含まれます。 ASDM では、アクセス ルールをアクセス リスト間で簡単にエクスポートできます。

たとえば、すでにグローバル アクセス ルールに含まれるアクセス ルールをインターフェイスと関連付ける必要がある場合、このように再設定する必要はありません。 ただし、[Cut] & [Paste] 操作を実行して実行できます。

1. 指定のアクセス ルールを右クリックして、[Cut] を選択します。



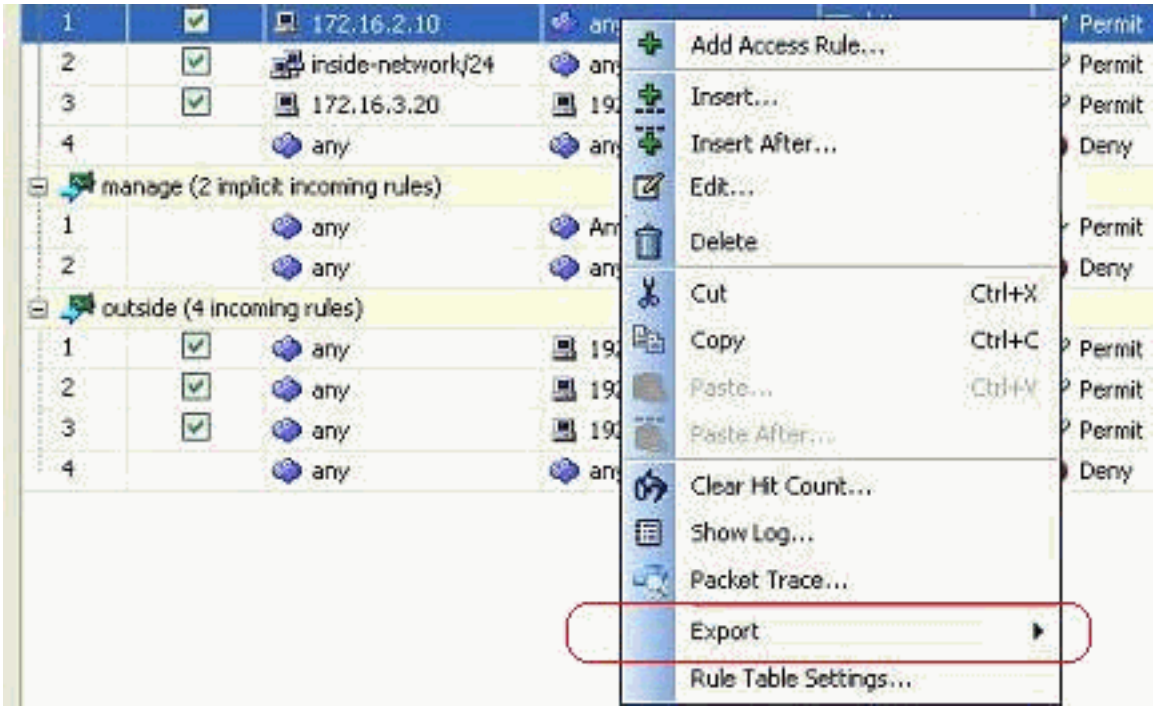
2. このアクセス ルールを挿入する必要があるアクセス リストを選択します。 ツール バーの [Paste] を使用して、アクセス ルールを挿入します。

アクセス リスト情報のエクスポート

アクセス リスト情報は、別のファイルにエクスポートできます。 この情報のエクスポートには、次の 2 種類の形式がサポートされています。

1. カンマ区切り（CSV）形式
2. HTML 形式

任意のアクセス ルールを右クリックし、[Export] を選択して、アクセス リスト情報をファイルに送信します。



次に、HTML 形式のアクセス リスト情報を示します。

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- ASDM の設定例およびテクニカル ノート
- ASA の設定例およびテクニカル ノート
- テクニカルサポートとドキュメント - Cisco Systems