ASA 8.2： ASDM での nat、global、static および access-list コマンドを使用したポート リダイレクション（ フォワーディング ）

目次

概要
前提条件
要件
使用するコンポーネント
表記法
ネットワーク図
アウトバウンド アクセスの許可
NAT を使用した inside ホストから outside ネットワークへのアクセスの許可
PAT を使用した inside ホストから outside ネットワークへのアクセスの許可
inside ホストから outside ネットワークへのアクセスの制限
同じセキュリティ レベルのインターフェイス間でのトラフィックの許可
信頼できないホストから信頼できるネットワーク上のホストへのアクセスの許可
特定のホストおよびネットワークでの NAT の無効化
static を使用したポート リダイレクション（ フォワーディング ）
static を使用した TCP/UDP セッションの制限
時間ベースのアクセス リスト
関連情報

概要

このドキュメントでは、ASDM を使用した Cisco Adaptive Security Appliance（ ASA ）でのポート リダイレクションの仕組みを説明します。 ASA でのトラフィックのアクセス コントロールとトランスレーション ルールの仕組みを説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- NAT の概要
- PIX/ASA 7.X： ポート リダイレクション

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。

- Cisco 5500 シリーズ ASA バージョン 8.2
- Cisco ASDM バージョン 6.3

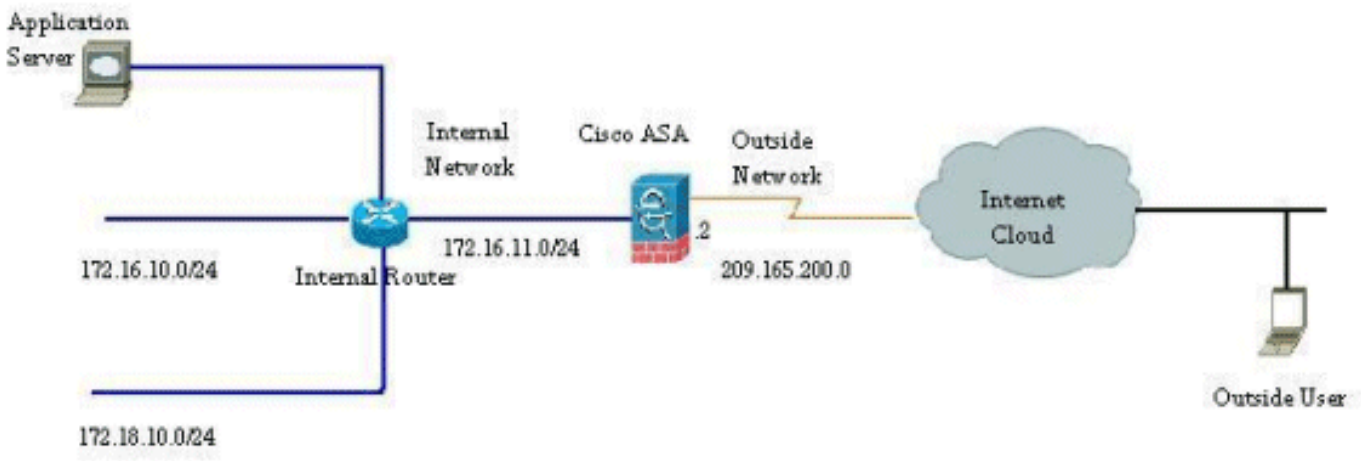
注: この構成は Cisco ASA ソフトウェア バージョン 8.0 ~ 8.2 でのみ適切に機能します。これは、NAT 機能の大幅な変更が行われていないためです。

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。

ネットワーク図

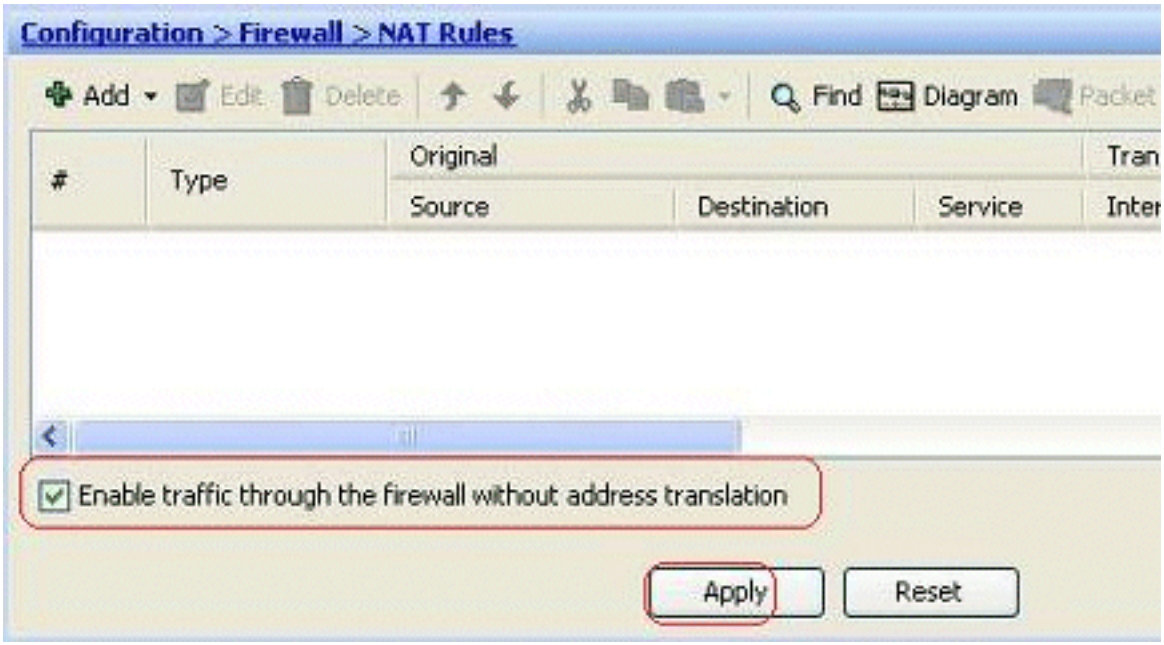


この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

アウトバウンド アクセスの許可

アウトバウンド アクセスは、セキュリティ レベルの高いインターフェイスからセキュリティ レベルの低いインターフェイスへの接続を意味します。 これには、inside から outside への接続、inside から非武装地帯（DMZ）への接続、および DMZ から outside への接続が含まれます。 発信元インターフェイスのセキュリティ レベルが宛先より高いという条件下では、ある DMZ から別の DMZ への接続もこれに含まれる可能性があります。

トランスレーション ルールが設定されていない場合、接続がセキュリティ アプライアンスを通過することはできません。 この機能は nat-control と呼ばれます。 以下に示す図に、アドレス変換を行わずに接続が ASA を経由できるようにするために ASDM でこの機能を無効にする方法を示します。 ただしトランスレーション ルールが設定されている場合、この機能を無効にする方法はすべてのトラフィックに対して有効ではないため、ネットワークをアドレス変換対象から明示的に除外する必要があります。

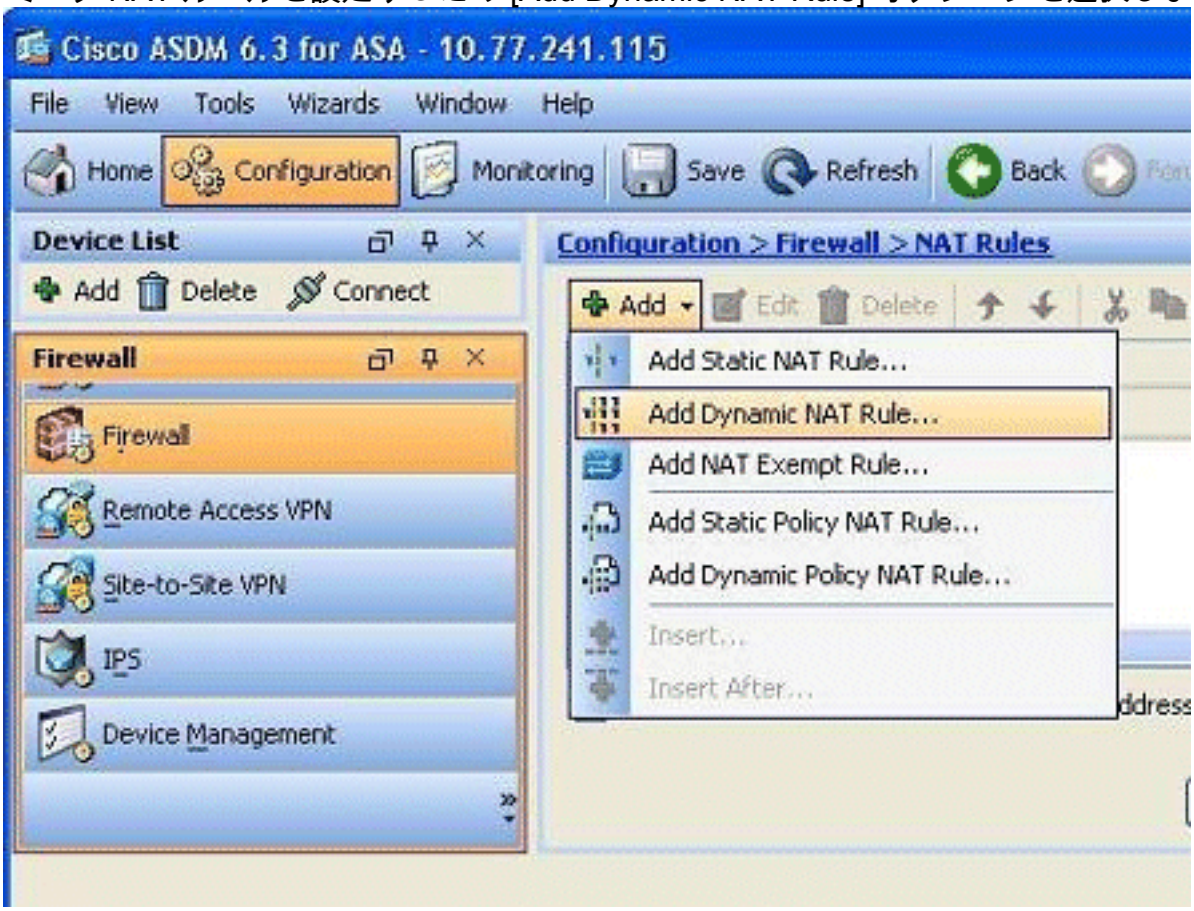


NAT を使用した inside ホストから outside ネットワークへのアクセスの許可

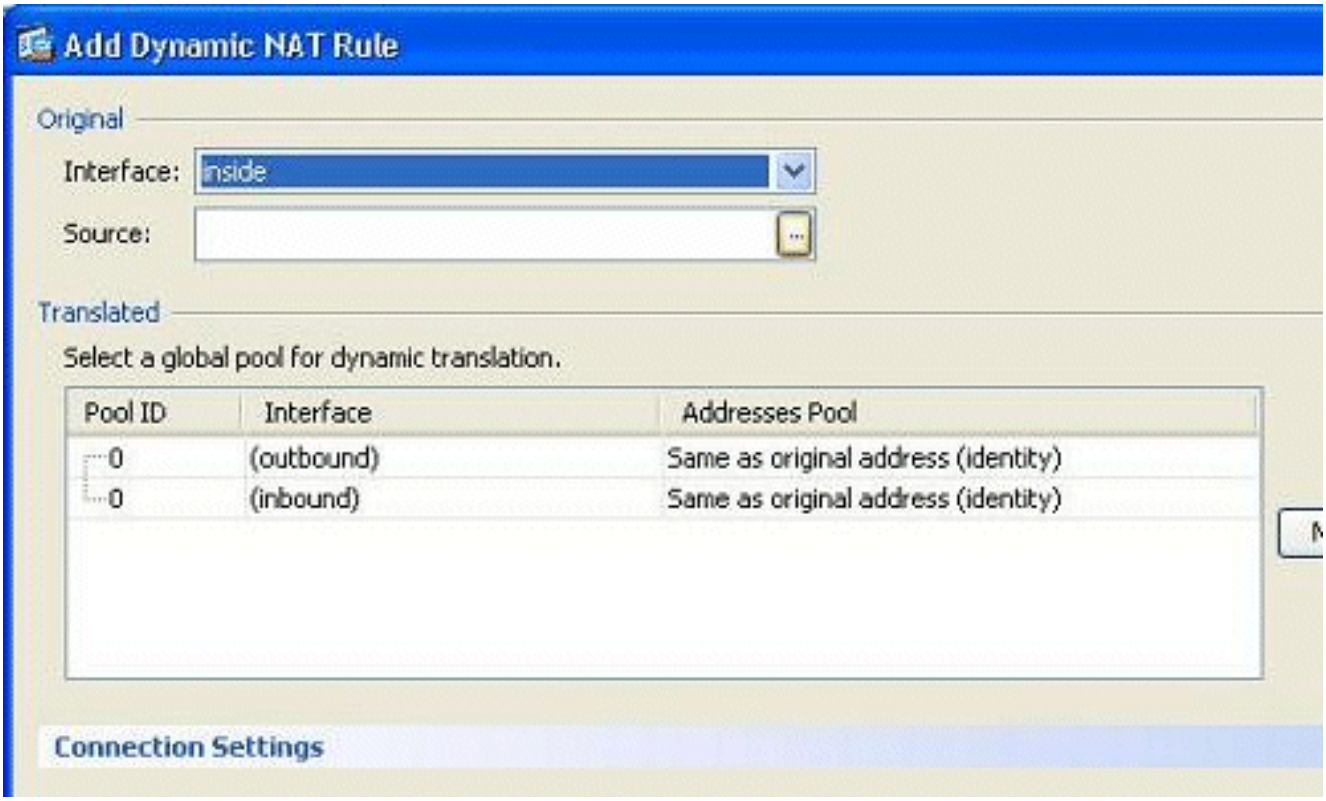
inside ホスト/ネットワークのグループに対して outside ネットワークへのアクセスを許可するには、ダイナミック NAT ルールを設定します。 このためには、アクセスを許可するホスト/ネットワークの実アドレスを選択し、変換 IP アドレスのプールにマップする必要があります。

NAT を使用して inside ホストから outside ネットワークへのアクセスを許可するには、次の手順を実行します。

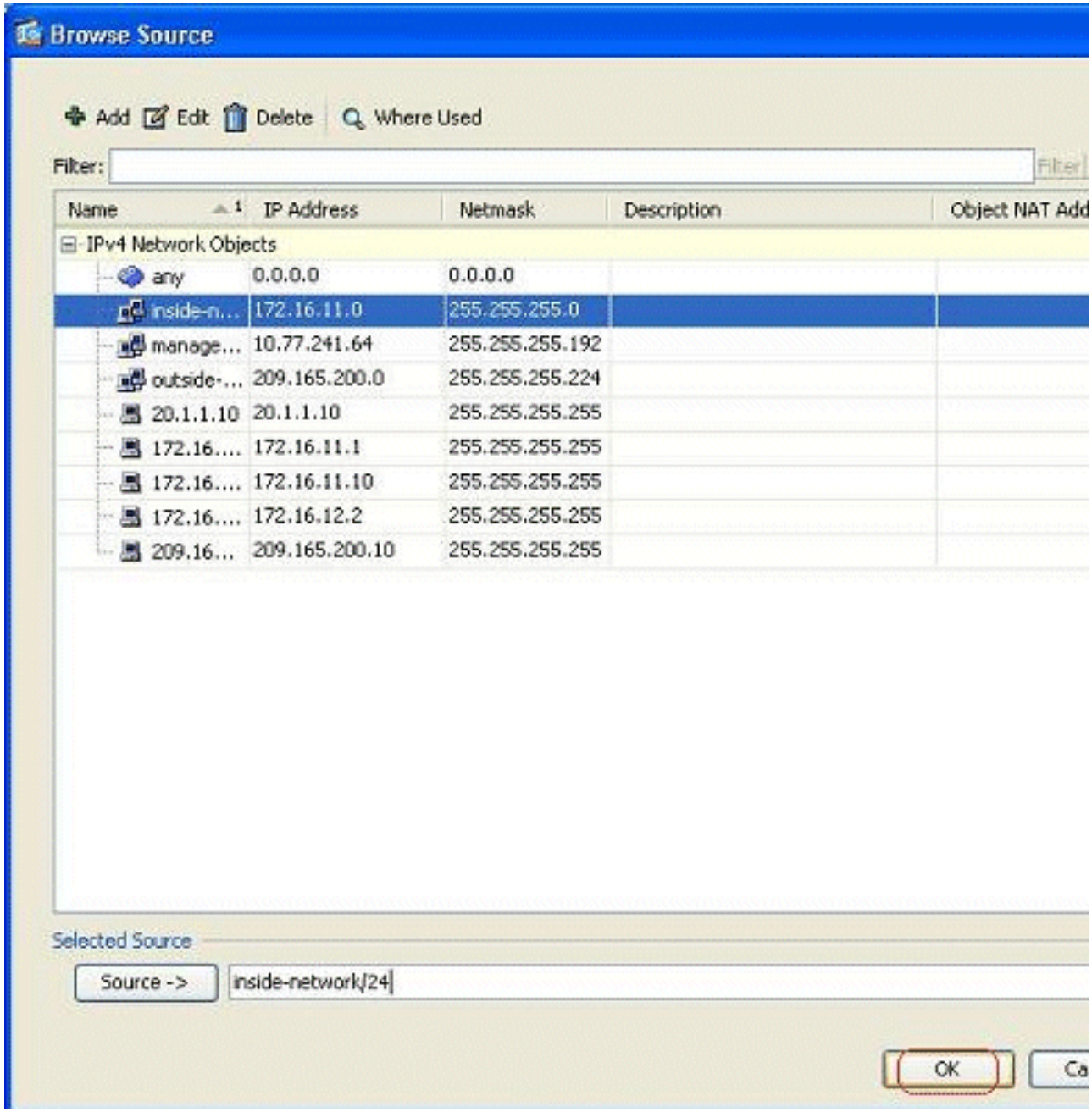
1. [Configuration] > [Firewall] > [NAT Rules] に移動して [Add] をクリックします。次にダイナミック NAT ルールを設定するため [Add Dynamic NAT Rule] オプションを選択します。



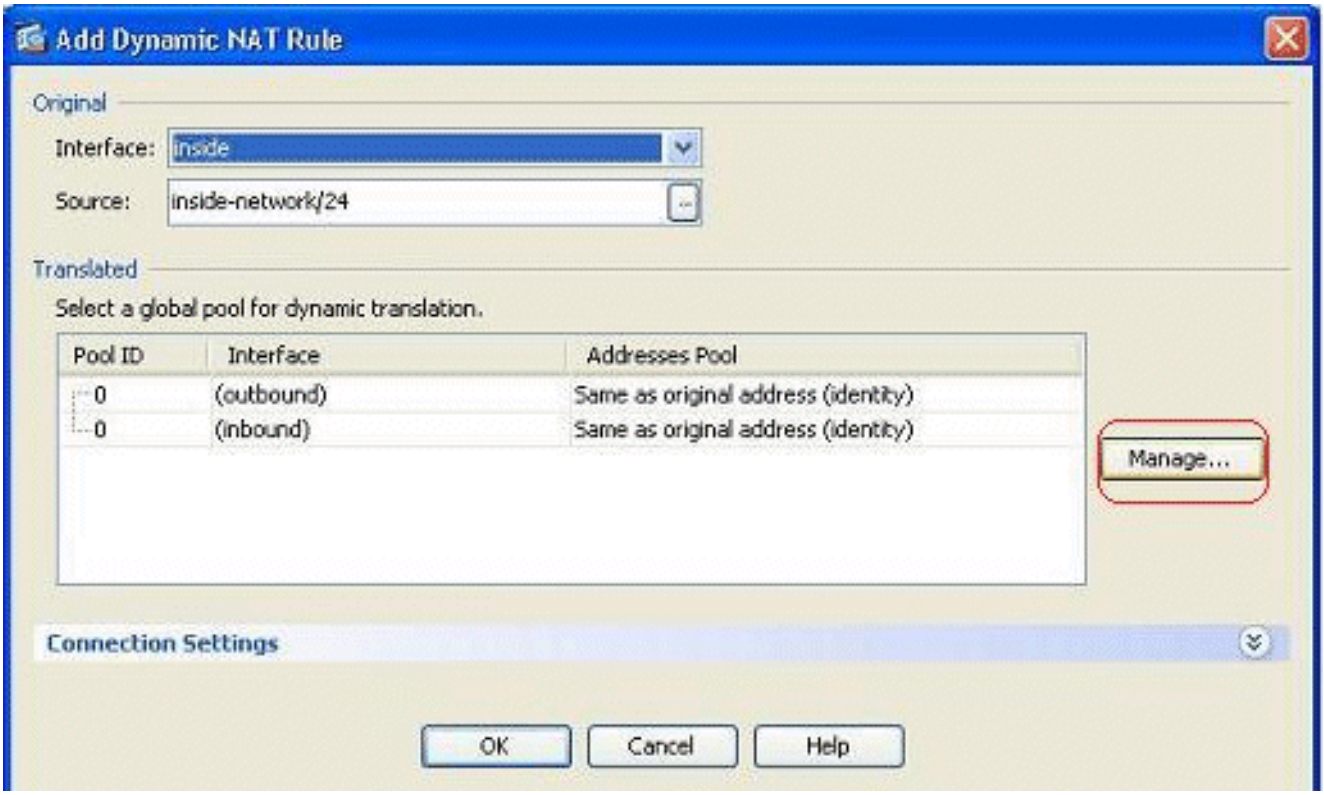
2. 実ホストの接続先インターフェイスの名前を選択します。 [Source] フィールドの [Details] ボタンを使用してホスト/ネットワークの実 IP アドレスを選択します。



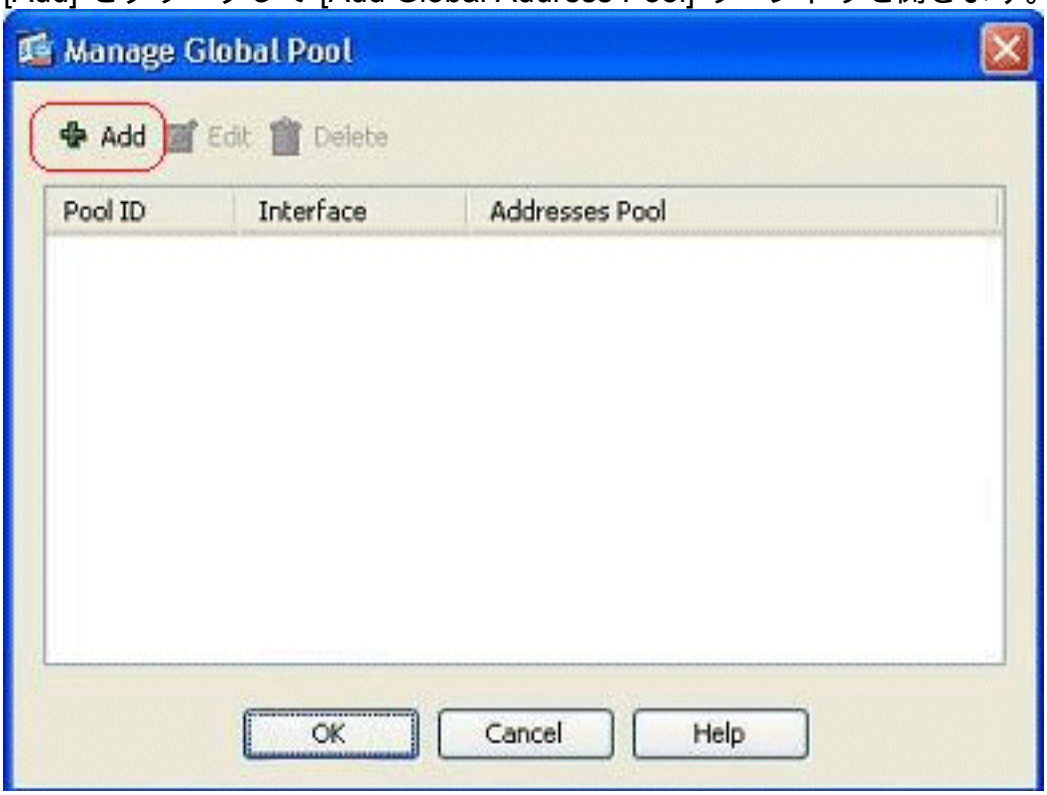
3. この例では *inside-network* 全体が選択されています。 [OK] をクリックして選択を完了します。



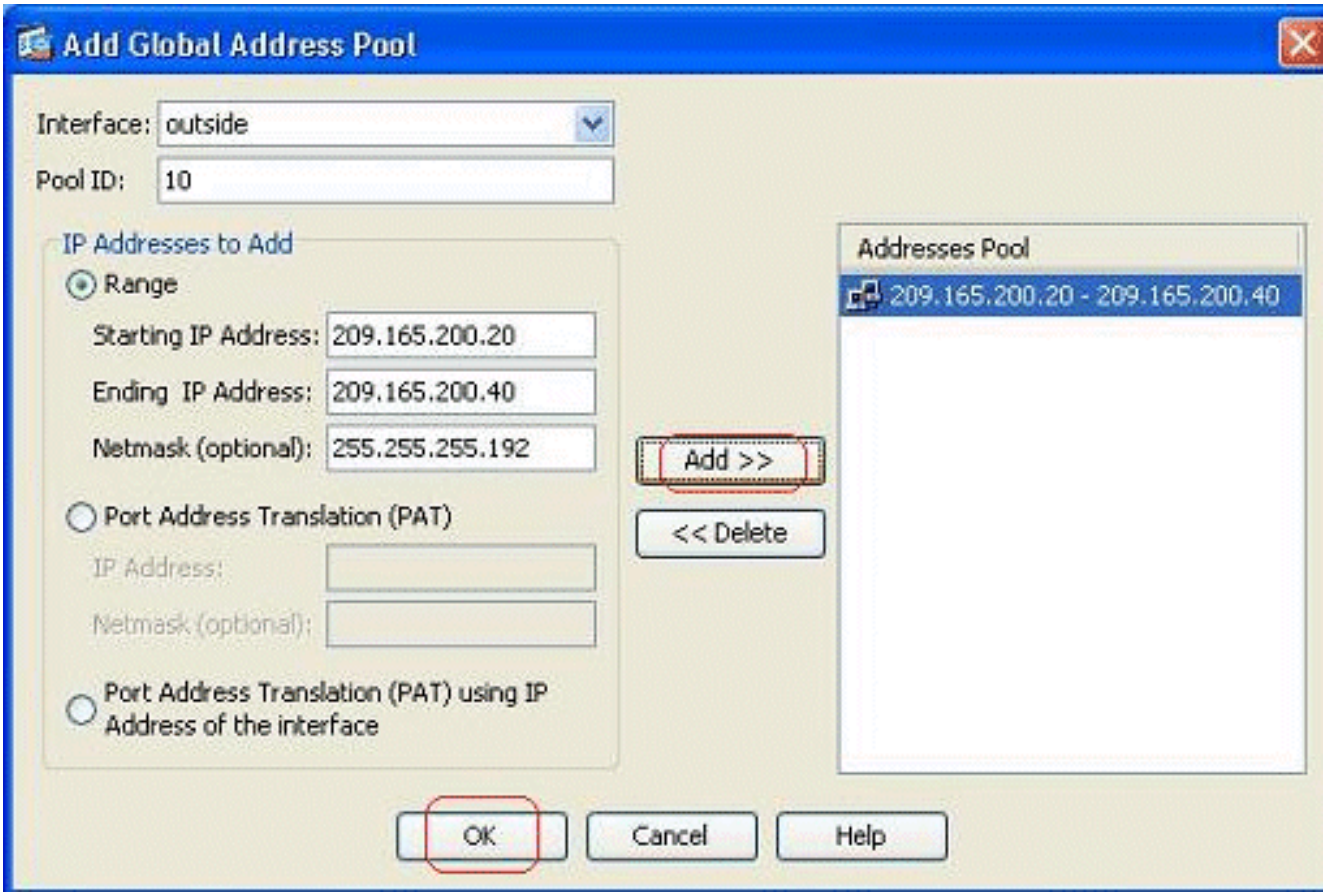
4. 実ネットワークをマップする IP アドレス プールを選択するため、[Manage] をクリックします。



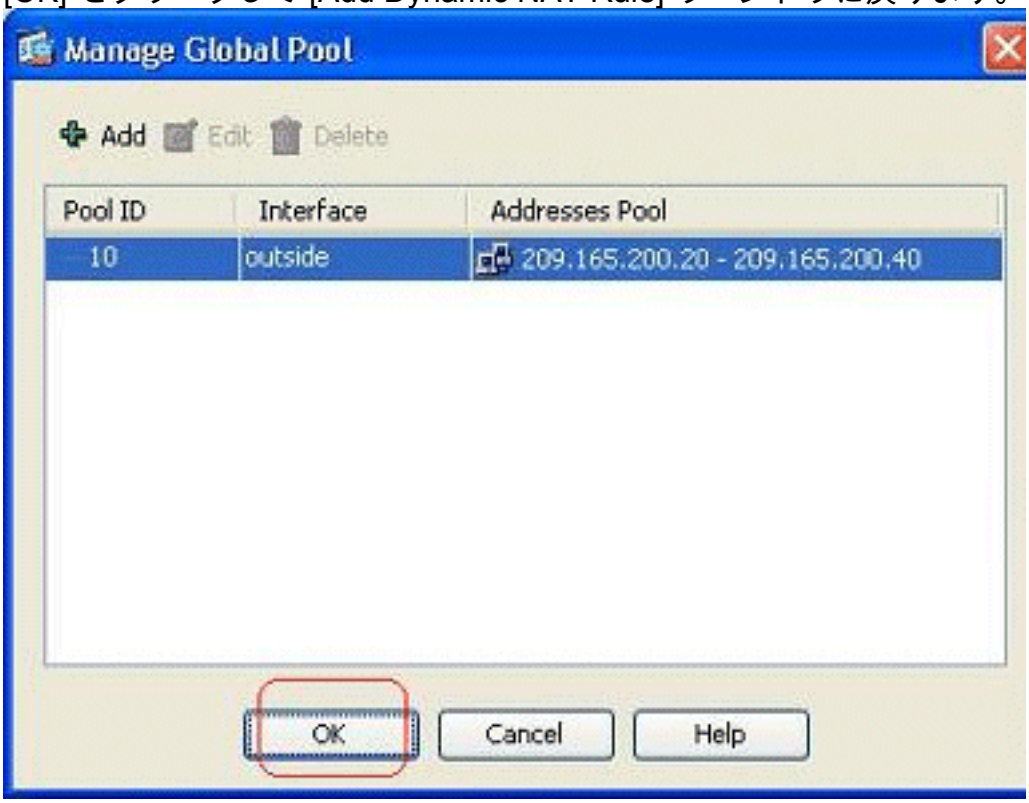
5. [Add] をクリックして [Add Global Address Pool] ウィンドウを開きます。



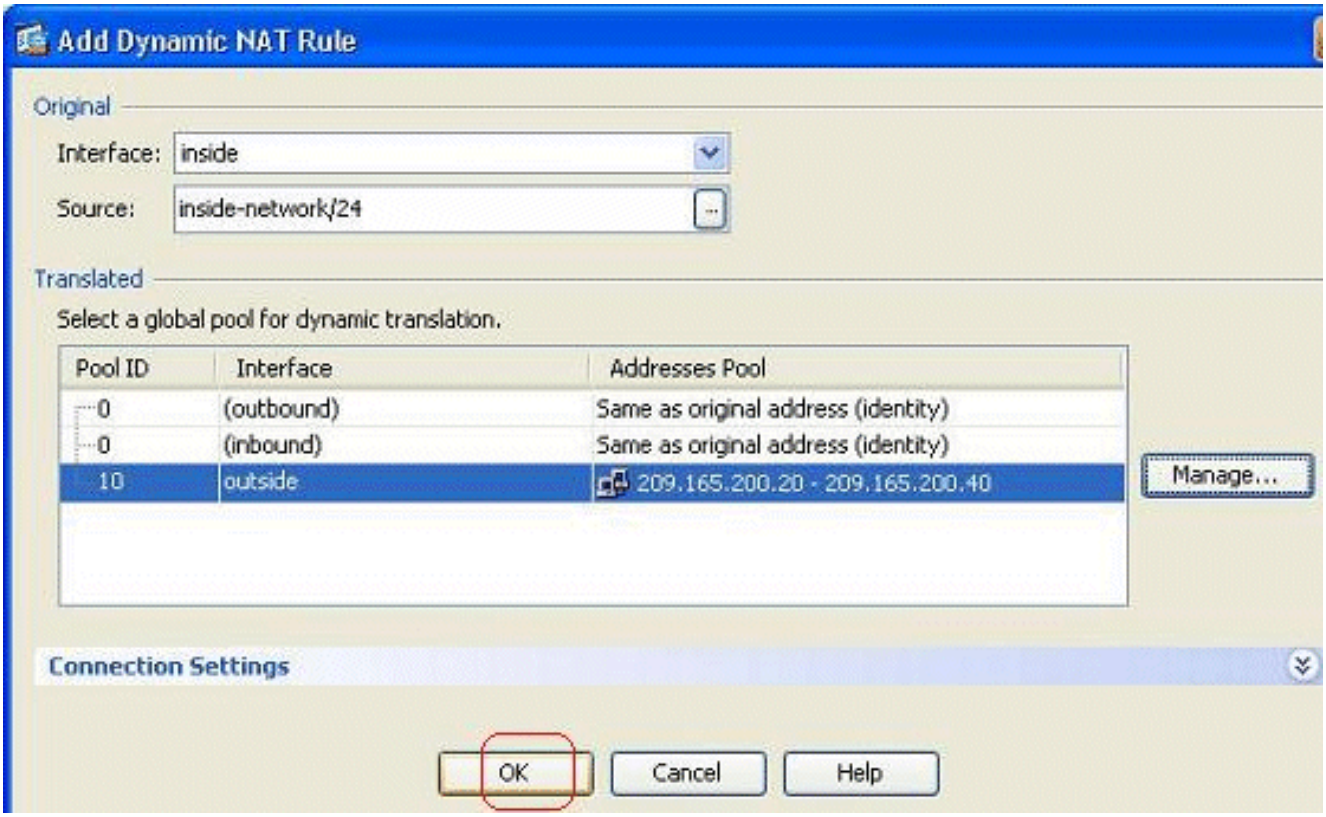
6. [Range] オプションを選択し、[Starting IP Address] と [Ending IP Address]、および egress インターフェイスを指定します。 また、アドレス プールにこれらのアドレスを追加するために、固有のプール ID を指定して [Add] をクリックします。 [OK] をクリックして [Manage Global Pool] ウィンドウに戻ります。



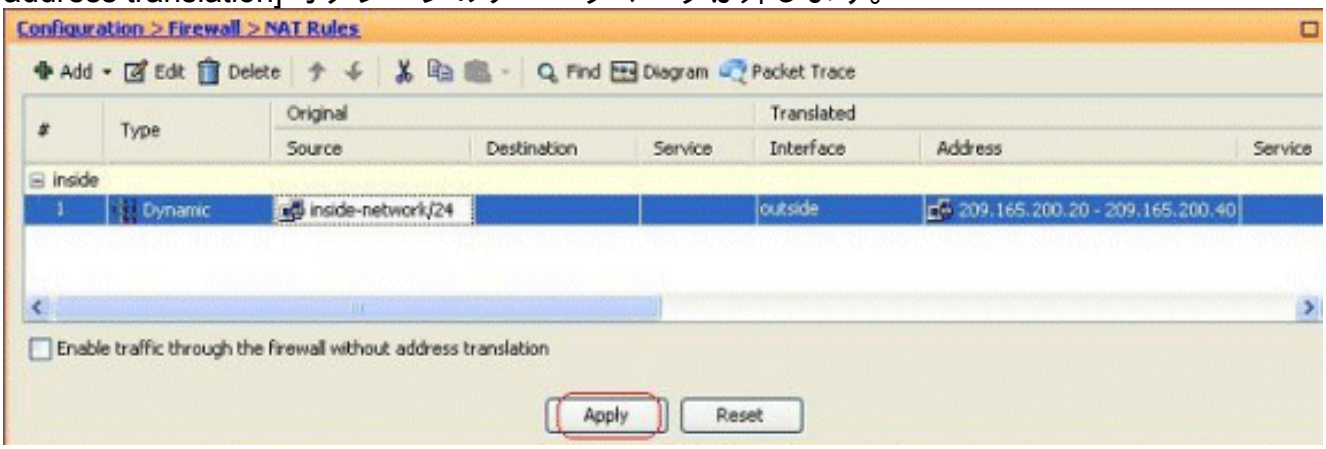
7. [OK] をクリックして [Add Dynamic NAT Rule] ウィンドウに戻ります。



8. [OK] をクリックしてダイナミック NAT ルールの設定を完了します。



9. [Apply] をクリックして変更を有効にします。**注:** [Enable traffic through the firewall without address translation] オプションのチェックマークは外します。



この ASDM 設定に対応する CLI 出力を以下に示します。

```
nat-control global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192 nat
(inside) 10 172.16.11.0 255.255.255.0
```

この設定では 172.16.11.0 ネットワークのホストは NAT プールの IP アドレス (209.165.200.20 ~ 209.165.200.40) のいずれかに変換されます。 ここでは NAT プール ID が非常に重要です。 同じ NAT プールを別の Internal/DMZ ネットワークに割り当てることができます。 マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。 その結果、PAT を実装するかまたは既存のアドレスプールを編集して拡張することになります。

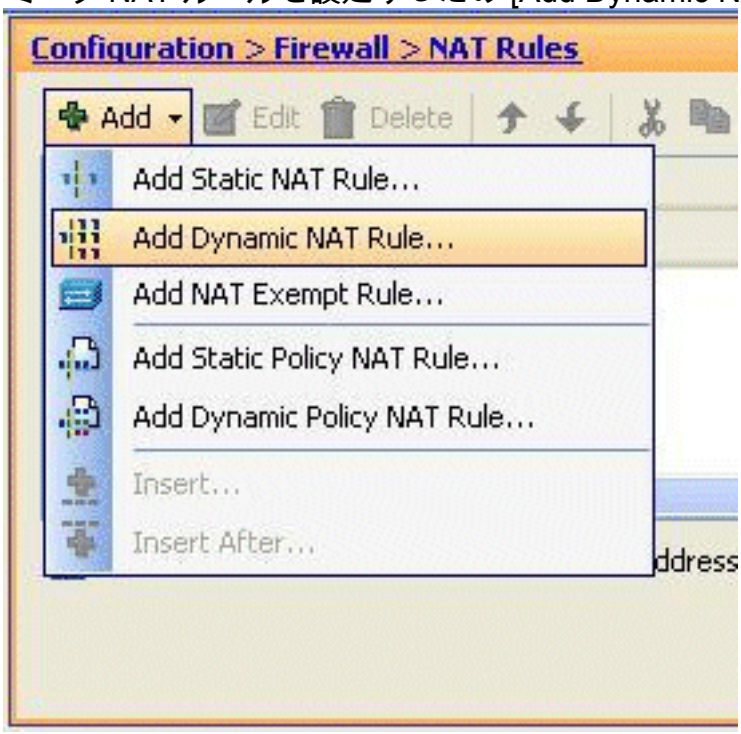
注: 既存のトランスレーション ルールを変更する場合には、変更を有効にするために clear xlate コマンドを使用する必要がある点に注意してください。 このコマンドを使用しないと、タイムアウトになるまで以前の既存の接続が接続テーブルに残ります。 **clear xlate** コマンドは既存の接続を即時に終了するため、このコマンドを使用する場合には注意してください。

PAT を使用した inside ホストから outside ネットワークへのアクセスの許可

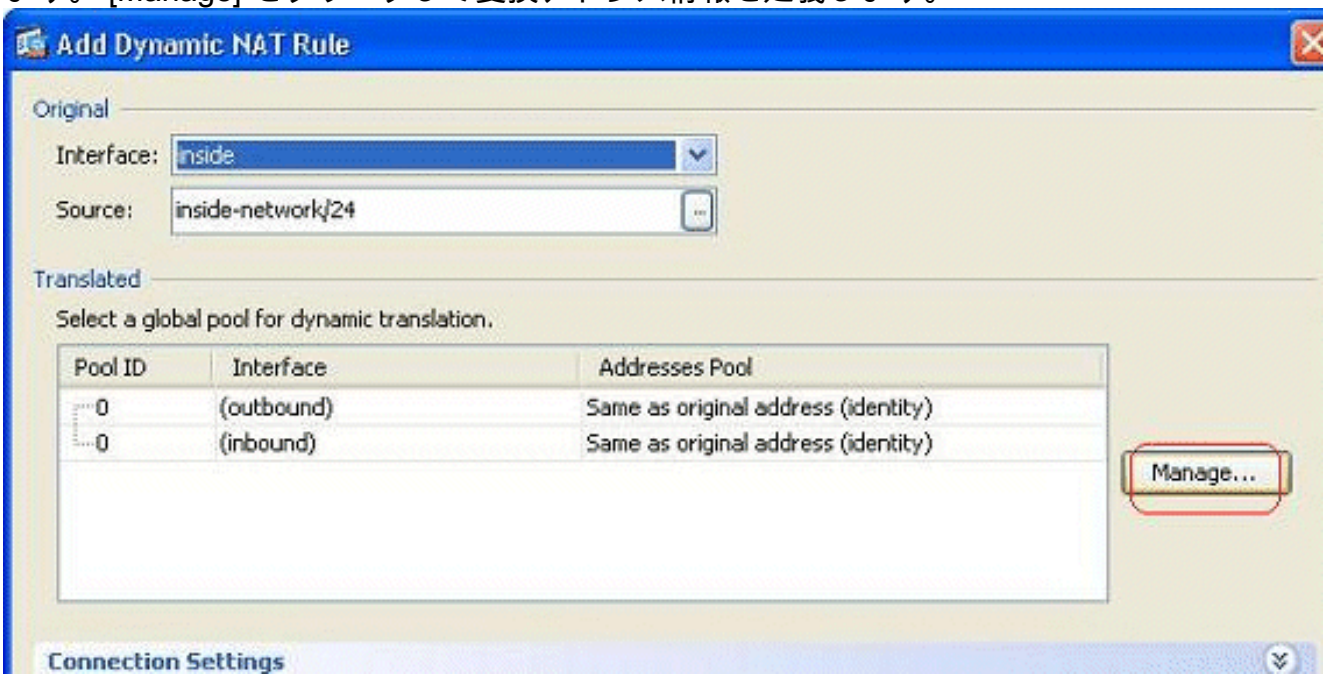
変換用に inside ホストで 1 つのパブリック アドレスを共有する場合は PAT を使用します。 **global** ステートメントに 1 つのアドレスが指定されている場合、そのアドレスはポート変換されます。 ASA ではインターフェイスごとに 1 つのポート変換が可能であり、この変換では、単一のグローバル アドレスへのアクティブな **xlate** オブジェクトが最大で 65,535 個サポートされます。

PAT を使用して inside ホストから outside ネットワークへのアクセスを許可するには、次の手順を実行します。

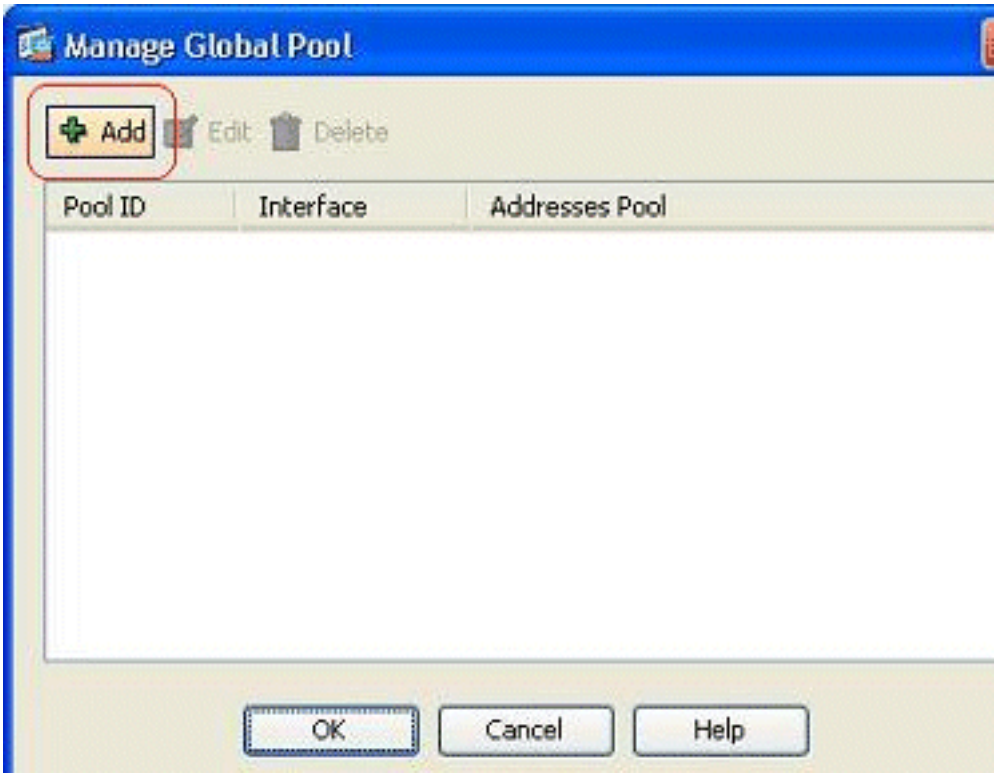
1. [Configuration] > [Firewall] > [NAT Rules] に移動して [Add] をクリックします。次にダイナミック NAT ルールを設定するため [Add Dynamic NAT Rule] オプションを選択します。



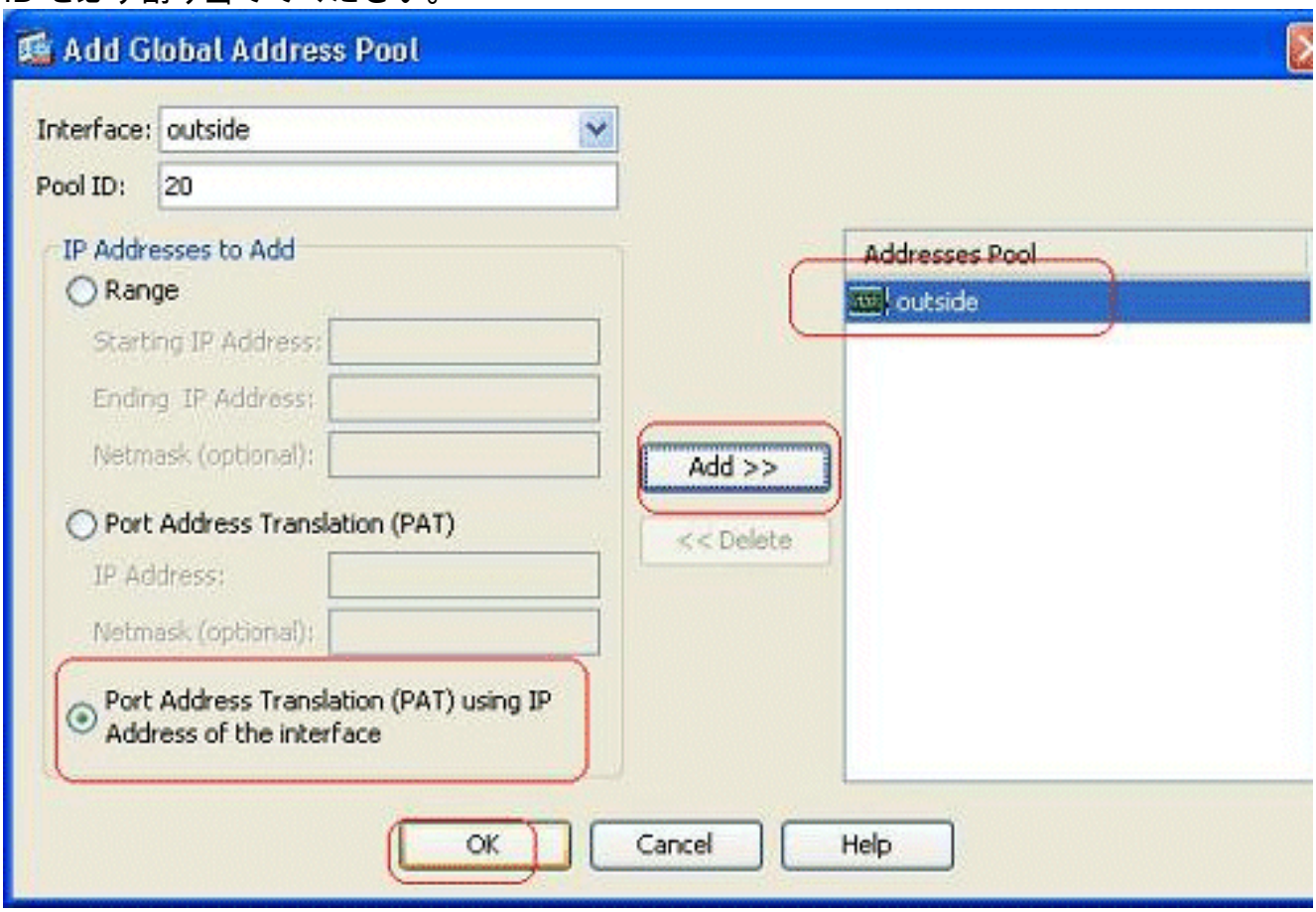
2. 実ホストの接続先インターフェイスの名前を選択します。 [Source] フィールドの [Details] ボタンを使用してホスト/ネットワークの実 IP アドレスを選択し、[inside-network] を選択します。 [Manage] をクリックして変換アドレス情報を定義します。



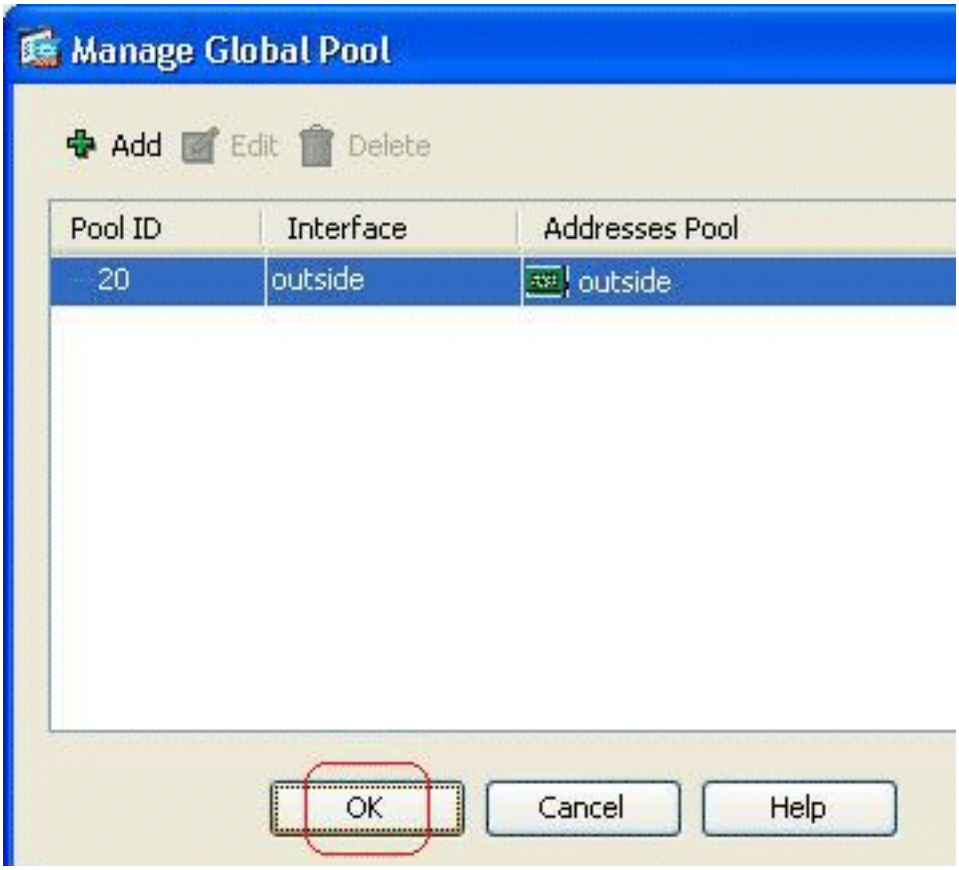
3. [Add] をクリックします。



4. [Port Address Translation (PAT) using IP address of the interface] オプションを選択し、[Add] をクリックしてアドレス プールに追加します。 この NAT アドレス プールに固有の ID を必ず割り当ててください。

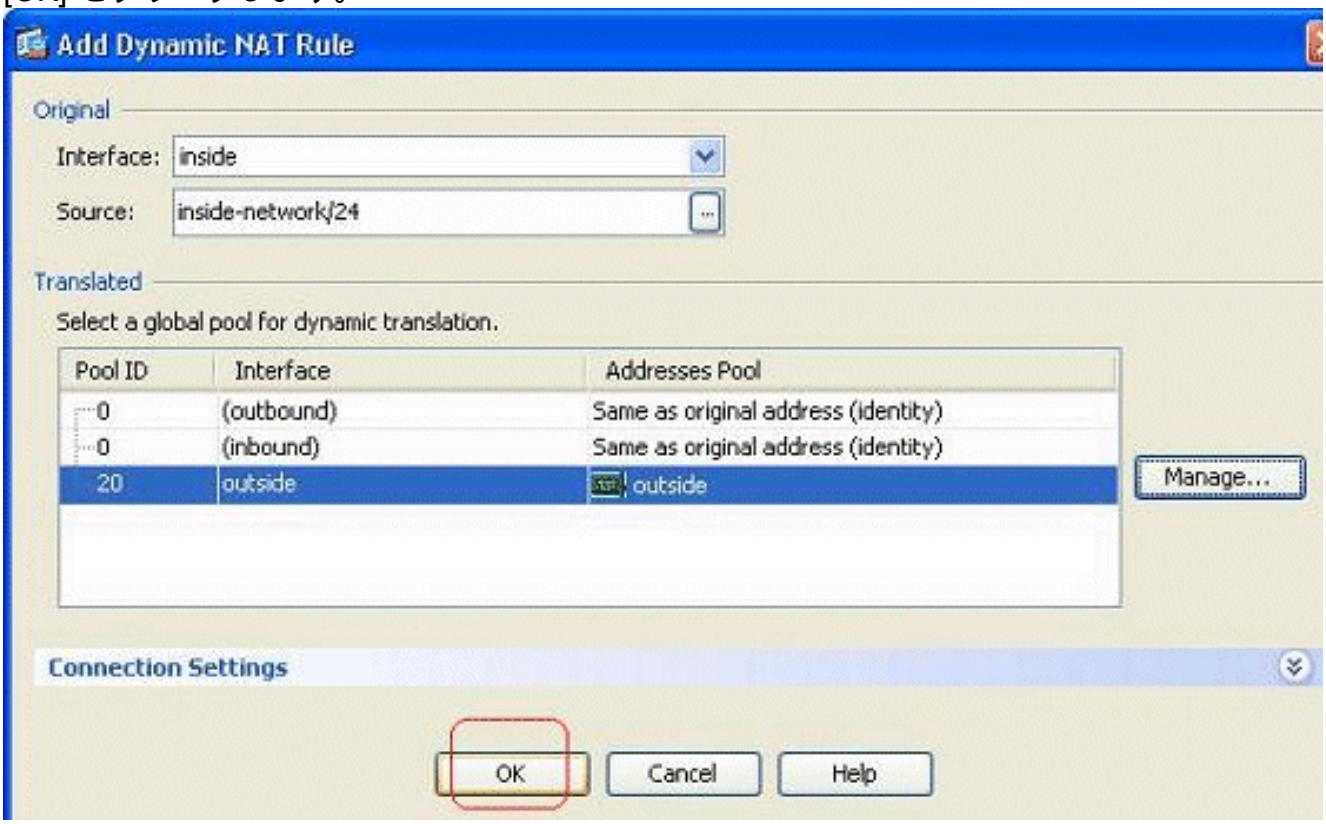


5. 設定されたアドレス プールを以下に示します。このアドレス プールでは outside インターフェイスが唯一の使用可能なアドレスです。 [OK] をクリックして [Add Dynamic NAT Rule]

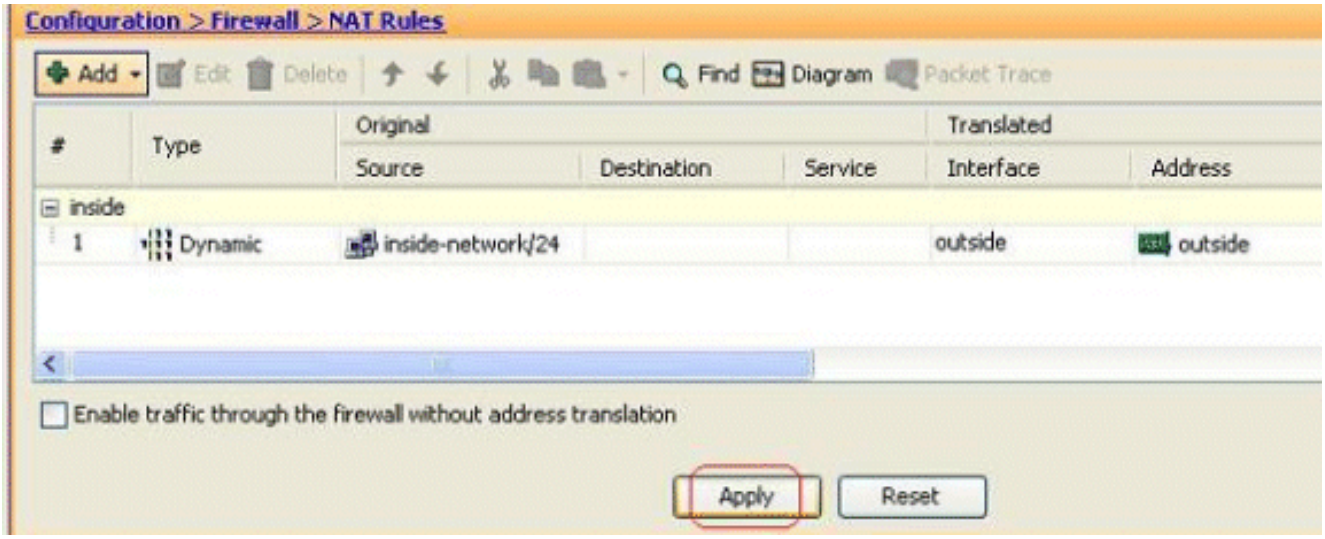


ウィンドウに戻ります。

6. [OK] をクリックします。



7. 設定されたダイナミック NAT ルールが [Configuration] > [Firewall] > [NAT Rules] ペインに表示されます。



この PAT 設定に対応する CLI 出力を以下に示します。

```
global (outside) 20 interface nat (inside) 20 172.16.11.0 255.255.255.0
```

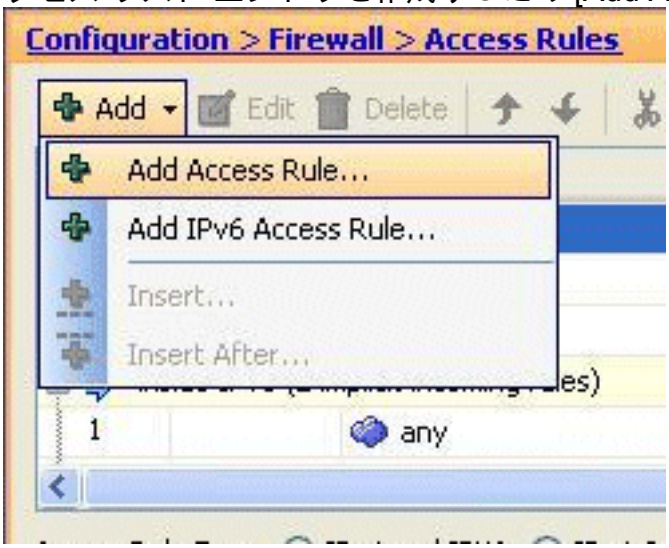
inside ホストから outside ネットワークへのアクセスの制限

アクセス ルールが定義されていない場合、セキュリティ レベルが高いインターフェイスのユーザはセキュリティ レベルが低いインターフェイスのすべてのリソースにアクセスできます。 特定のユーザに対して特定のリソースへのアクセスを制限するには、ASDM でアクセス ルールを使用します。 この例では、特定の 1 ユーザに対して外部リソース (FTP、SMTP、POP3、HTTPS、WWW) へのアクセスを許可し、その他のすべてのユーザに対してこれらの外部リソースへのアクセスを制限する方法を説明します。

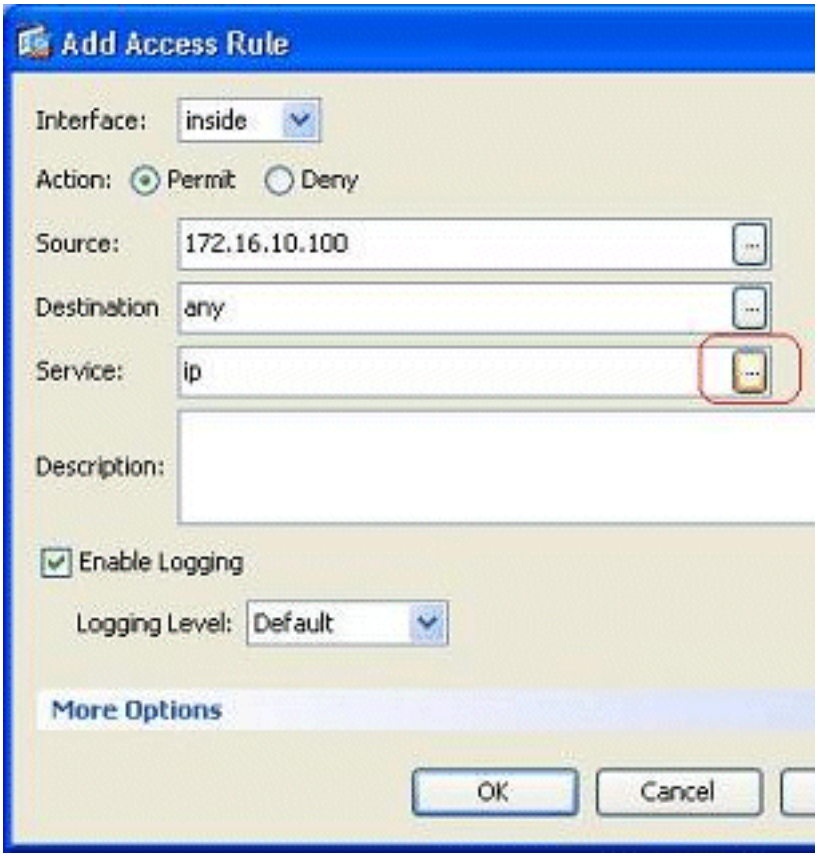
注: すべてのアクセス リストの終わりには「暗黙拒否」ルールがあります。

次の手順を実行します。

1. [Configuration] > [Firewall] > [Access Rules] に移動して [Add] をクリックします。新しいアクセス リスト エントリを作成するため [Add Access Rule] オプションを選択します。

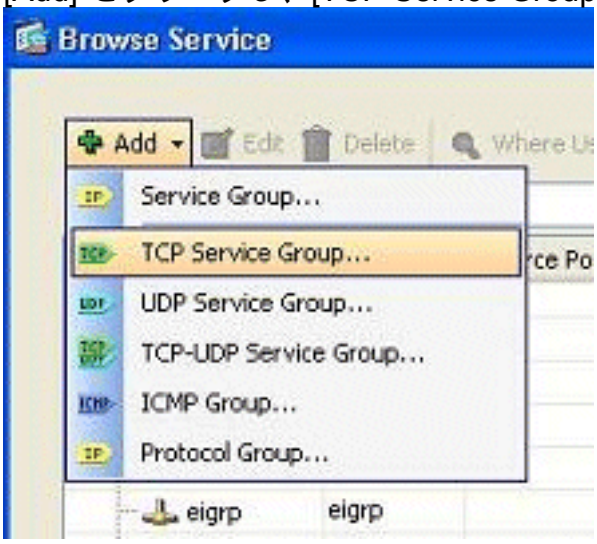


2. アクセスを許可する送信元 IP アドレスを [Source] フィールドから選択します。[Destination] で [any] を選択し、[Interface] で [inside] を選択し、[Action] で [Permit] を選択します。 最後に [Service] フィールドの [Details] ボタンをクリックし、必要なポートの TCP

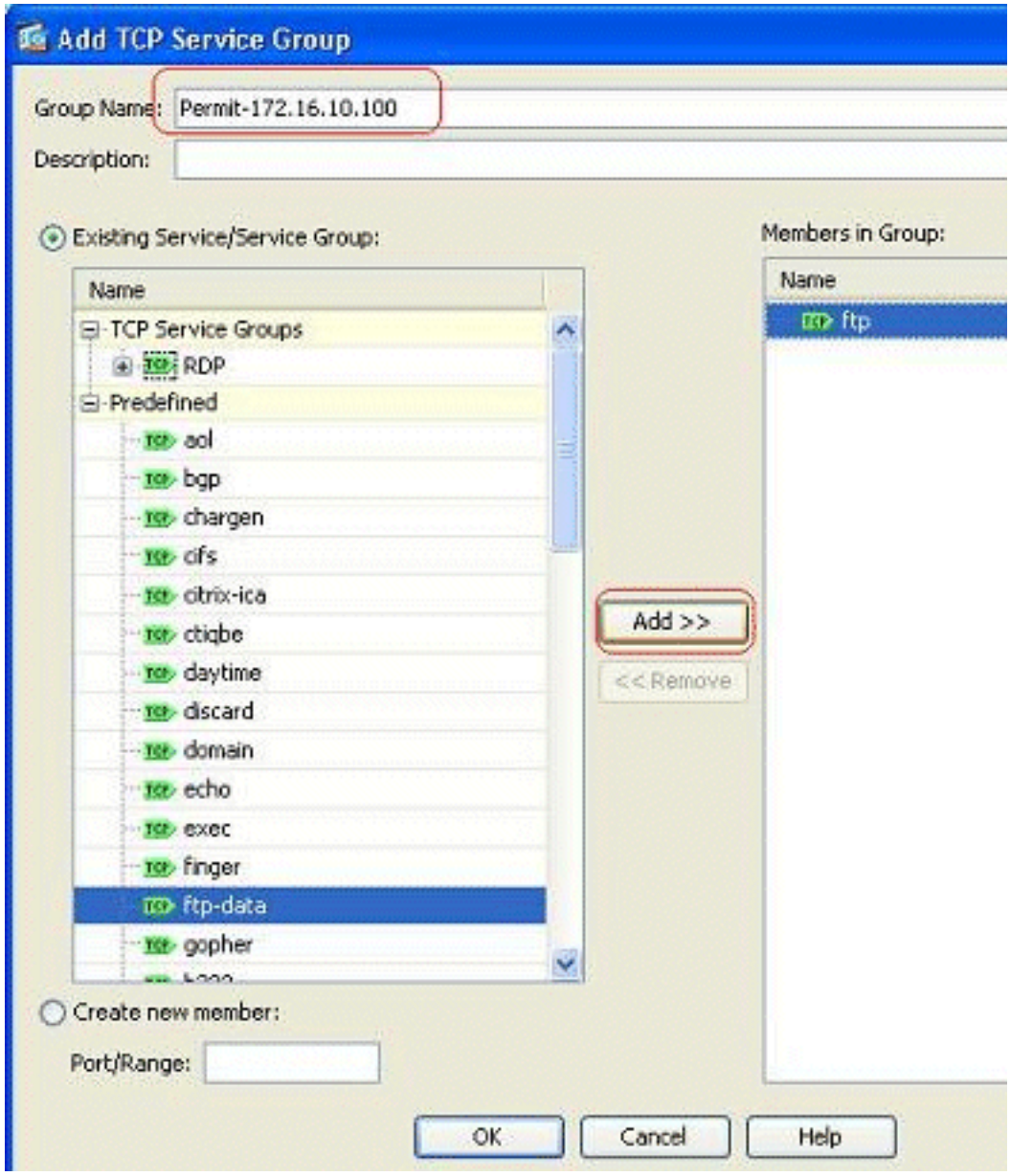


サービス グループを作成します。

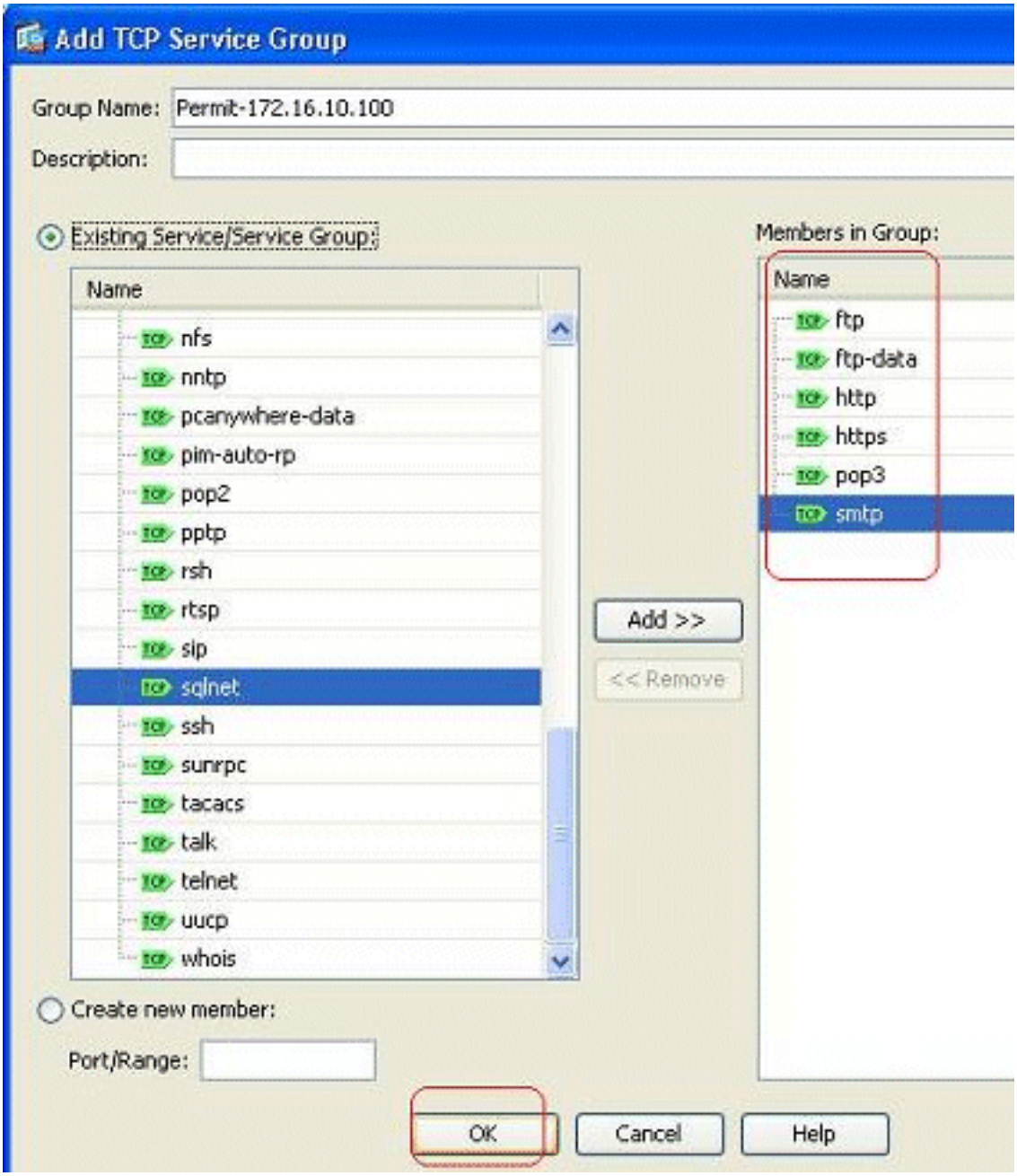
3. [Add] をクリックし、[TCP Service Group] オプションを選択します。



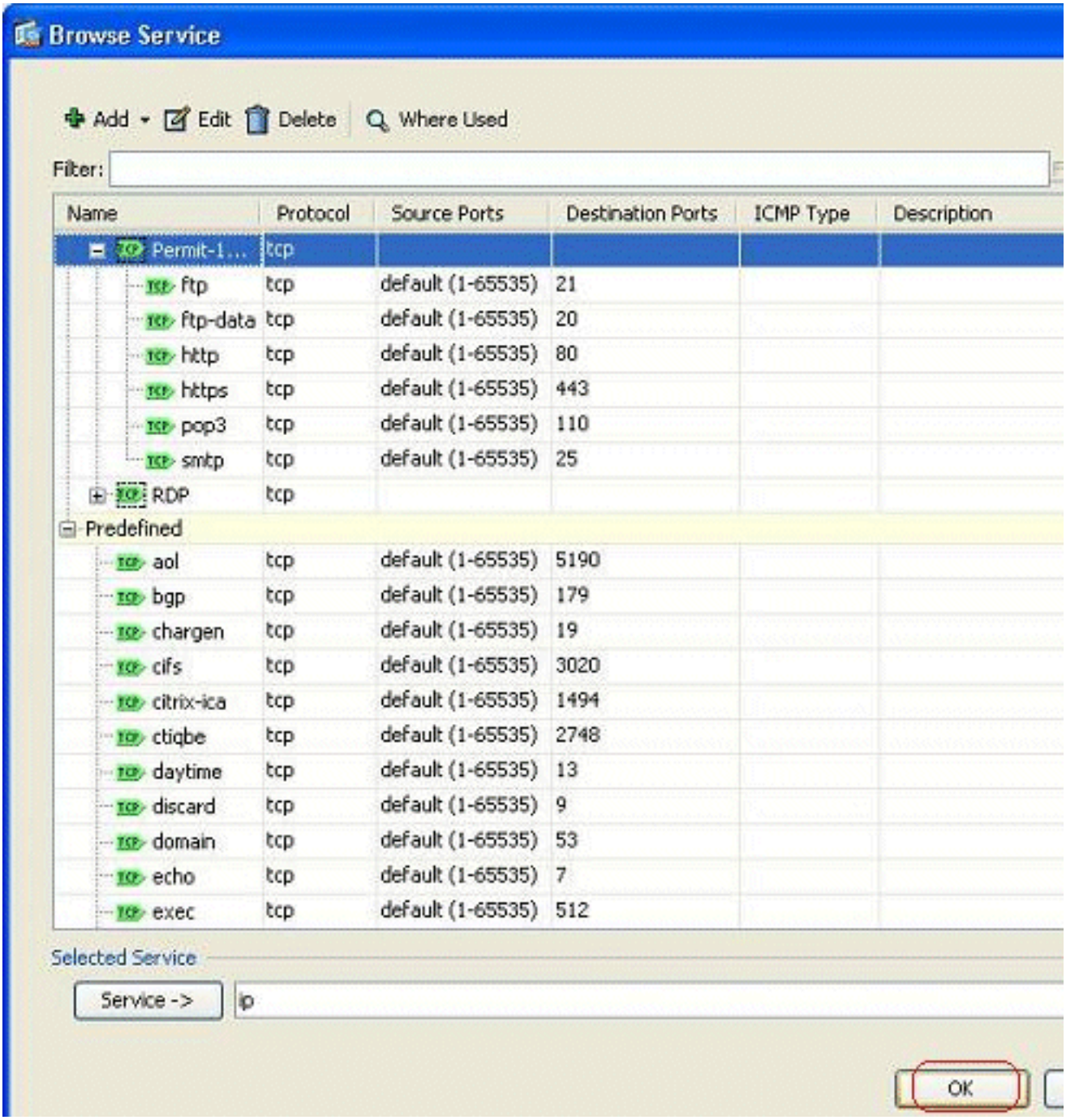
4. このグループの名前を入力します。 必要なポートを 1 つずつ選択して [Add] をクリックし、これらのポートを [Members in Group] フィールドに移動します。



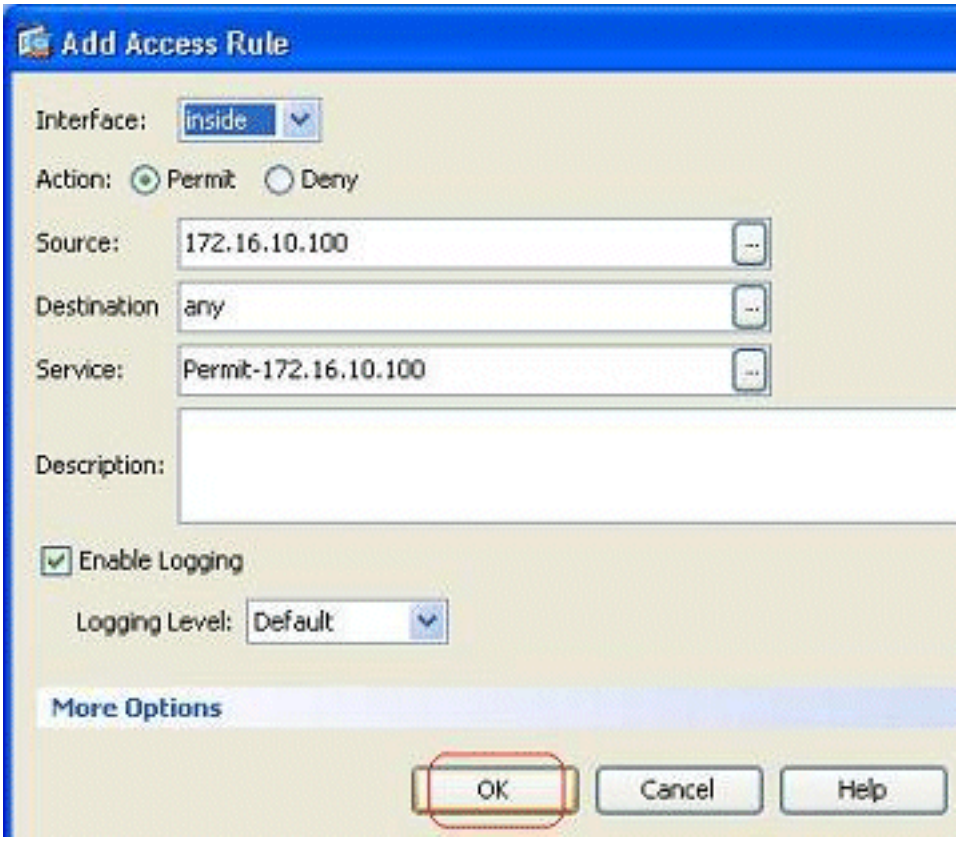
5. 選択したポートがすべて右側のフィールドに表示されていることを確認します。 [OK] をクリックしてサービス ポート選択操作を完了します。



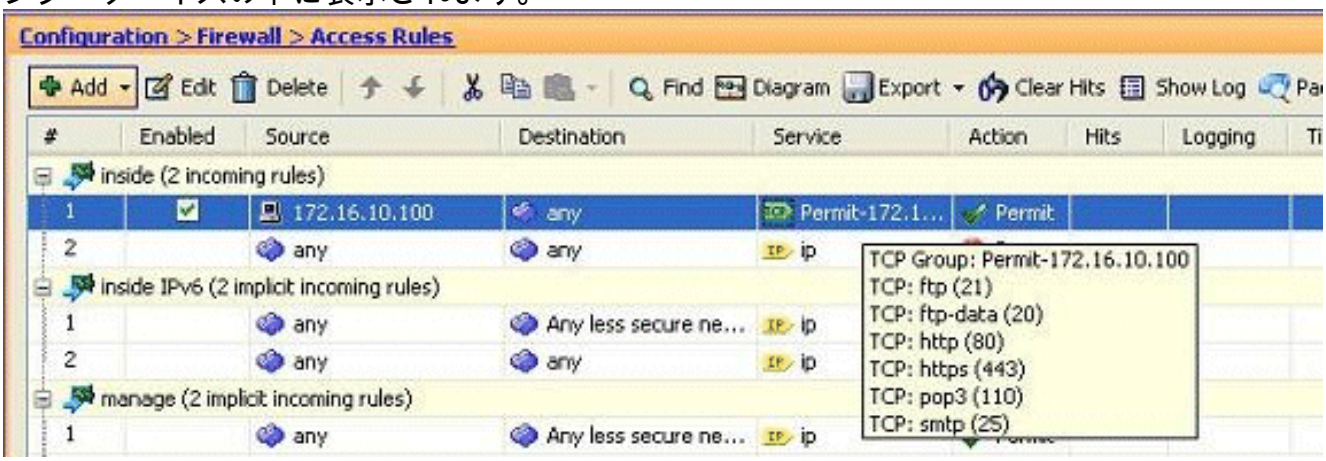
6. 設定した TCP サービス グループが次のように表示されます。 [OK] をクリックします。



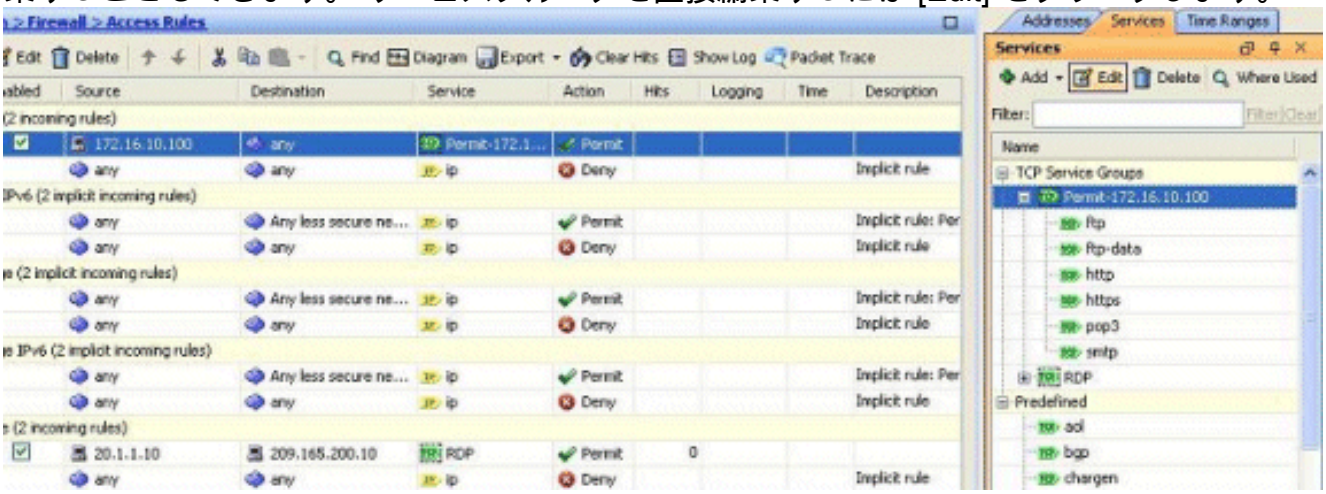
7. [OK] をクリックして設定を完了します。



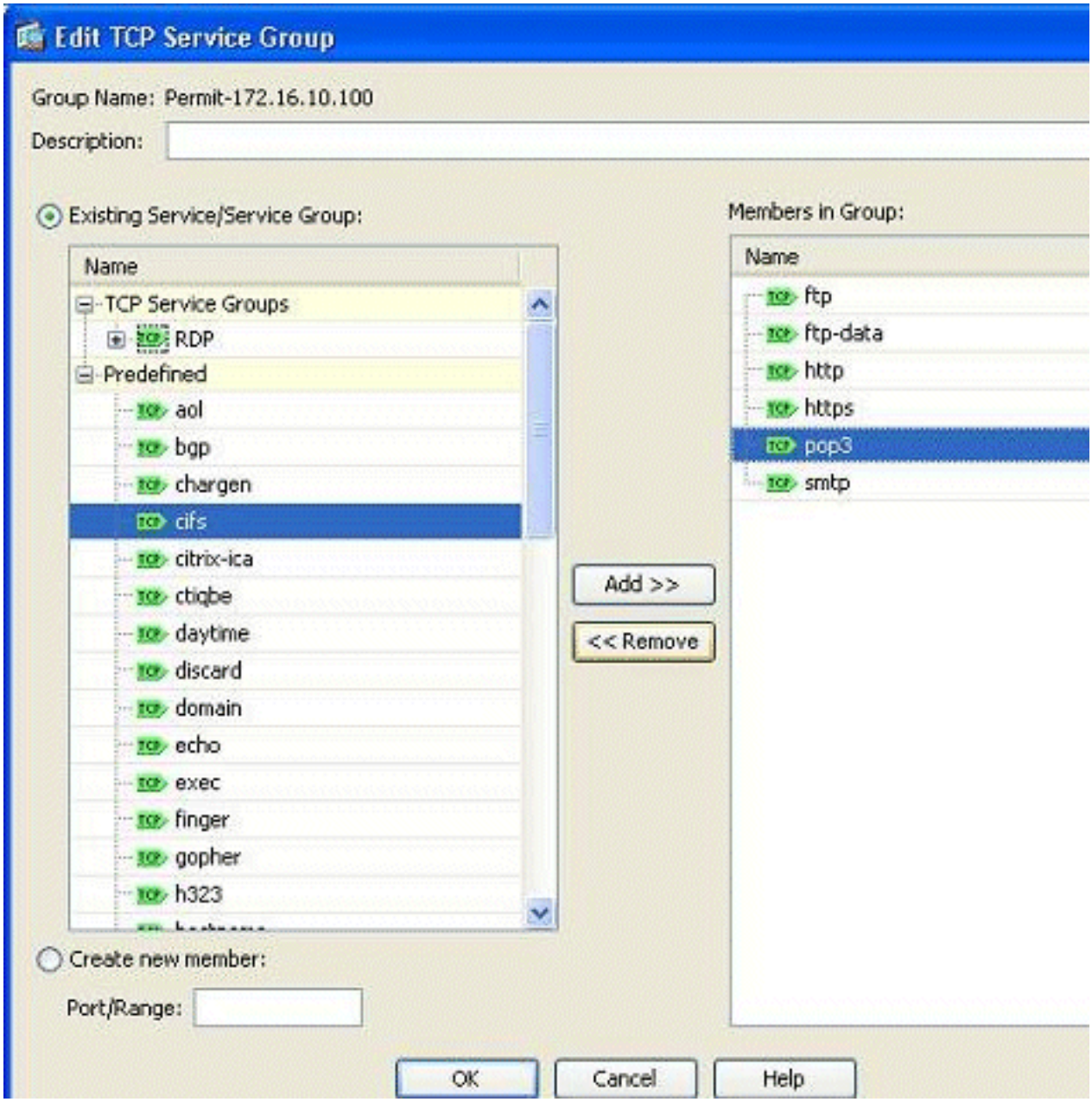
8. 設定したアクセス ルールは [Configuration] > [Firewall] > [Access Rules] ペインの [inside] インターフェイスの下に表示されます。



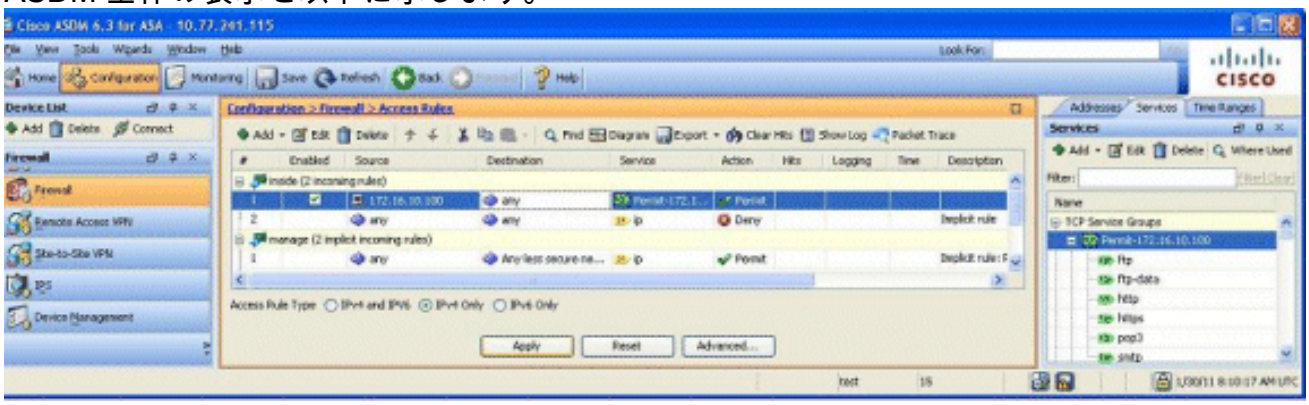
9. 操作のしやすさの点から、右側のペインの [Service] タブで TCP サービスグループを直接編集することもできます。 サービスグループを直接編集するには [Edit] をクリックします。



10. [Edit TCP Service Group] ウィンドウが再び表示されます。 要件に基づいて変更を行い、[OK] をクリックして変更を保存します。



11. ASDM 全体の表示を以下に示します。



対応する CLI 設定を以下に示します。

```
object-group service Permit-172.16.10.100 TCP port-object eq ftp port-object eq ftp-data port-
object eq www port-object eq https port-object eq pop3 port-object eq smtp ! access-list
inside_access_in extended permit TCP host 172.16.10.100 any object-group Permit-172.16.10.100 !
access-group inside_access_in in interface inside !
```

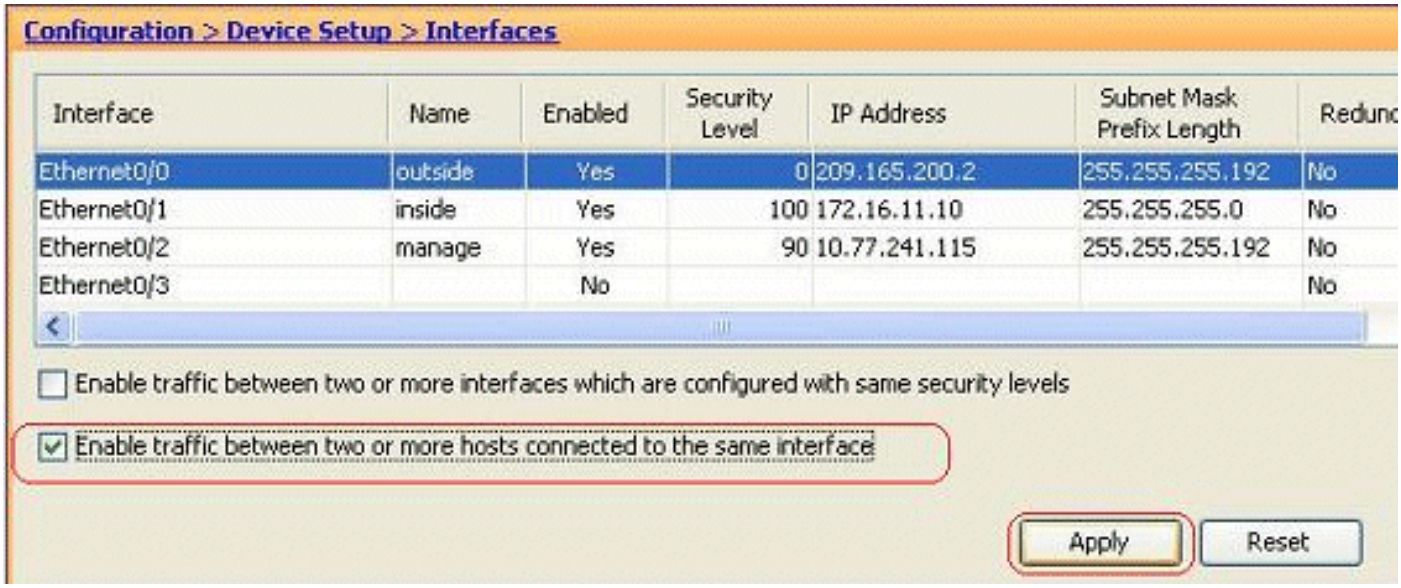
アクセス コントロールの実装の詳細については、『ASDM GUI を使用したアクセス リストの追加または変更』を参照してください。

同じセキュリティ レベルのインターフェイス間でのトラフィックの許可

この項では、同じセキュリティ レベルのインターフェイス間でのトラフィックを有効にする方法を説明します。

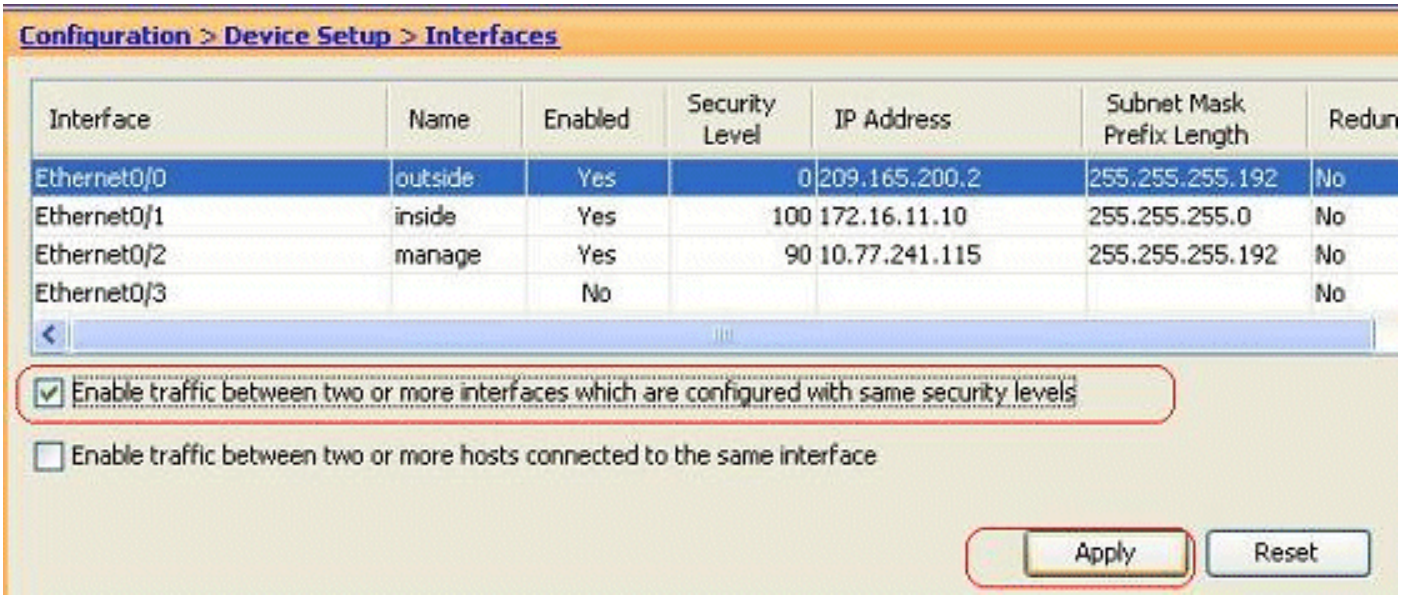
インターフェイス内通信を有効にする手順を以下で説明します。

これは、あるインターフェイスに入り、その後同じインターフェイスからルーティングされる VPN トラフィックの場合に役立ちます。 この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。 [Configuration] > [Device Setup] > [Interfaces] に移動し、[Enable traffic between two or more hosts connected to the same interface option] オプションを選択します。



インターフェイス間通信を有効にする手順を以下で説明します。

同等のセキュリティ レベルが設定されているインターフェイス間の通信を許可する場合に役立ちます。 [Configuration] > [Device Setup] > [Interfaces] に移動し、[Enable traffic between two or more interfaces which are configured with same security levels] オプションを選択します。



以下にこの両方の設定に対応する CLI を示します。

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

信頼できないホストから信頼できるネットワーク上のホストへのアクセスの許可

スタティック NAT 変換とアクセス ルールを適用して、ホストに対しアクセスを許可します。 外部ユーザが社内ネットワーク上の任意のサーバにアクセスできるようにするには、このように設定する必要があります。 内部ネットワークのサーバにはプライベート IP アドレスが設定されます。このプライベート IP アドレスは、インターネット上でルーティング不可能です。 このため、スタティック NAT ルールを使用してプライベート IP アドレスをパブリック IP アドレスに変換する必要があります。 1 つの内部サーバ (172.16.11.5) があるとします。 このようにアクセスを許可するには、このプライベート サーバ IP をパブリック IP に変換する必要があります。 この例では、172.16.11.5 を 209.165.200.5 に変換するために双方向スタティック NAT を実装する方法を説明します。

アクセス ルールを実装して外部ユーザに対してこの Web サーバへのアクセスを許可するセクションについては説明しません。 わかりやすくするため、簡単な CLI スニペットを以下に示します。

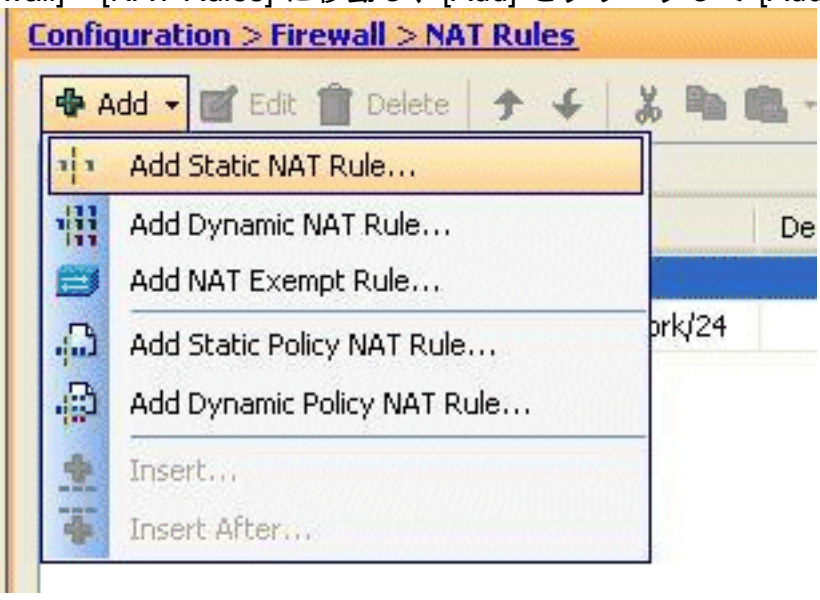
```
access-list 101 permit TCP any host 209.165.200.5
```

詳細については、『ASDM GUI を使用したアクセス リストの追加または変更』を参照してください。

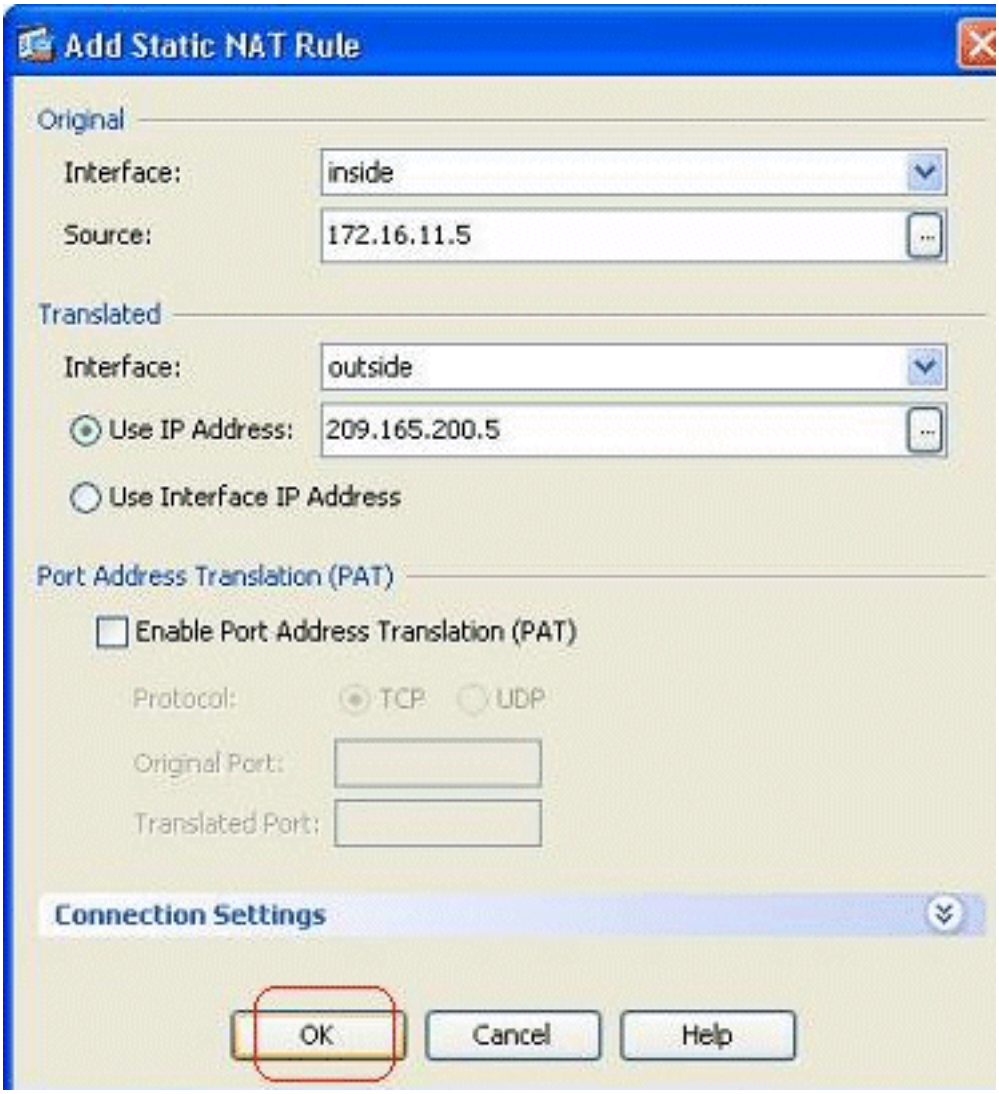
注: キーワード「any」を指定すると、すべての外部ユーザに対してこのサーバへのアクセスが許可されます。 また、サービス ポートに対してこのキーワードが指定されていない場合でも、開いているサービス ポートを介してサーバにアクセスできます。 このため実装の際には十分に注意してください。アクセスの許可を個々の外部ユーザとサーバの必要なポートに制限することを推奨します。

スタティック NAT クライアントを設定するには、次の手順を実行します。

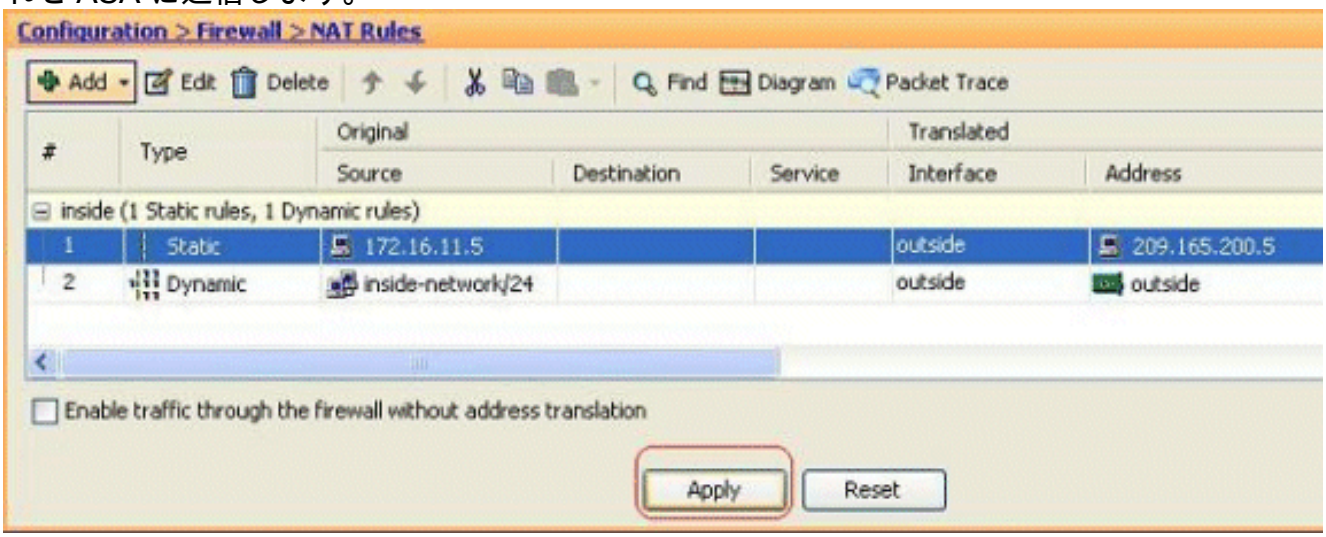
1. [Configuration] > [Firewall] > [NAT Rules] に移動し、[Add] をクリックして [Add Static NAT Rule] を選択します。



2. 変換前の IP アドレスと変換後の IP アドレス、およびそれぞれの関連インターフェイスを指定し、[OK] をクリックします。



3. 設定したスタティック NAT エントリは次のように表示されます。 [Apply] をクリックしてこれを ASA に送信します。



この ASDM 設定の簡単な CLI の例を以下に示します。

```
! static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255 !
```

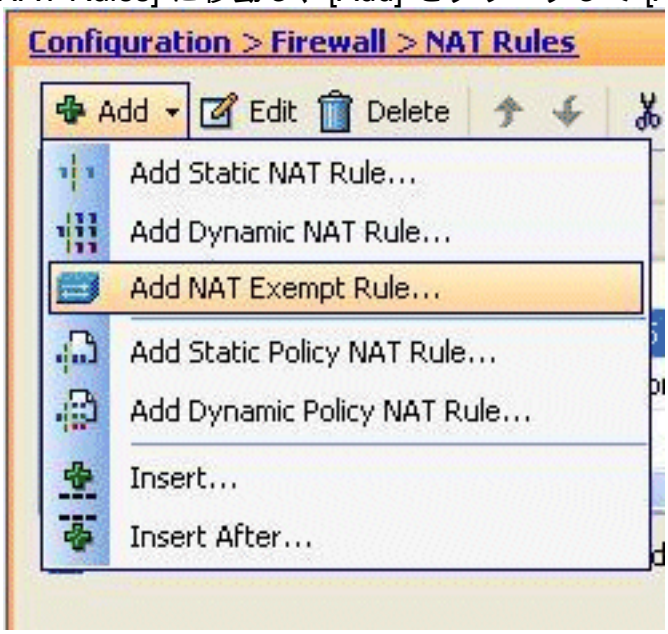
特定のホストおよびネットワークでの NAT の無効化

特定のホストまたはネットワークを NAT から除外するには、NAT 免除ルールを追加してアドレス変換を無効にします。 これにより、変換ホストとリモート ホストの両方が接続を開始できます

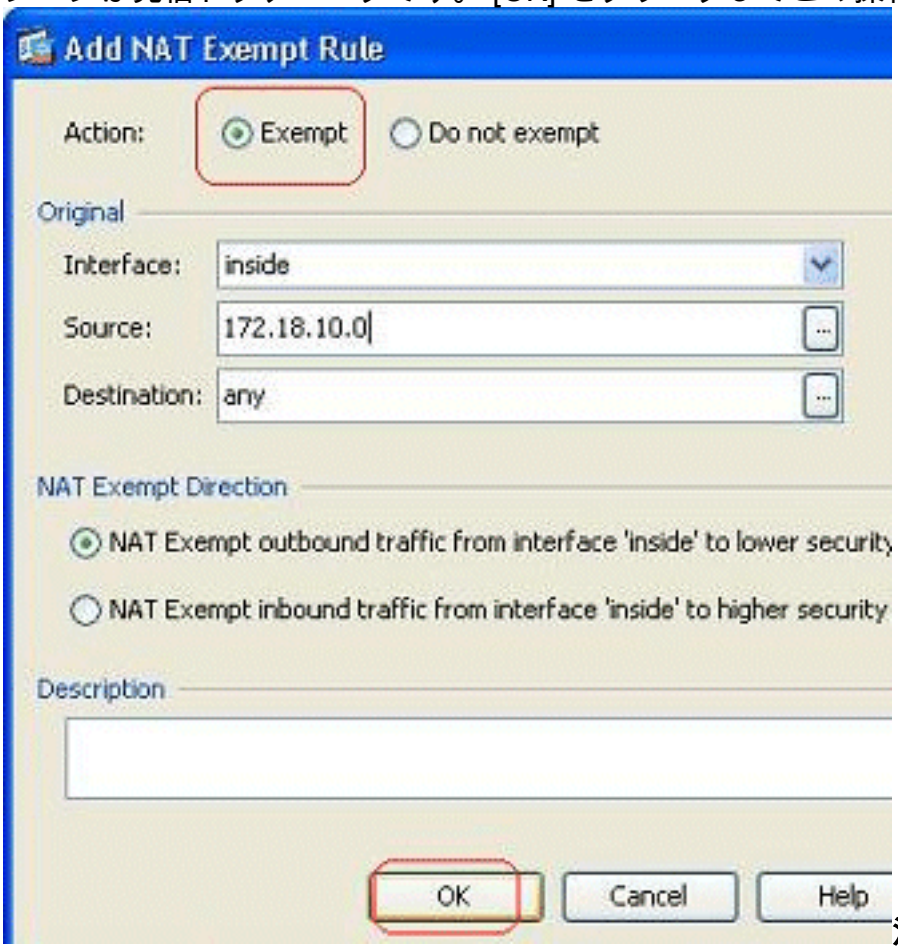
。

次の手順を実行します。

1. [Configuration] > [Firewall] > [NAT Rules] に移動し、[Add] をクリックして [Add NAT Exempt Rule] を選択します。



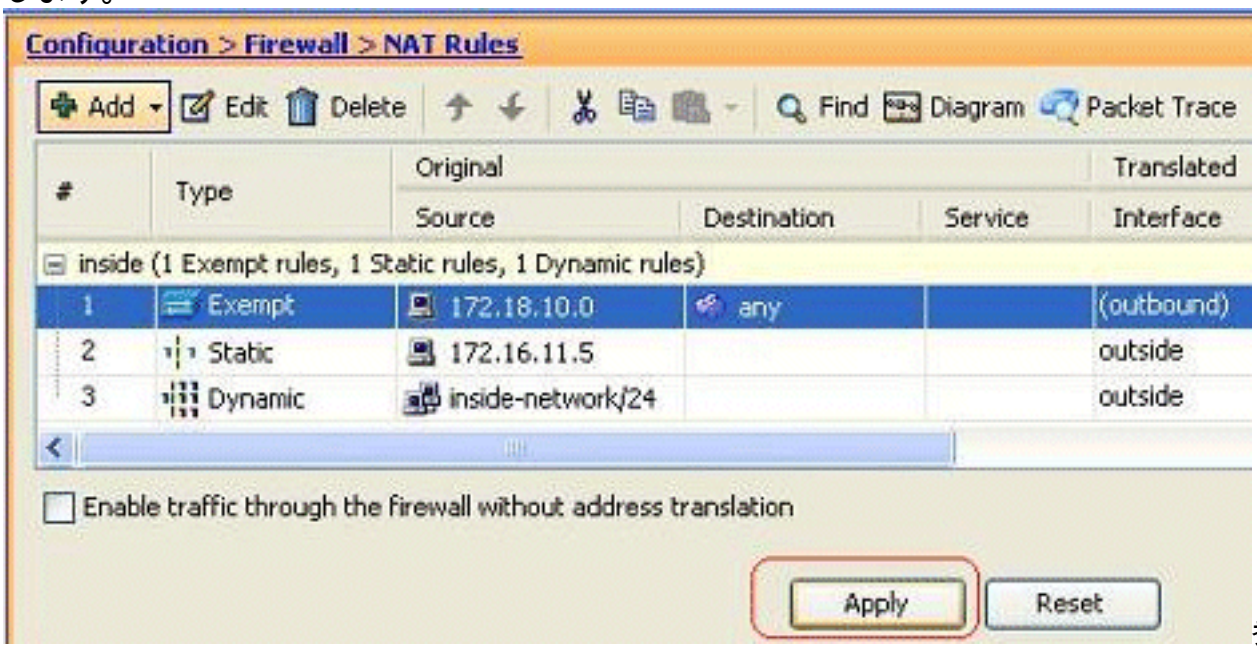
2. この例では、inside ネットワーク 172.18.10.0 がアドレス変換対象から免除されます。[Exempt] オプションが選択されていることを確認します。 [NAT Exempt Direction] には 2 つのオプションがあります。セキュリティ レベルが低いインターフェイスへの発信トラフィックセキュリティ レベルが高いインターフェイスへの着信トラフィックデフォルト オプションは発信トラフィックです。 [OK] をクリックしてこの操作を完了します。



注: [Do not exempt] オプションを選択すると、特定のホストが NAT から除外されず、「deny」キーワードによって個々

のアクセス ルールが追加されます。 これは、特定のホストを除くサブネット全体が NAT 免除対象となるため、特定のホストを NAT 免除対象にしないようにする場合に役立ちます。

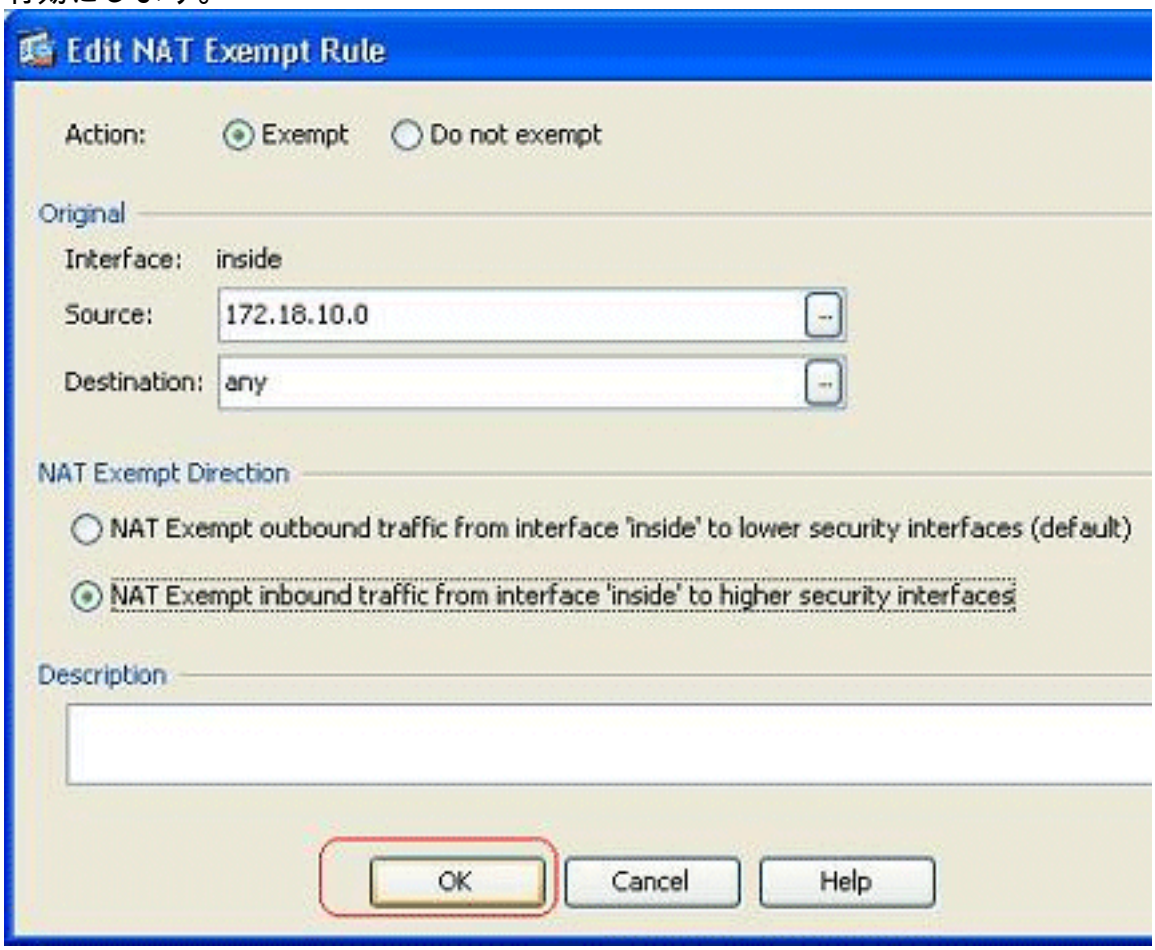
3. 発信方向の NAT 免除ルールを以下に示します。 [Apply] をクリックして ASA に設定を送信します。



参考までに、対応する CLI 出力を以下に示します。

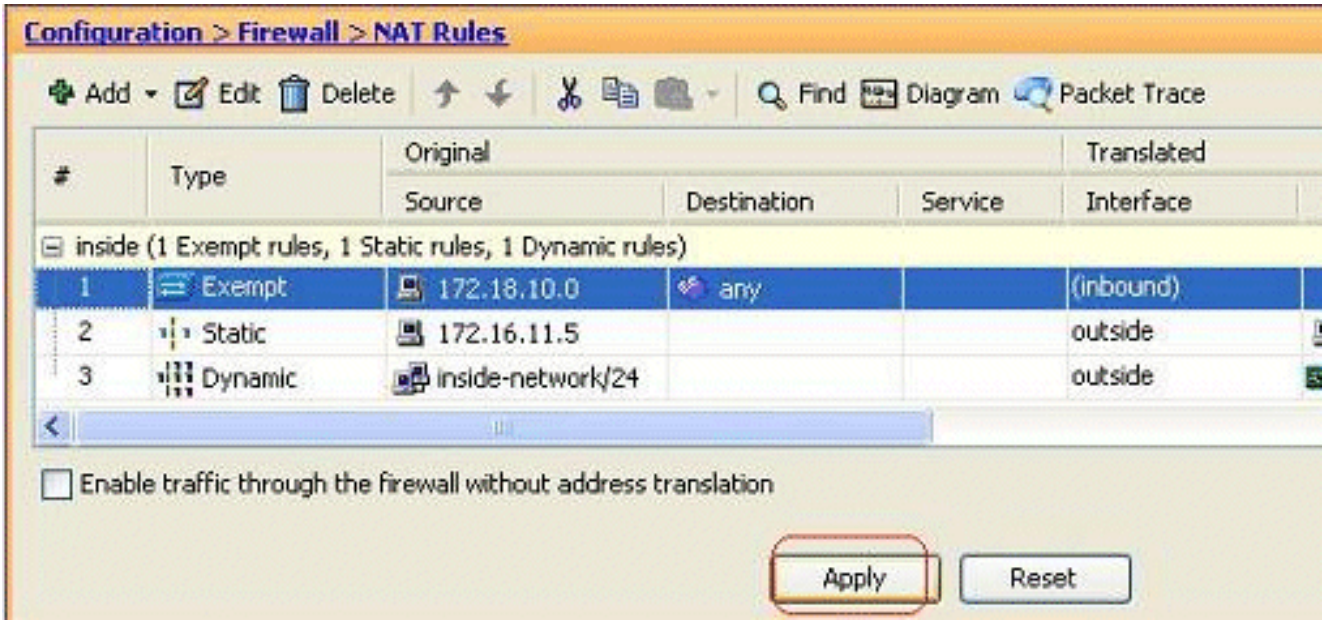
```
access-list inside_nat0_outbound extended
permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. この方向の NAT 免除ルールの編集方法を以下に示します。 [OK] をクリックしてオプションを有効にします。



^

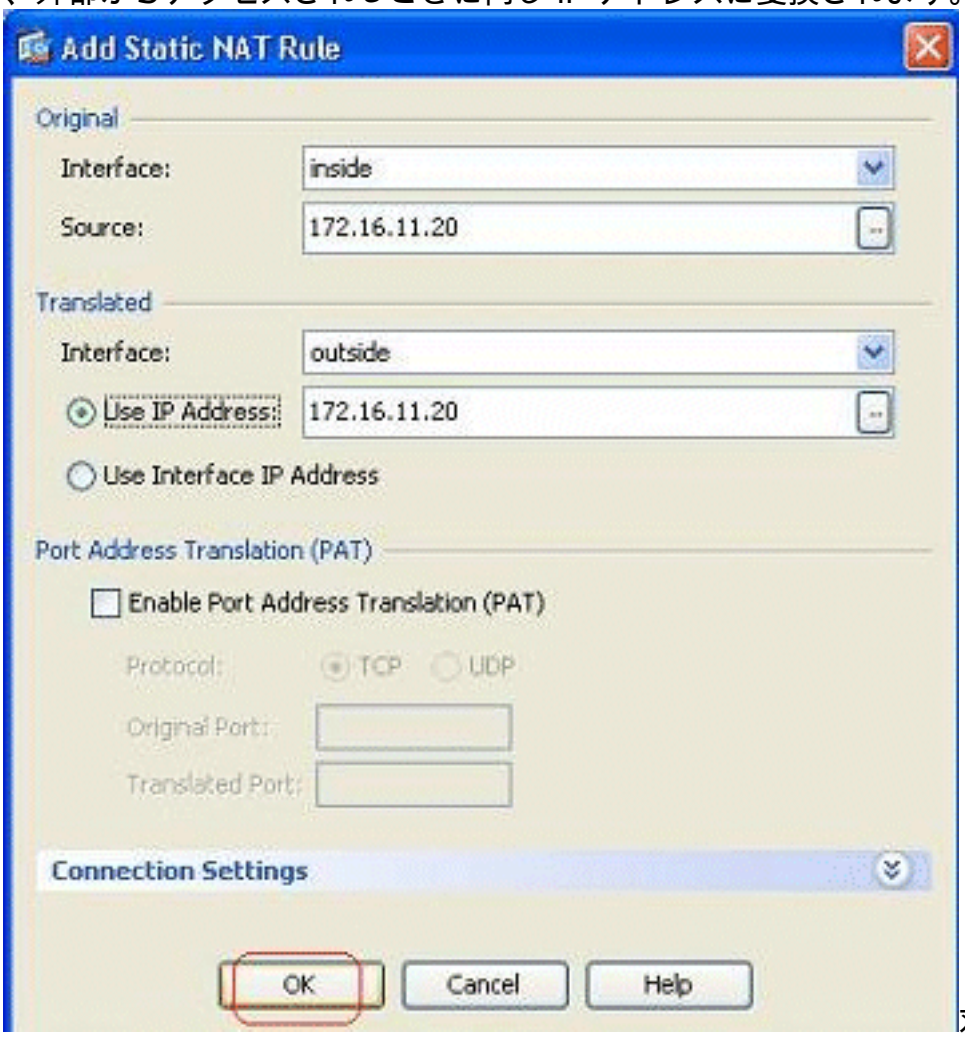
5. 方向が *inbound* に変更されたことがわかります。



[Apply] をクリックして次の CLI 出力を ASA に送信します。`access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any`
`!`

`nat (inside) 0 access-list inside_nat0_outbound` **`outside`** **注:** この出力から、新しいキーワード（outside）が **nat 0** コマンドの終わりに追加されていることがわかります。 この機能は **Outside NAT** と呼ばれます。

6. NAT を無効にするもう 1 つの方法として、アイデンティティ NAT を実装する方法があります。 アイデンティティ NAT はホストを同じ IP アドレスに変換します。 標準的なスタティック アイデンティティ NAT の例を以下に示します。この例ではホスト（172.16.11.20）が、外部からアクセスされるときに同じ IP アドレスに変換されます。



対応する CLI 出力を以下

に示します。

```
! static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255 !
```

static を使用したポート リダイレクション（フォワーディング）

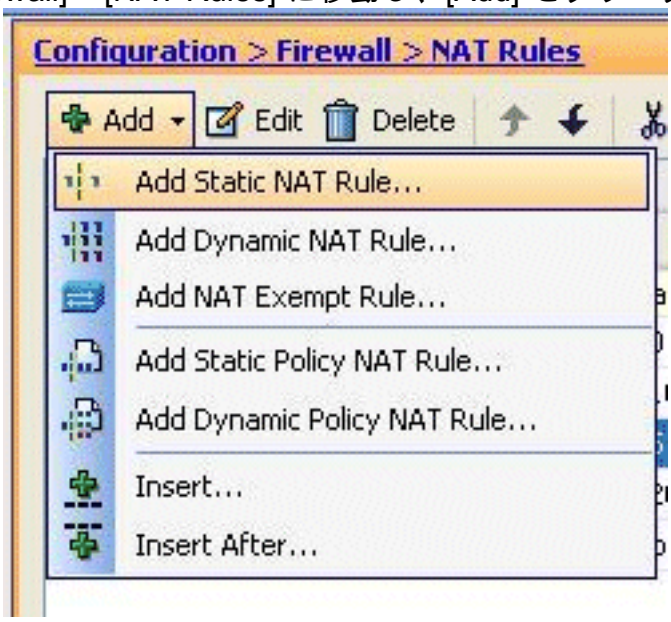
ポート フォワーディング（ポート リダイレクション）は、外部ユーザが特定ポートから内部サーバにアクセスする場合に便利な機能です。 このためには、内部サーバに設定されているプライベート IP アドレスをパブリック IP アドレスに変換し、特定のポートでのアクセスを許可します。

以下の例では、外部ユーザが SMTP サーバ 209.165.200.15 にポート 25 でアクセスすることを求めています。 このためには次の 2 つの手順を実行します。

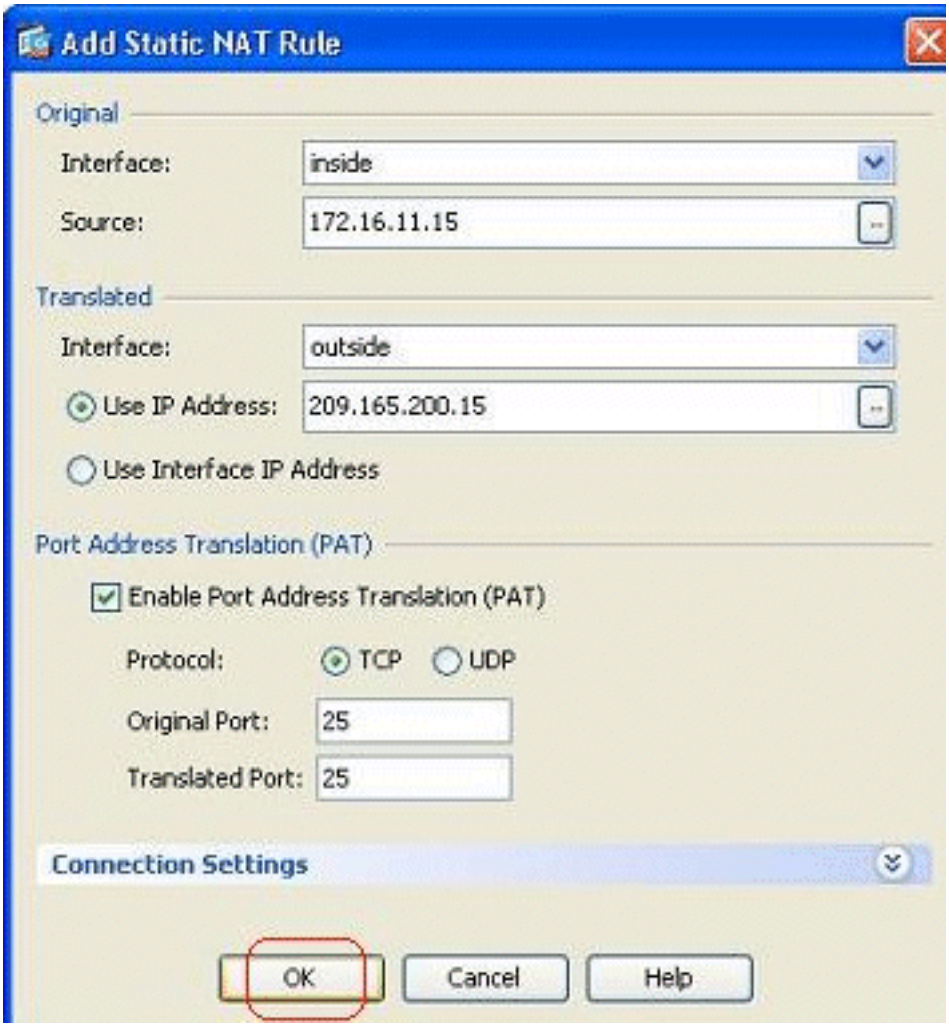
1. 内部メール サーバ 172.16.11.15、ポート 25 をパブリック IP アドレス 209.165.200.15、ポート 25 に変換します。
2. パブリック メール サーバ 209.165.200.15 へのポート 25 でのアクセスを許可します。

外部ユーザがこのサーバ 209.165.200.15 にポート 25 でアクセスすると、このトラフィックは内部メール サーバ 172.16.11 15、ポート 25 にリダイレクトされます。

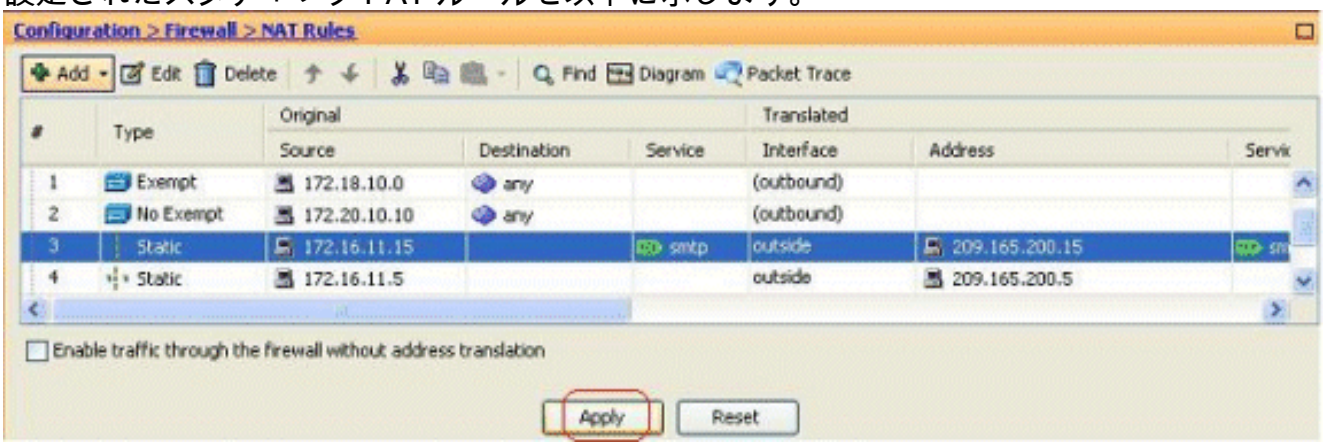
1. [Configuration] > [Firewall] > [NAT Rules] に移動し、[Add] をクリックして [Add Static NAT Rule] を選択します。



2. 変換前のソース IP アドレスと変換後の IP アドレス、およびこれらのアドレスに関連付けられているインターフェイスを指定します。 [Enable Port Address Translation (PAT)] を選択し、リダイレクトするポートを指定して [OK] をクリックします。



3. 設定されたスタティック PAT ルールを以下に示します。



対応する CLI 出力を以下に示します。

```
! static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask 255.255.255.255
!
```

4. これは、外部ユーザに対して 209.165.200.15 のパブリック SMTP サーバへのアクセスを許可するアクセス ルールです。

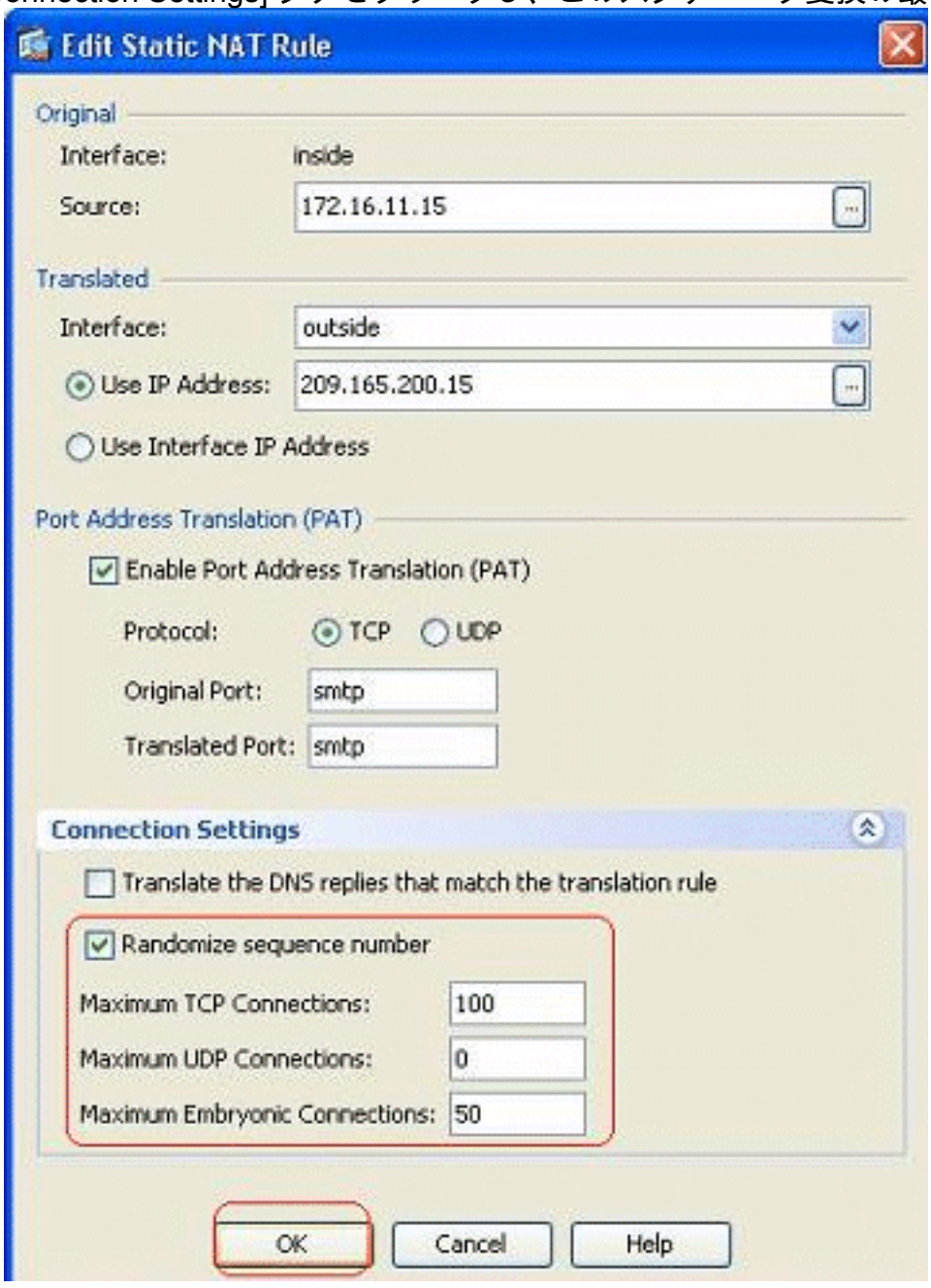
注: アクセス ルールのソースで **any** キーワードの代わりに特定のホストを使用してください。

static を使用した TCP/UDP セッションの制限

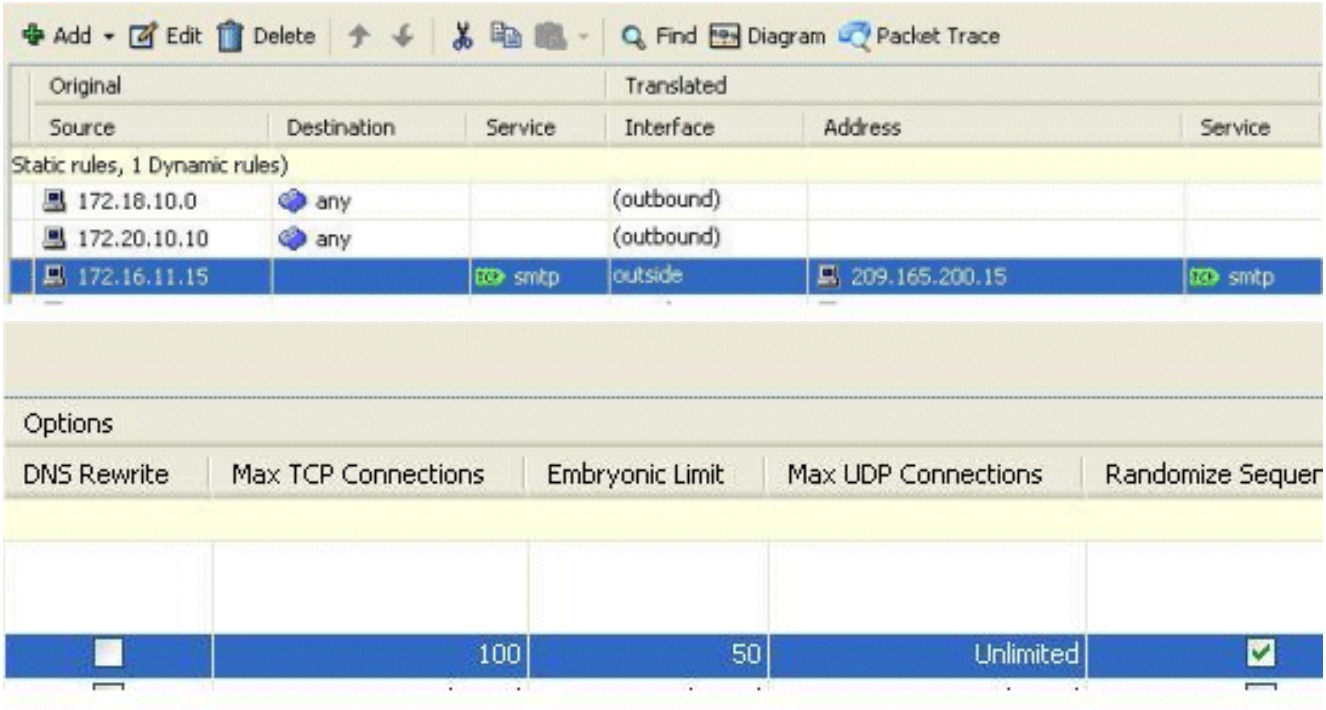
スタティック ルールを使用して TCP/UDP 接続の最大数を指定できます。 また、初期接続の最大数も指定できます。 初期接続とは、ハーフオープン状態の接続です。 大きい値を指定すると、ASA のパフォーマンスに影響します。 これらの接続を制限することで、DoS や SYN のような特定の攻撃をある程度防ぐことができます。 攻撃を完全に緩和するには MPF フレームワークでポリシーを定義する必要がありますが、このドキュメントではこれについては説明しません。 このトピックに関する細く情報については、『ネットワーク攻撃の緩和策』を参照してください。

次の手順を実行します。

1. [Connection Settings] タブをクリックし、このスタティック変換の最大接続数を指定します。



2. 特定のスタティック変換の接続制限を以下に示します。



対応する CLI 出力を以下に示します。!

```
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask 255.255.255.255
TCP 100 50 !
```

時間ベースのアクセス リスト

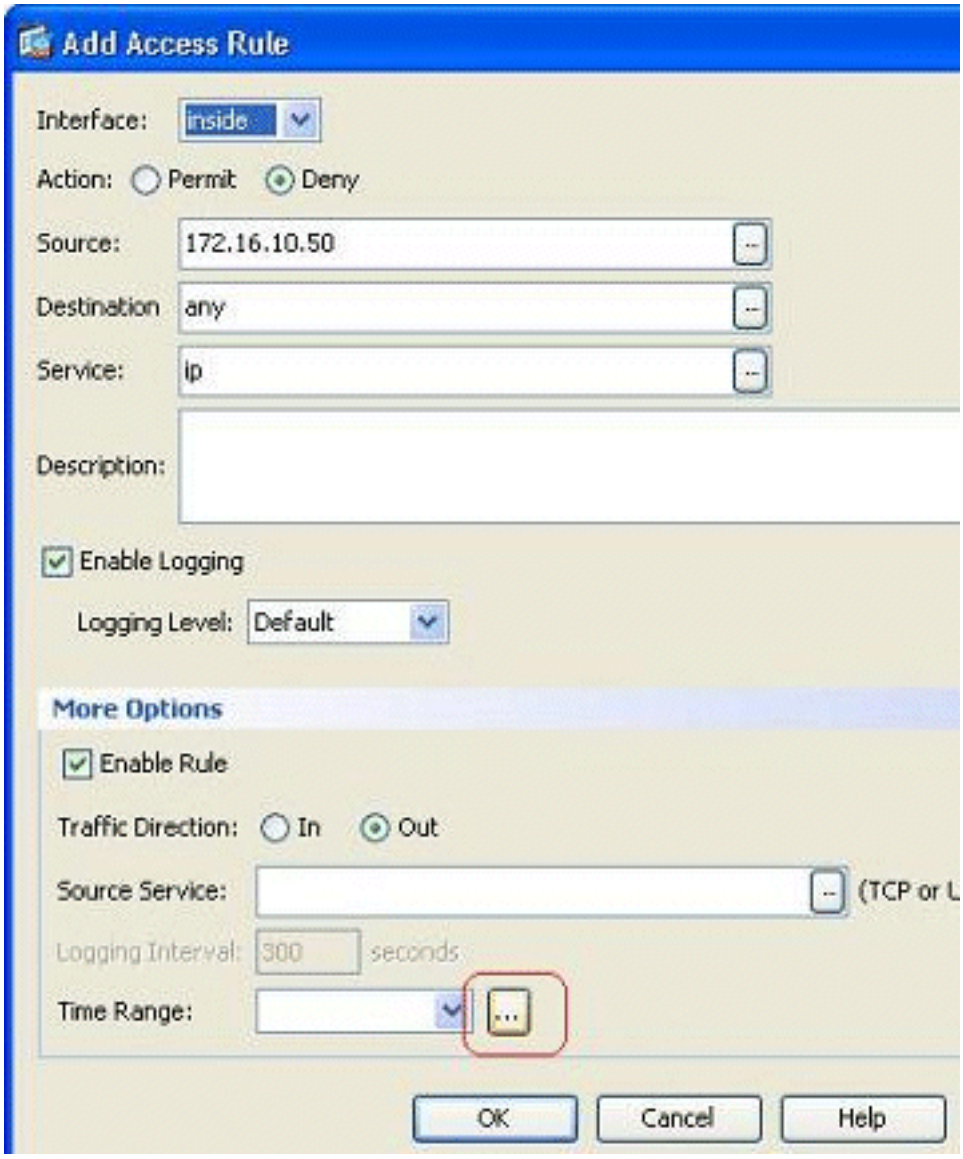
この項では、ASDM を使用して時間ベースのアクセス リストを実装する方法を説明します。 アクセス ルールを時間ベースで適用できます。 このように適用するには、日/週/月/年でタイミングを指定する時間範囲を定義する必要があります。 次にこの時間範囲を必要なアクセス ルールにバインドする必要があります。 時間範囲は次の 2 とおりの方法で定義できます。

1. 絶対（absolute）：開始時刻と終了時刻を指定して時間範囲を定義します。
2. 定期的（periodic）：繰り返しとも呼ばれます。 指定した間隔で発生する時間範囲を定義します。

注: この機能は実装のためにシステム クロック設定を使用するため、時間範囲を設定する前に ASA で正しい日時が設定されていることを確認してください。 ASA を NTP サーバと同期させることで、良好な結果を得ることができます。

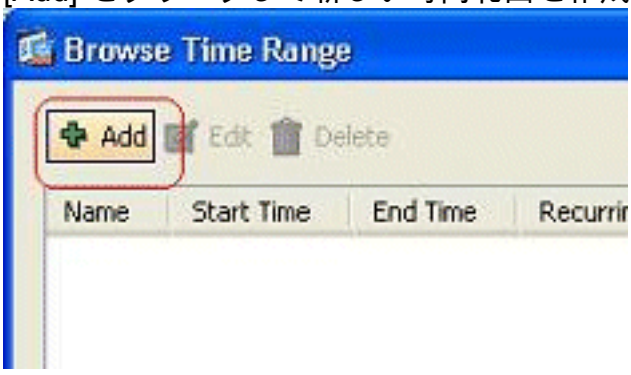
ASDM でこの機能を設定するには、次の手順を実行します。

1. アクセス ルールを定義するときに、[Time Range] フィールドの [Details] ボタンをクリック

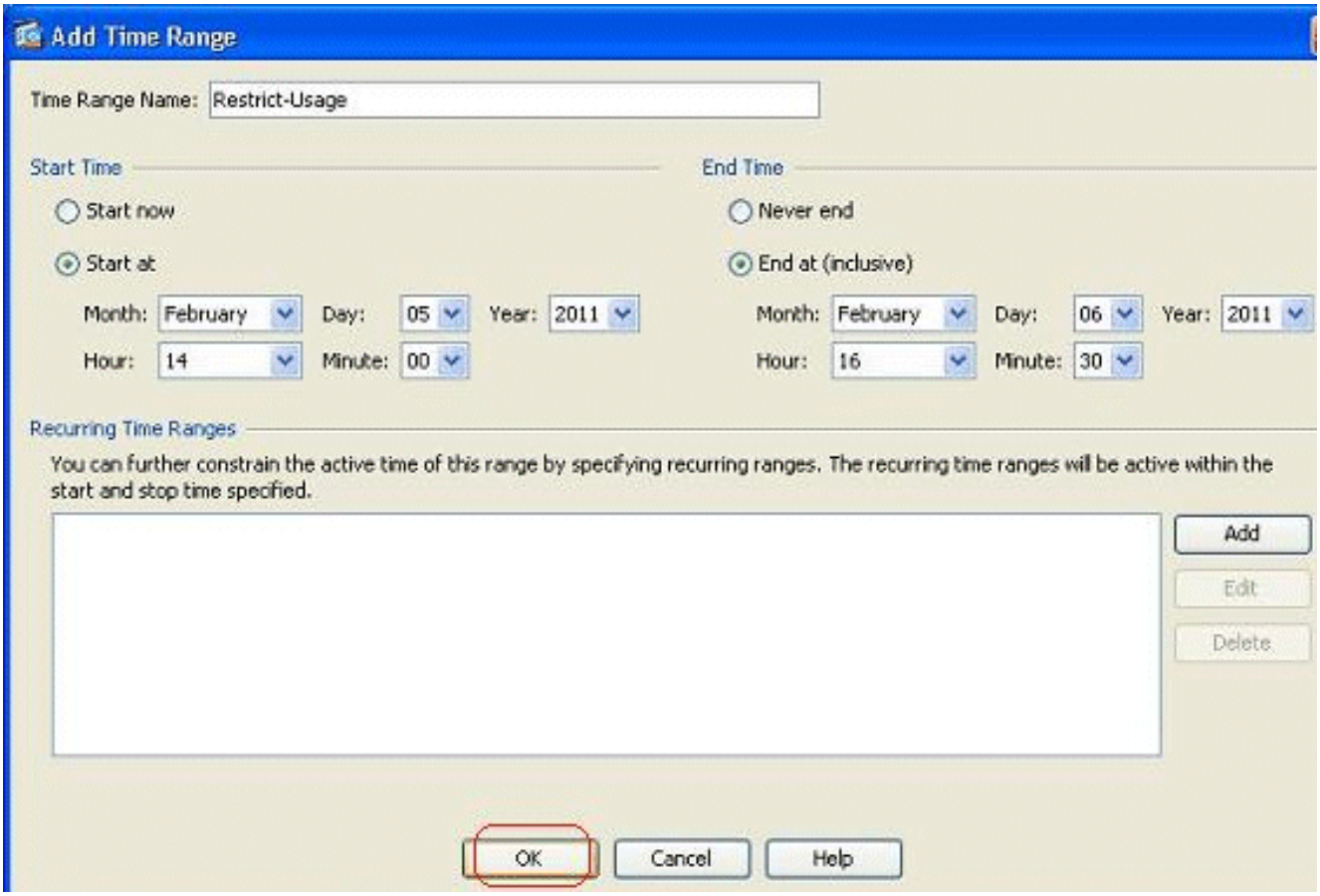


します。

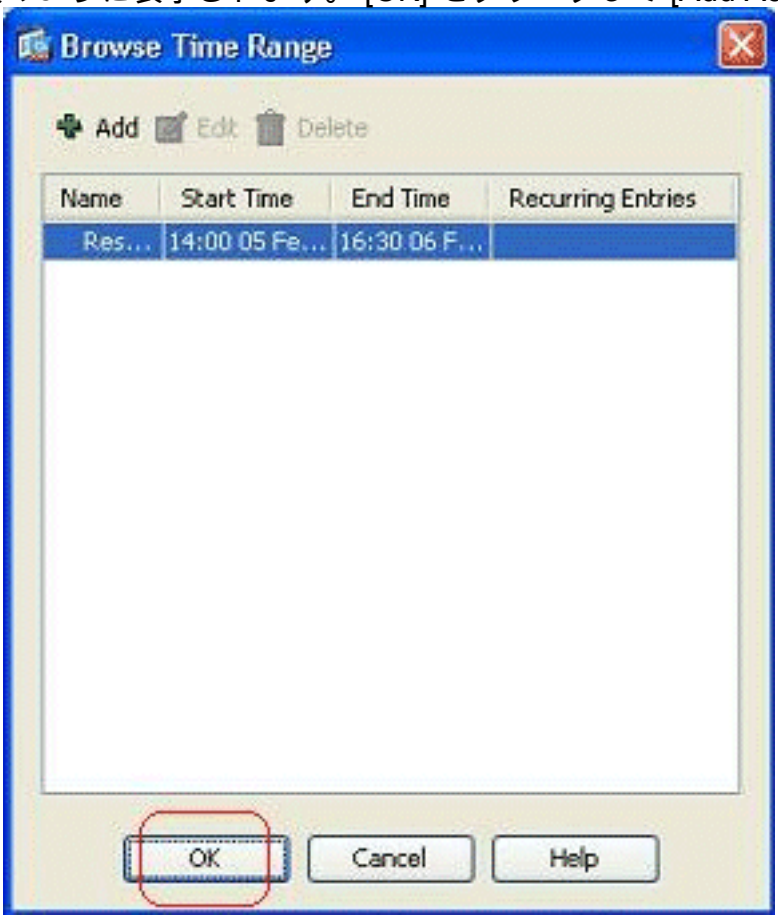
2. [Add] をクリックして新しい時間範囲を作成します。



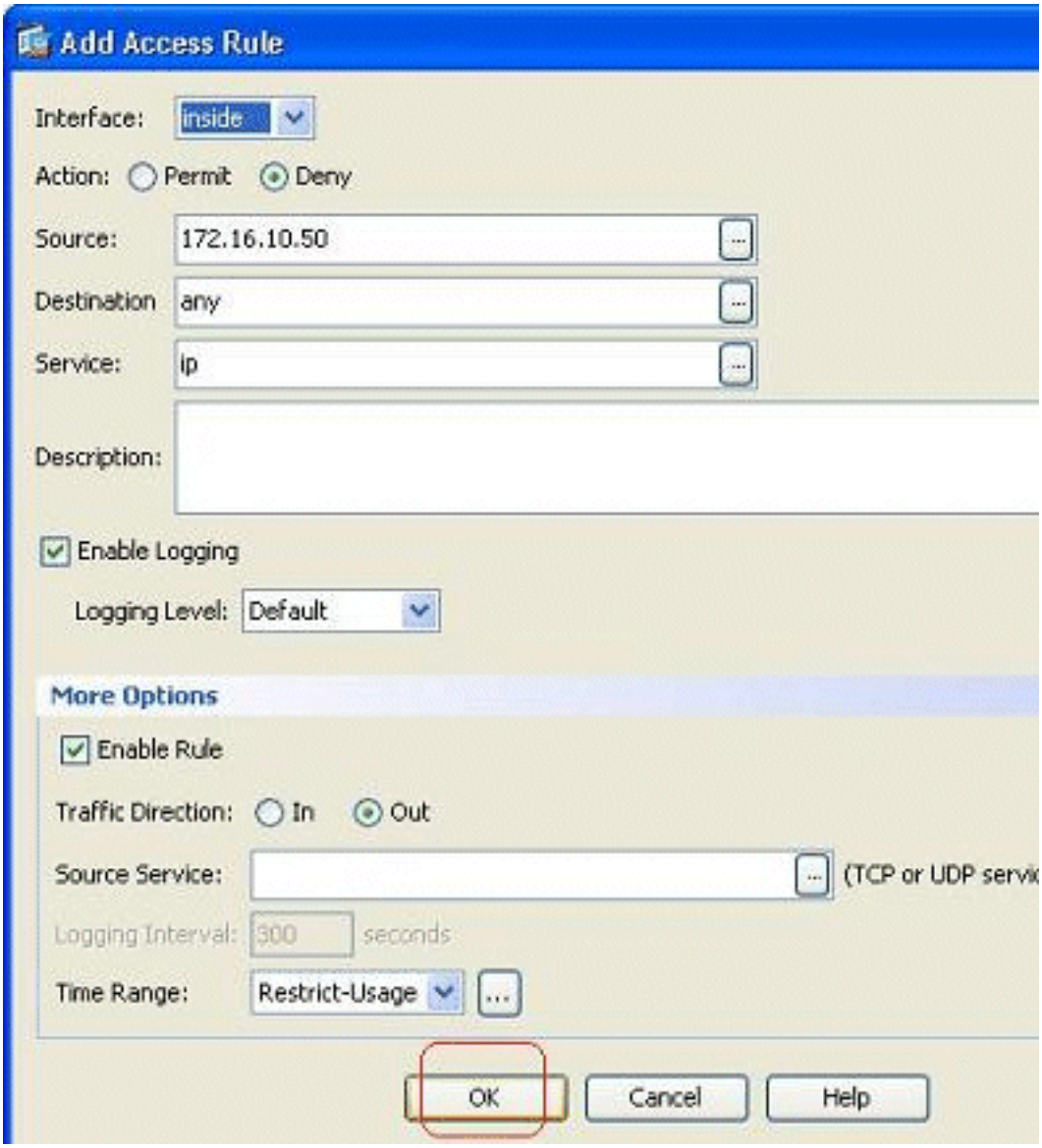
3. 時間範囲の名前を定義し、開始時刻と終了時刻を指定します。 [OK] をクリックします。



4. 時間範囲が次のように表示されます。 [OK] をクリックして [Add Access Rule] ウィンドウに戻ります。



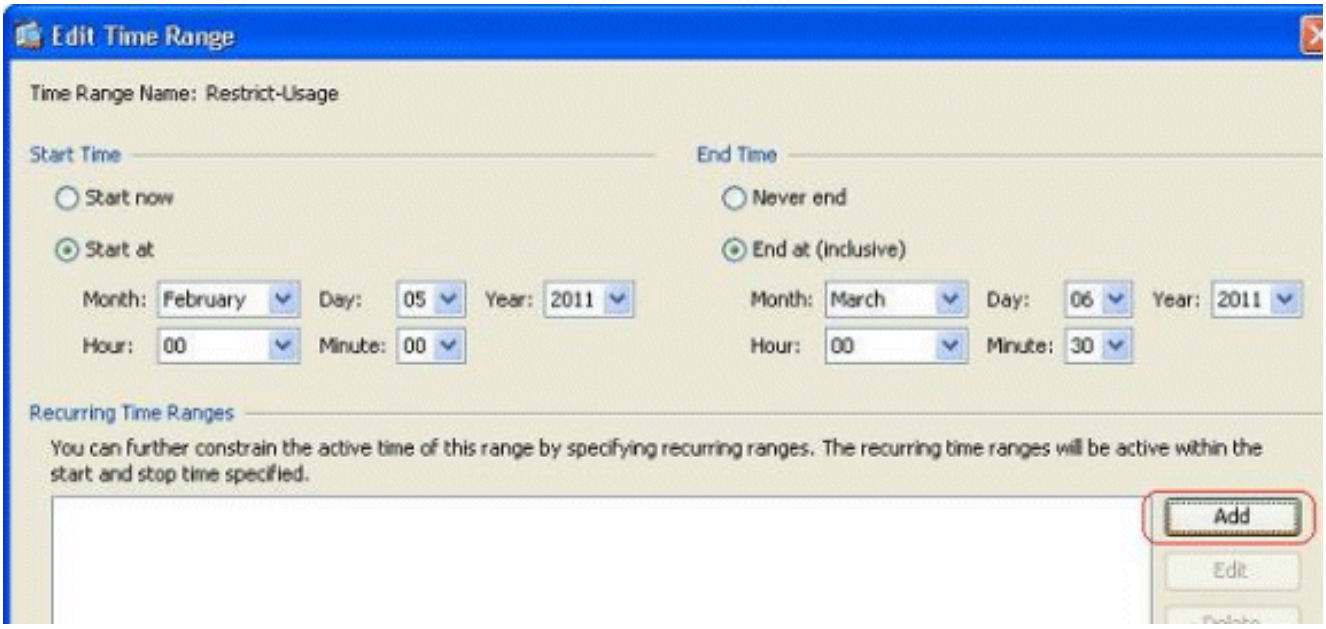
5. 時間範囲 Restrict-Usage がこのアクセス ルールにバインドされていることがわかります。



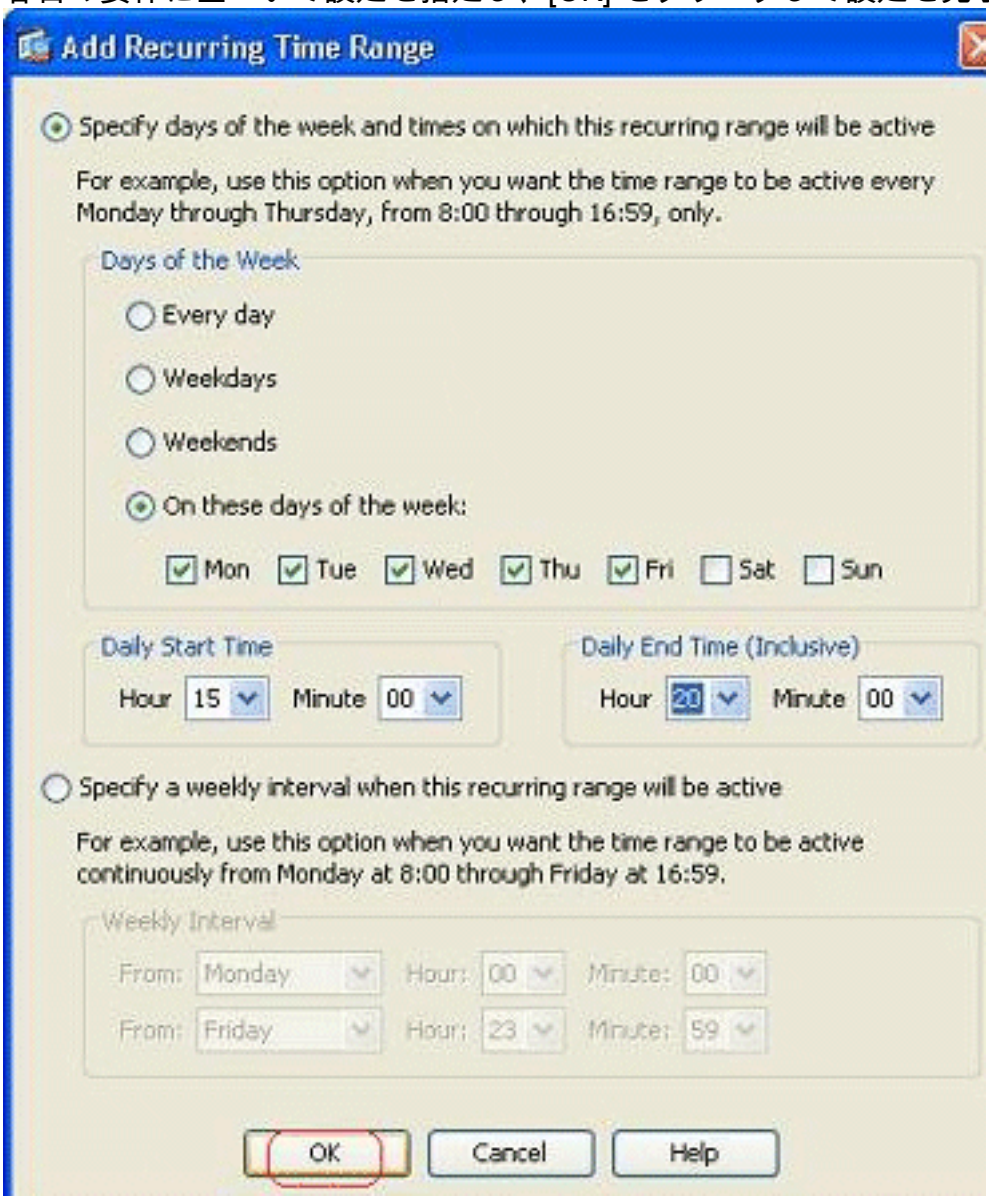
このアクセス ルール設定では、2011 年 2 月 5 日午後 2 時から 2011 年 2 月 6 日午後 4 時 30 分まで、172.16.10.50 のユーザに対してすべてのリソースの使用が制限されます。 対応する CLI 出力を以下に示します。

```
time-range Restrict-Usage absolute start 14:00 05 February 2011 end 16:30 06 February 2011
! access-list inside_access_out extended deny ip host 172.16.10.50 any time-range Restrict-
Usage ! access-group inside_access_out in interface inside
```

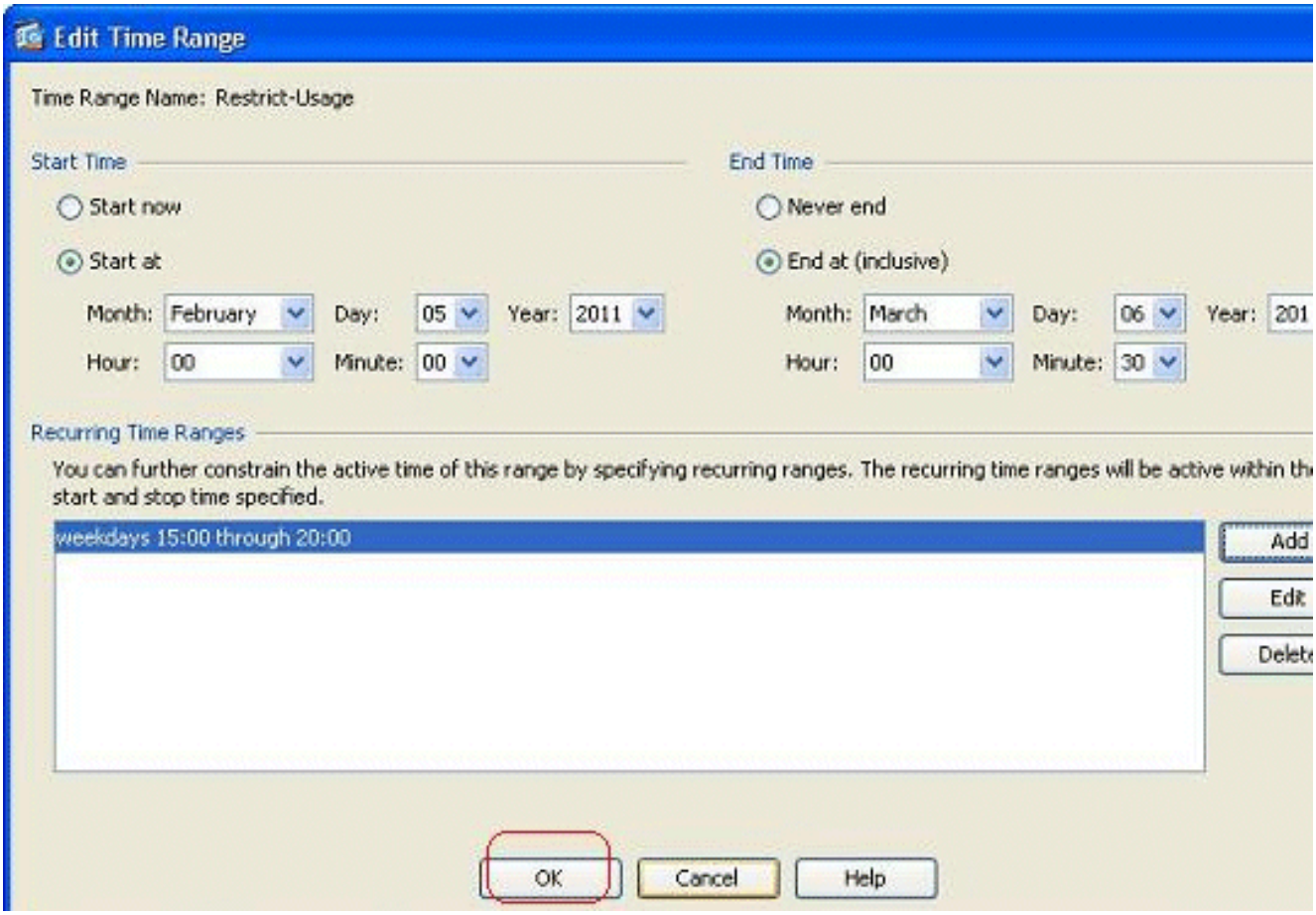
6. 定期的な時間範囲の指定方法の例を以下に示します。 [Add] をクリックして繰り返し時間範囲を定義します。



7. 各自の要件に基づいて設定を指定し、[OK] をクリックして設定を完了します。



8. [OK] をクリックして [Time Range] ウィンドウに戻ります。



この設定では、土日を除くすべての平日の午後 3 時から午後 8 時まで、172.16.10.50 のユーザに対してすべてのリソースに対するアクセスが拒否されます。

```
! time-range Restrict-Usage absolute start 00:00 05 February 2011 end 00:30 06 March 2011
periodic weekdays 15:00 to 20:00 ! access-list inside_access_out extended deny ip host
172.16.10.50 any time-range Restrict-Usage ! access-group inside_access_out in interface
inside
```

注: time-range コマンドに absolute 値と periodic 値の両方が指定されている場合、**periodic** コマンドは absolute start 時刻を経過した後にのみ評価の対象になり、absolute end 時刻を経過した後は評価の対象にはなりません。

関連情報

- Cisco ASA のマニュアル ページ：
- テクニカルサポートとドキュメント - Cisco Systems