



# CHAPTER 5

## NAT の設定

---

この章では、Cisco 4700 Series Application Control Engine (ACE) アプライアンスで NAT を設定する方法について説明します。内容は、次のとおりです。

- [NAT の概要](#)
- [NAT のアイドル タイムアウトの設定](#)
- [ダイナミック NAT および PAT の設定](#)
- [サーバファーム ベースのダイナミック NAT の設定](#)
- [スタティック NAT とスタティック ポート リダイレクションの設定](#)
- [NAT の設定と統計情報の表示](#)
- [Clearing Xlates のクリア](#)
- [NAT 設定の例](#)

## NAT の概要

クライアントがデータセンターのサーバにアクセスする場合は、サーバへの接続時に IP ヘッダーに IP アドレスを組み込みます。クライアントとサーバの間の ACE は、予約済みダイナミック NAT アドレス プールまたはスタティック NAT アドレス マッピングに基づいてクライアント IP アドレスを保存するか、その IP アドレスをサーバ ネットワークのルーティング可能なアドレスに変換し、要求をサーバに送信できます。

この IP アドレス変換プロセスは NAT または送信元 NAT (SNAT) と呼ばれます。ACE は、サーバからの応答パケットがクライアントに戻るようにすべての SNAT マッピングをトラッキングします。統計またはアカウンティング目的でクライアントの IP アドレスを保存するよう要求された場合、SNAT を実行しないでください。

宛先 NAT (DNAT) は、公的にアドレス指定可能な宛先 IP アドレスとともに表示されるように、内部ホストの IP アドレスとポートを変換します。一般的に、スタティック NAT とポートリダイレクションを使用して DNAT を設定します。ポートリダイレクションを使用して、サーバがカスタム サーバ上のサービスをホスティングするよう設定できます (例、ポート 8080 で HTTP をホスティングするサーバ)。

サーバにセキュリティを提供するには、サーバのプライベート IP アドレスを、グローバルにルーティング可能な IP アドレス (クライアントがサーバへの接続に使用) にマッピングします。この場合、ACE はクライアントからサーバにデータを送信する際、グローバル IP アドレスをサーバのプライベート IP アドレスに変換します。反対にサーバがクライアントに応答した場合、セキュリティ上の理由により、ACE はローカル サーバの IP アドレスをグローバル IP アドレスに変換します。このプロセスは DNAT と呼ばれます。

1024 より大きい TCP および UDP ポート番号と ICMP ID を変換するように、ACE を設定することもできます。このプロセスは Port Address Translation (PAT; ポートアドレス変換) と呼ばれます。ACE は、PAT の各 IP アドレスに 64 K - 1 K のポートを提供します。ポート 0 ~ 1024 は予約され、PAT 用に使えません。

ACE では次の場合を除き、デフォルトにより暗黙的な PAT をフローで実行します。

- パケットをルーティングするだけの場合
- パケットをブリッジングするだけの場合
- 透過的なロード バランシングを実行する場合

- サーバのロード バランシングは、転送アクションとともにポリシーに設定します。

NAT の利点は次のとおりです。

- 内部ネットワーク上でプライベート アドレスを使用できます。プライベート アドレスはインターネット上でルーティングできません。
- NAT は、他のネットワークに対してローカル アドレスを非表示にするので、攻撃者はデータセンターのサーバの実アドレスを知ることができません。
- オーバーラップするサブネットに 2 つのインターフェイスが接続されている場合にオーバーラップするアドレスなどの IP ルーティング問題を解決できます。

ACE では、次のタイプの NAT および PAT を提供します。

- インターフェイス ベースのダイナミック NAT
- インターフェイス ベースのダイナミック PAT
- サーバファーム ベースのダイナミック NAT
- スタティック NAT
- スタティック ポート リダイレクション

このセクションの内容は、次のとおりです。

- [ダイナミック NAT](#)
- [ダイナミック PAT](#)
- [サーバファーム ベースのダイナミック NAT](#)
- [スタティック NAT](#)
- [スタティック ポート リダイレクション](#)
- [NAT コマンドの最大数](#)
- [グローバル アドレスに関する注意事項](#)

## ダイナミック NAT

ダイナミック NAT は一般的に SNAT 用に使用され、ローカル送信元アドレスグループを、宛先ネットワーク上でルーティング可能なグローバル送信元アドレスのプールに変換します。グローバル プールは、ローカル グループより少ないアドレスで構成されます。ローカル ホストが宛先ネットワークにアクセスするときに、ACE はローカル ホストにグローバル プールの IP アドレスを割り当てます。

この変換は、ユーザの設定したアイドル時間が経過するとタイムアウトするので、ユーザは同じ IP アドレスを維持することはありません。このため、(Access Control List [ACL; アクセス制御リスト] によって接続が許可されている場合でも) ダイナミック NAT を使用するホストに、宛先ネットワーク上のユーザは確実に接続できません。ホストのグローバル IP アドレスを予測できないほか、ACE はローカル ホストが開始する側でないかぎり、変換を作成しません。ホストへの確実なアクセスについては、「[スタティック NAT とスタティック ポート リダイレクションの設定](#)」を参照してください。



(注)

変換中であれば、グローバル ホストは ACL で許可されている場合に、ローカル ホストへの接続を開始できます。アドレスは予測不能なので、ホストに接続できる可能性は非常に低くなります。ただし、接続できた場合は、ACL のセキュリティに頼ることになります。

ダイナミック NAT の短所は、次のとおりです。

- グローバル アドレス プールのアドレスがローカル グループより少ない場合、トラフィック量が予想を超えるとアドレスが不足する可能性があります。  
この現象が頻繁に発生した場合はダイナミック PAT を使用します。ダイナミック PAT は単一 IP アドレスの複数のポートを使用して 64,000 を超える変換を実行できます。
- グローバル プールで大量のルーティング可能なアドレスを使用する必要があり、宛先ネットワークがインターネットなどの登録アドレスを必要とする場合、使用可能なアドレスが不足することがあります。



(注)

ACE では、ダイナミック NAT とダイナミック PAT に使用する NAT プールで仮想 IP (VIP) アドレスを設定することができます。このアクションは、VIP アドレスを使用して NAT の実サーバを起点とする接続 (クライアントに接続) を使用する場合に利用できます。この機能は、クライアント側ネットワークの実 IP

アドレスの数に制限がある場合に特に便利です。送信元アドレスを同じ IP アドレス (VIP) に変換されている複数の実サーバで PAT を実行する場合は、**nat-pool** コマンドで **pat** キーワードを設定する必要があります。

ダイナミック NAT の利点は、一部のプロトコルでは PAT を使用できないということです。マルチメディア アプリケーションなど、あるポートではデータ ストリームを流し、別のポートで制御パスを提供する一部のアプリケーションでは、ダイナミック PAT は動作しません。

## ダイナミック PAT

SNAT (ステートフル ネットワーク アドレス変換) にも使用されるダイナミック PAT は、複数のローカル送信元アドレスおよびポートを、この目的で予約された IP アドレスおよびポートのプールから宛先ネットワーク上でルーティング可能な 1 つのグローバル IP アドレスおよびポートに変換します。ACE は複数の接続、ホスト、またはその両方のローカル アドレスとローカル ポートを単一のグローバル アドレスと 1024 より大きいポート番号で始まる固有のポートに変換します。

ローカル ホストが特定の送信元ポート上の宛先ネットワークに接続する場合、ACE はローカル ホストにグローバル IP アドレスと固有のポート番号を割り当てます。各ホストには同じ IP アドレスが与えられますが、送信元ポート番号が固有なので、ACE は、宛先として IP アドレスとポート番号を組み込んだリターントラフィックを正しいホストに送信します。

ACE は、固有のローカル IP アドレスごとに 64,000 を超えるポートをサポートします。変換がローカル アドレスおよびローカル ポート固有なので、接続ごとに新しい送信元ポートが生成されて、それぞれ独立した変換を必要とします。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは異なる変換が必要です。

この変換が有効なのは、接続されている間だけなので、ユーザは同じグローバル IP アドレス ポートを維持することはありません。この理由から、(ACL によって接続が許可されている場合でも) ダイナミック PAT を使用するホストに、宛先ネットワーク上のユーザが確実に接続できません。ホストのローカルまたはグローバル ポート番号を予測できないほか、ACE はローカル ホストが開始する側でないかぎり、変換を作成しません。ホストへの確実なアクセスについては、「[スタティック NAT とスタティック ポート リダイレクションの設定](#)」を参照してください。

ダイナミック PAT では 1 つのグローバル アドレスを使用するだけなので、ルーティング可能アドレスの節約になります。ダイナミック PAT は、制御パス ポートとは異なるポートでデータ ストリームを流す一部のマルチメディア アプリケーションでは動作しません。

## サーバ ファーム ベースのダイナミック NAT

インターフェイス レベルのダイナミック NAT に加え、ACE ではサーバ ファーム レベルでのダイナミック NAT もサポートされます。サーバ ファーム ベースのダイナミック NAT (SNAT にも使用) は、プライマリ サーバやバックアップサーバ ファーム内の実サーバの IP アドレスのみに NAT を実行したい場合に利用できます。インターフェイス ベースのダイナミック NAT と同じように、サーバ ファーム ベースのダイナミック NAT では、IP アドレスのプールを使用して送信元アドレスを変換します。インターフェイス ベースのダイナミック NAT とは異なり、サーバ ファーム ベースのダイナミック NAT では、プライマリ サーバ ファームの IP アドレス、またはバックアップサーバ ファームの IP アドレス、あるいはそほ両方を変換します。

この機能は次の場合に使用します。

- ACE がワンアーム モード (ACE と、クライアントおよびサーバの両トラフィックに使用する Cisco 6500 および 7600 シリーズ Catalyst MSFC の間に設定された VLAN が 1 つの構成) で設定されている場合。プライマリサーバとバックアップサーバのファームはいずれも、内部の顧客ネットワーク (同じ VLAN、または別の VLAN を介してアクセス可能) に置かれています。プライマリサーバファームは、レイヤ 2 に接続され、バックアップサーバファームはレイヤ 3 ホップ分を隔てた位置にあります。この場合、バックアップサーバファームにのみ NAT を実行し、プライマリサーバファームには実行しないでください。
- ACE がワンアーム モードに設定され、プライマリサーバファームがローカル、バックアップサーバファームがリモートにあり、いずれも外部のパブリックネットワークからアクセスできる場合。この場合、プライマリサーバファームの SNAT にはプライベートプールの IP アドレスを使用し、バックアップサーバファームには外部からルーティングできる公共の IP アドレスセットを使用します。
- レイヤ 7、または選択したサーバファームに基づいて送信元 NAT を実行する場合。

サーバファームベースのダイナミック NAT の設定については、「[サーバファームベースのダイナミック NAT の設定](#)」を参照してください。

## スタティック NAT

スタティック NAT は一般的に DNAT (ダイナミック NAT) 用に使用され、各ローカル アドレスを固定のグローバル アドレスに変換します。ダイナミック NAT および PAT では、変換のタイムアウト後も、各ホストは異なるアドレスまたはポートを使用します。スタティック NAT では、グローバル アドレスは連続する各接続で同じあり、持続型の変換ルールが適用されるので、スタティック NAT によりグローバル ネットワーク上のホストは、ローカル ホストへトラフィックを開始できます (ACL で許可されている場合)。

ダイナミック NAT とスタティック NAT の主な違いは、次のとおりです。

- スタティック NAT が、ローカル IP アドレスと固定のグローバル IP アドレスの間で 1 対 1 で対応するのに対し、ダイナミック NAT はグローバル アドレスのプールからグローバル IP アドレスを割り当てます。
- スタティック NAT では、同じ数のローカル IP アドレスとグローバル IP アドレスが必要です。ダイナミック NAT では、グローバル アドレスのプールはローカル アドレスより少なくなります。

## スタティック ポート リダイレクション

スタティック ポート リダイレクションも DNAT 用に使用され、スタティック NAT と同じ機能を実行します。さらに、ローカルおよびグローバル アドレスの TCP または UDP ポート、あるいは ICMP ID を変換します。スタティック ポート リダイレクションでは、複数のスタティック NAT ステートメントで同じグローバル アドレスを使用できます (そのアドレスとともに異なるポート番号を使用する場合)。

たとえば、グローバル ユーザが FTP、HTTP、および SMTP にアクセスするために単一アドレスを提供しますが、ローカル ネットワーク上のプロトコルごとにサーバが異なる場合、異なるポートで同じグローバル IP アドレスを使用するサーバごとにスタティック ポートのリダイレクション ステートメントを指定できます。

## NAT コマンドの最大数

ACE は、次の **nat** コマンド、**nat-pool** コマンド、および **nat static** コマンドの最大数をサポートします。この数はすべてのコンテキストの間で分割されます。

- **nat** コマンド - 8,192
- **nat-pool** コマンド - 8,192
- **nat static** コマンド - 8,192

## グローバル アドレスに関する注意事項

ローカル アドレスをグローバル アドレスに変換するときには、次のグローバル アドレスを使用できます。

- グローバル インターフェイスと同じネットワーク上のアドレス - (ACE から発信するトラフィックが通過する) グローバル インターフェイスと同じネットワーク上のアドレスを使用した場合、ACE はプロキシ ARP を使用し変換されたアドレスの要求に回答して、ローカル アドレス宛でのトラフィックを代行受信します。このソリューションにより、ACE は他のネットワークに対するゲートウェイになる必要がないので、ルーティングが簡素化されます。ただし、この方式は、変換に使用できるアドレス数に制限があります。



---

(注) NAT または PAT には、グローバル インターフェイスの IP アドレスを使用できません。

---

- 固有のネットワーク上のアドレス - グローバル インターフェイス ネットワーク上で使用できる数より多くのアドレスが必要な場合、別のサブネット上のアドレスを指定できます。ACE は、プロキシ ARP を使用して変換されたアドレス要求に回答し、ローカル アドレス宛でのトラフィックを代行受信します。ACE で変換されたアドレス宛でのトラフィックを送信するアップストリーム ルータ上でスタティック ルートを追加する必要があります。

サブネット上でグローバル IP アドレス範囲は設定できません。たとえば、次のコマンド (**nat-pool 2 10.0.6.1 10.0.7.20 netmask 255.255.255.0**) は許可されず、無効な IP アドレス エラーが生成されます。

NAT プールを設定するときに、ネットマスクを設定する必要があります。ネットマスク 255.255.255.255 は、ACE にその範囲の IP アドレスをすべて使用させます。



# NAT のアイドル タイムアウトの設定

コンフィギュレーション モードで **timeout xlate** コマンドを使用すると、NAT のアイドル タイムアウトを設定できます。このコマンドの構文は次のとおりです。

**timeout xlate seconds**

*number* 引数には、60 ~ 2147483 の整数を指定します。デフォルトは 10800 秒 (3 時間) です。*seconds* 値は、Xlate スロットがアイドルになってから解放されるまで ACE が待つ時間を決定します。

たとえば、アイドル タイムアウトを 120 秒 (2 分) を指定するには、次のように入力します。

```
host1/Admin(config)# timeout xlate 120
```

NAT アイドル タイムアウトをデフォルト値の 10800 秒に戻すには、次のように入力します。

```
host1/Admin(config)# no timeout xlate 120
```

## ダイナミック NAT および PAT の設定

ここでは、SNAT 用に、ACE でダイナミック NAT および PAT を設定する方法について説明します。ダイナミック NAT、およびダイナミック PAT の概要については、「[NAT の概要](#)」を参照してください。このセクションの内容は、次のとおりです。

- [ダイナミック NAT および PAT の設定のクイック スタート](#)
- [ACL の設定](#)
- [ダイナミック NAT および PAT のインターフェイス設定](#)
- [NAT のグローバル IP アドレス プールの作成](#)
- [クラス マップの設定](#)
- [パッシブ FTP 用のクラス マップの設定](#)
- [ポリシー マップの設定](#)
- [ダイナミック NAT および PAT のレイヤ 3 とレイヤ 4 ポリシー マップアクションとしての設定](#)

- サービス ポリシーを使用したダイナミック NAT および PAT ポリシー マップのインターフェイスへ適用

## ダイナミック NAT および PAT の設定のクイック スタート

表 5-1 に、ダイナミック NAT および PAT の設定に必要なステップの概要を示します。各ステップには CLI、または作業を完了するのに必要な手順の参照が含まれます。CLI コマンドに関連した各機能すべてのオプションの詳細については、次の表 5-1 を参照してください。

表 5-1                   ダイナミック NAT および PAT の設定のクイック スタート

---

### 作業内容とコマンドの例

---

1. 複数のコンテキストで操作している場合、対象のコンテキストで操作しているかどうかを CLI プロンプトを確認します。必要に応じて、正しいコンテキストに変更します。

```
host1/Admin# changeto C1
host1/C1#
```

他に特に指定がなければ、この表の残りの例では C1 ユーザ コンテキストを使用します。コンテキストの作成方法の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

---

2. コンフィギュレーション モードを開始します。

```
host1/C1# config
host1/C1(config)#
```

---

3. NAT を必要とするトラフィックを許可するよう ACL を設定します。

```
host1/C1(config)# access-list NAT_ACCESS extended permit tcp
192.168.12.0 255.255.255.0 172.27.16.0 255.255.255.0 eq 80
host1/C1(config-acl)# exit
```

---

4. NAT を必要とするトラフィックを受信するように、ローカルインターフェイス (クライアント インターフェイス) を設定します。ACE がワナームードで動作している場合は、このステップを省略します。

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1500
host1/C1(config-if)# ip address 192.168.12.100 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit
```

---

表 5-1 ダイナミック NAT および PAT の設定のクイック スタート (続き)

---

**作業内容とコマンドの例**

---

5. グローバル IP アドレス プールについて 2 番目のインターフェイス (サーバ インターフェイス) を設定します。

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# mtu 1500
host1/C1(config-if)# ip address 172.27.16.2 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit
```

---

6. クラス マップを設定し、クライアント送信元アドレスのステップ 3 で設定した ACL の一致ステートメントを定義します。

```
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)# match access-list NAT_ACCESS
host1/C1(config-cmap)# exit
```

---

7. ポリシー マップを設定し、クラス マップをポリシー マップに関連付けます。

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

---

8. ダイナミック NAT をポリシー マップ アクションとして設定します。

```
host1/C1(config-pmap-c)# nat dynamic 1 vlan 200
host1/C1(config-pmap-c)# exit
host1/C1(config-pmap)# exit
```

---

9. サービス ポリシーを使用して、インターフェイス上でポリシーを起動します。ACE がワンアーム モードで動作している場合、ステップ 10 で指定したインターフェイスに **service-policy** コマンドを使用します。

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# service-policy input NAT_POLICY
host1/C1(config-if)# ctrl-z
```

---

10. サーバ インターフェイスに NAT プールを設定します。ダイナミック PAT を設定するには、**nat-pool** コマンドに **pat** キーワードを含めます。

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.41 netmask
255.255.255.0 pat
host1/C1(config-if)# Ctrl-Z
```

---

表 5-1 ダイナミック NAT および PAT の設定のクイック スタート (続き)

**作業内容とコマンドの例**

11. (任意) 設定の変更内容をフラッシュ メモリに保存します。

```
host1/Admin# copy running-config startup-config
```

12. ダイナミック NAT および PAT の設定を表示して、確認します。

```
host1/C1# show running-config class-map
host1/C1# show running-config policy-map
host1/C1# show running-config service-policy
```

## ACL の設定

セキュリティ ACL を使用して、NAT を必要とするトラフィックを許可できます。ACL の設定については、第 1 章「[セキュリティ アクセス コントロール リストの設定](#)」を参照してください。

ダイナミック NAT に ACL を設定するには、コンフィギュレーション モードで **access-list** コマンドを使用します。このコマンドの構文は次のとおりです。

```
access-list name [line number] extended {deny | permit}
  {protocol} {src ip_address netmask | any | host src ip_address}
  [operator port1 [port2]] {dest ip_address netmask | any | host
  dest_ip_address} [operator port3 [port4]]
```

たとえば、次のように入力します。

```
host1/C1(config)# access-list NAT_ACCESS extended permit tcp
192.168.12.0 255.255.255.0 172.27.16.0 255.255.255.0 eq 80
```

設定から ACL を削除するには、次のように入力します。

```
host1/C1(config)# no access-list NAT_ACCESS
```

## ダイナミック NAT および PAT のインターフェイス設定

クライアントのインターフェイスと、実サーバのインターフェイスを設定します。ACE がワンアーム モードで動作している場合、クライアントのインターフェイスは設定しないでください。詳細については、『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』を参照してください。

## NAT のグローバル IP アドレス プールの作成

ダイナミック NAT は指定したグローバル IP アドレスのプールを使用します。PAT が設定されたサーバを区別するため、そのサーバのグループの単一グローバル IP アドレスを定義するか、ダイナミック NAT のみを使用するときにグローバル IP アドレス範囲を定義できます。単一の IP アドレスまたはアドレス範囲を使用するには、ID をアドレス プールに割り当てます。サーバ VLAN インターフェイス上に NAT プールを設定します。



(注)

パケットが、NAT 用に設定していないインターフェイスを出力する場合、ACE はパケットを変換せずに送信します。

ダイナミック NAT の IP アドレスのプールを作成するには、インターフェイス コンフィギュレーション モードで **nat-pool** コマンドを使用します。このコマンドの構文は次のとおりです。

```
nat-pool pool_id ip_address1 [ip_address2] netmask mask [pat]
```

キーワード、引数、およびオプションは次のとおりです。

- *pool\_id* - グローバル IP アドレスの NAT プールの ID。1 ~ 2147483647 の整数を入力します。



(注)

同じ ID の NAT プールを複数設定する場合、ACE は最後に設定された NAT プールを使用してから、他の NAT プールを使用します。

- *ip\_address1* - NAT に使用する単一の IP アドレス。または *ip\_address2* 引数を使用する場合は、グローバル アドレス範囲の最初の IP アドレス。ドット付き 10 進表記で IP アドレスを入力します (たとえば、172.27.16.10)。
- *ip\_address2* - (任意) NAT に使用するグローバル IP アドレス範囲の最上位 IP アドレス。ドット付き 10 進表記で IP アドレスを入力します (たとえば、172.27.16.109)。NAT プールで最大 64 K アドレスを設定できます。

PAT を指定する場合、NAT プール範囲で最大 32 の IP アドレスを設定できます。サブネット上で IP アドレス範囲は設定できません。たとえば、次のコマンド (**nat-pool 2 10.0.6.1 10.0.7.20 netmask 255.255.255.0**) は許可されず、無効な IP アドレス エラーが生成されます。



(注) ACE では、ダイナミック NAT とダイナミック PAT に使用する NAT プールで仮想 IP (VIP) アドレスを設定することができます。このアクションは、VIP アドレスを使用して NAT の実サーバを起点とする接続 (クライアントに接続) を使用する場合に利用できます。この機能は、クライアント側ネットワークの実 IP アドレスの数に制限がある場合に特に便利です。送信元アドレスを同じ IP アドレス (VIP) に変換されている複数の実サーバで PAT を実行する場合は、**nat-pool** コマンドで **pat** キーワードを設定する必要があります。

- **netmask mask** - IP アドレス プールのサブネット マスクを指定します。ドット付き 10 進表記でマスクを入力します (たとえば、255.255.255.255)。ネットワーク マスク 255.255.255.255 では、ACE に指定された範囲の IP アドレスが使用できます。
- **pat** - (任意) ACE が NAT のほかに PAT を実行するよう指定します。

ACE が NAT プールの IP アドレスを消費したとき、PAT 規則が設定されていれば、この規則に切り替わります。たとえば、次のように設定できます。

```
host1/Admin(config-if)# nat-pool 1 10.1.100.10 10.1.100.99 netmask
255.255.255.255
host1/Admin(config-if)# nat-pool 1 10.1.100.100 10.1.100.100 netmask
255.255.255.255 pat
```

ネットワーク設定に次の条件がある場合、プールごとに単一の IP アドレスを複数の PAT プールに設定する必要があります。

- トラフィックは同じ送信元 IP アドレスから着信します。
- 送信元ポートの範囲は 1 ~ 64000 です。
- 1 つの宛先ポートから複数の宛先アドレスに送られます。
- 1 つの PAT プール内のすべてのポートが使用されます。

次を設定するのではなく、

```
host1/Admin(config-if)# nat-pool 1 3.3.3.3 3.3.3.5 netmask
255.255.255.255 pat
```

次を設定します。

```
host1/Admin(config-if)# nat-pool 1 192.161.12.3 netmask
255.255.255.255 pat
```

```
host1/Admin(config-if)# nat-pool 1 192.161.12.4 netmask
255.255.255.255 pat
```

```
host1/Admin(config-if)# nat-pool 1 192.161.12.5 netmask  
255.255.255.255 pat
```

設定範囲 32 (PAT プールごとの IP アドレスの最大数) のグローバル IP アドレスで構成された NAT プールに PAT を設定するには、次のように入力します。

```
host1/C1(config)# interface vlan 200  
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.41 netmask  
255.255.255.255 pat
```



(注)

インターフェイスから NAT プールを削除する前に、NAT プールに関連付けられたサービス ポリシーとポリシー マップを削除する必要があります。

設定から NAT プールを削除するには、次のように入力します。

```
host1/C1(config-if)# no nat-pool 1
```

## クラス マップの設定

コンフィギュレーション モードで **class-map** コマンドを使用すると、ダイナミック NAT および PAT にトラフィック クラスを設定できます。クラス マップの詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

このコマンドの構文は次のとおりです。

### **class-map match-any name**

*name* 引数には、クラス マップに対する UID を指定します (64 文字までの英数字で、引用符が含まれないテキスト文字列により指定)。

たとえば、次のように入力します。

```
host1/C1(config)# class-map match-any NAT_CLASS  
host1/C1(config-cmap)#
```

設定からクラス マップを削除するには、次のように入力します。

```
host1/C1(config)# no class-map match-any NAT_CLASS
```

ACL の一致基準を入力するか、クラス マップ コンフィギュレーション モードで **match** コマンドを使用してクライアント送信元アドレスを入力します。たとえば、次のように入力します。

## ■ ダイナミック NAT および PAT の設定

```
host1/C1(config-cmap)# match access-list NAT_ACCESS
```

または

```
host1/C1(config-cmap)# match source-address 192.168.12.15
255.255.255.0
```

クラス マップから一致ステートメントを削除するには、次のように入力します。

```
host1/C1(config-cmap)# no match access-list NAT_ACCESS
```

## パッシブ FTP 用のクラス マップの設定

送信元 NAT でパッシブ FTP を使用している場合は、送信元 NAT への追加のクラス マップをパッシブ データ接続に設定する必要があります。その後で、このクラス マップをレイヤ 4 マルチマッチ ポリシーに関連付け、**nat dynamic** コマンドをこのクラス マップ下のポリシー マップ アクションとして設定します。パッシブ FTP 用のクラス マップを設定するには、次のコマンドを入力します。

```
host1/C1(config)# class-map match-any FTP_NAT_CLASS
host1/C1(config-cmap)# match virtual address 172.16.35.37 any
```

## ポリシー マップの設定

コンフィギュレーション モードで **policy-map** コマンドを使用すると、ダイナミック NAT および PAT にトラフィック ポリシーを設定できます。ポリシー マップの詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

このコマンドの構文は次のとおりです。

```
policy-map multi-match name
```

**name** 引数は、ポリシー マップに割り当てられた名前です。「"」記号で囲わずに、最大 64 文字までの英数字でスペースを入れずにテキスト文字列を入力します。

たとえば、次のように入力します。

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)#
```

設定からポリシー マップを削除するには、次のように入力します。

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```



事前に作成されたクラス マップとポリシー マップを関連付けます。たとえば、次のように入力します。

```
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

ポリシー マップとクラス マップの関連付けを解除するには、次のように入力します。

```
host1/C1(config-pmap)# no class NAT_CLASS
```

必要に応じてポリシー マップ アクションを設定します。たとえば、次のように設定します。

```
host1/C1(config-pmap-c)# loadbalance policy L7_POLICY
host1/C1(config-pmap-c)# loadbalance VIP inservice
```

パッシブ FTP の場合は、FTP\_NAT\_CLASS クラス マップ（「[パッシブ FTP 用のクラス マップの設定](#)」を参照）をレイヤ 4 ポリシー マップに関連付けます。たとえば、ポリシー マップ コンフィグレーション モードで次のコマンドを入力します。

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)# class FTP_NAT_CLASS
```

次のセクションに進んで、**nat dynamic** コマンドをパッシブ FTP を使用する場合の FTP クラス マップ下のポリシー アクションとして設定します。または、**nat dynamic** コマンドを NAT\_CLASS クラス マップ下のポリシー アクションとして設定します。

## ダイナミック NAT および PAT のレイヤ 3 とレイヤ 4 ポリシー マップ アクションとしての設定

ポリシー マップ クラス コンフィギュレーション モードで **nat dynamic** コマンドを使用すると、ダイナミック NAT および PAT (SNAT) をレイヤ 3 とレイヤ 4 のポリシー マップ アクションとして設定できます。ACE は、トラフィック ポリシーに適用するインターフェイスから (**service-policy** インターフェイス コンフィギュレーション コマンドを介して)、**nat** コマンドで指定されたインターフェイスへダイナミック NAT を適用します。ワンアーム モードで動作している場合、使用する インターフェイスは 1 つの VLAN だけです。

このコマンドの構文は次のとおりです。

```
nat dynamic pool_id vlan number
```

## ■ ダイナミック NAT および PAT の設定

キーワード、引数、およびオプションは次のとおりです。

- **dynamic pool\_id** - 指定された VLAN で **nat-pool** コマンドを使用して設定された IP アドレスのグローバル プールの ID を示します (「[NAT のグローバル IP アドレス プールの作成](#)」を参照)。ダイナミック NAT は、ローカル送信元 IP アドレスのグループを宛先ネットワークでルーティング可能なグローバル IP アドレスのプールに変換します。トラフィック ポリシーに適用されたインターフェイスを出力するすべてのパケットには、グローバル プールで使用できるアドレスの 1 つに変換された送信元アドレスがあります。1 ~ 2147483647 の整数を入力します。
- **vlan number** - グローバル IP アドレスのサービインターフェイスを指定します。このインターフェイスは、ネットワーク デザインがワンアーム モードで動作している場合を除き、NAT が必要なトラフィックのフィルタリング および受信を行う場合に ACE で使用するインターフェイスとは別のものではないと見なされません。この場合、VLAN 番号は同じになります。



(注)

パケットが、NAT 用に設定していないインターフェイスを出力する場合、ACE はパケットを変換せずに送信します。

次の例では、**nat** コマンドをダイナミック NAT の レイヤ 3 および 4 のポリシー マップ アクションとして指定します。

```
host1/C1(config)# policy-map multi-action NAT_POLICY
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)# nat dynamic 1 vlan 200
```

ポリシー マップからダイナミック NAT アクションを削除するには、次のように入力します。

```
host1/C1(config-pmap-c)# no nat dynamic 1 vlan 200
```

## サービス ポリシーを使用したダイナミック NAT および PAT ポリシー マップのインターフェイスへ適用

インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用すると、ダイナミック NAT および PAT ポリシーマップを起動して、インターフェイスに関連付けることができます。 **service-policy** コマンドの詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

**(注)**

ダイナミック NAT は、入力サービス ポリシーとしてのみ設定できます。出力サービス ポリシーとしては設定できません。同じ NAT ポリシーを、ローカルおよびグローバルの両方には適用できません。

このコマンドの構文は次のとおりです。

```
service-policy input policy_name
```

キーワードと引数は次のとおりです。

- **input - VLAN** インターフェイスの入力方向に接続する（適用する）トラフィック ポリシーを指定します。トラフィック ポリシーは、インターフェイスが受信するすべてのトラフィックを評価します。
- **policy\_name** - 事前に定義されたポリシー マップの名前。名前には、64 文字までの英数字を指定できます。

たとえば、サービス ポリシーを特定のインターフェイスに適用するには、次のように入力します。

```
host1/C1(config)# interface vlan 100  
host1/C1(config-if)# mtu 1700  
host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0  
host1/C1(config-if)# service-policy input NAT_POLICY
```

サービス ポリシーをコンテキストのインターフェイスすべてにグローバルに適用するには、次のように入力します。

```
host1/C1(config)# service-policy input NAT_POLICY
```

インターフェイスからサービス ポリシーを削除するには、次のように入力します。

```
host1/C1(config-if)# no service-policy input NAT_POLICY
```

サービス ポリシーをコンテキストのすべてのインターフェイスからグローバルに削除するには、次のように入力します。

```
host1/C1(config)# no service-policy input NAT_POLICY
```

**(注)**

サービス ポリシーを適用した最後の VLAN インターフェイスからトラフィック ポリシーを個別に削除したり、同じコンテキストのすべての VLAN インターフェイスからトラフィック ポリシーをグローバルに削除した場合、ACE は関連付けられているサービス ポリシー統計情報を自動的にリセットします。この動作は、次回、トラフィック ポリシーを特定の VLAN インターフェイスに付加し

たり、同じコンテキストのすべての VLAN インターフェイスにグローバルに付加したりする場合には、ACE でサービス ポリシー統計情報に新しい開始ポイントを提供します。

---

## サーバファームベースのダイナミック NAT の設定

ここでは、SNAT 用に、ACE でファームベースのダイナミック NAT を設定する方法について説明します。サーバファームベースのダイナミック NAT の設定については、「[NAT の概要](#)」を参照してください。このセクションの内容は、次のとおりです。

- [サーバファームベースのダイナミック NAT 設定のクイックスタート](#)
- [サーバファームベースのダイナミック NAT への ACL の設定](#)
- [サーバファームベースのダイナミック NAT へのインターフェイスの設定](#)
- [ダイナミック NAT のグローバル IP アドレス プールの作成](#)
- [実サーバとサーバファームの設定](#)
- [サーバファームベースのダイナミック NAT へのレイヤ 7 ロードバランシングのクラスマップの設定](#)
- [サーバファームベースのダイナミック NAT へのレイヤ 7 ロードバランシングのポリシーマップの設定](#)
- [サーバファームベースのダイナミック NAT のレイヤ 7 ポリシーアクションとしての設定](#)
- [サーバファームベースのダイナミック NAT へのレイヤ 3 およびレイヤ 4 クラスマップの設定](#)
- [サーバファームベースのダイナミック NAT へのレイヤ 3 およびレイヤ 4 ポリシーマップの設定](#)
- [サービスポリシーを使用したレイヤ 3 およびレイヤ 4 ポリシーマップのインターフェイスへの適用](#)

## サーバファーム ベースのダイナミック NAT 設定のクイックスタート

表 5-2 に、サーバファーム ベースのダイナミック NAT の設定に必要な手順の簡単な概要を示します。各ステップには CLI、または作業を完了するのに必要な手順の参照が含まれます。CLI コマンドに関連した各機能すべてのオプションの詳細については、次の表 5-2 を参照してください。

表 5-2 サーバファーム ベースのダイナミック NAT 設定のクイックスタート

---

### 作業内容とコマンドの例

---

1. 複数のコンテキストで操作している場合、対象のコンテキストで操作しているかどうかを CLI プロンプトを確認します。必要に応じて、正しいコンテキストに変更します。

```
host1/Admin# changeto C1  
host1/C1#
```

他に特に指定がなければ、この表の残りの例では C1 ユーザ コンテキストを使用します。コンテキストの作成方法の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

2. コンフィギュレーション モードを開始します。

```
host1/C1# config  
host1/C1(config)#
```

3. NAT を必要とするトラフィックを許可するよう ACL を設定します。

```
host1/C1(config)# access-list ACL1 line 10 extended permit tcp  
10.0.0.0 255.0.0.0 eq 8080 any  
host1/C1(config-acl)# exit
```

---

表 5-2 サーバファーム ベースのダイナミック NAT 設定のクイック スタート

---

**作業内容とコマンドの例**


---

4. ロード バランシング用に実サーバとサーバファームを設定します。ステップ 9 の **nat dynamic** コマンドは、このサーバファームを参照します。

```

host1/C1(config)# rserver SERVER1
host1/C1(config-rserver-host)# ip address 172.27.16.201
host1/C1(config-rserver-host)# active
host1/C1(config-rserver-host)# exit
host1/C1(config)# rserver SERVER2
host1/C1(config-rserver-host)# ip address 172.27.16.202
host1/C1(config-rserver-host)# active
host1/C1(config-rserver-host)# exit
host1/C1(config)# serverfarm SF1
host1/C1(config-sfarm-host)# rserver SERVER1 3000
host1/C1(config-sfarm-host-rs)# active
host1/C1(config-sfarm-host-rs)# exit
host1/C1(config-sfarm-host)# rserver SERVER2 3001
host1/C1(config-sfarm-host-rs)# active
host1/C1(config-sfarm-host-rs)# exit
host1/C1(config-sfarm-host)# exit

```

5. クライアント トラフィックのフィルタリングと受信が行えるように、ローカル インターフェイス (クライアント VLAN) を設定します。ACE がワナアーム モードで動作している場合は、このステップを省略します。

```

host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1500
host1/C1(config-if)# ip address 192.168.12.100 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit

```

6. NAT プールについて 2 番めのインターフェイス (サーバ VLAN) を設定します。

```

host1/C1(config)# interface vlan 200
host1/C1(config-if)# mtu 1500
host1/C1(config-if)# ip address 172.27.16.200 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit

```

7. レイヤ 7 ロード バランシングのクラス マップを設定し、一致基準を定義します。

```

host1/C1(config)# class-map type http loadbalance match-any
L7_CLASS
host1/C1(config-cmap-http-lb)# match http content .*cisco.com

```

---

表 5-2 サーバファーム ベースのダイナミック NAT 設定のクイック スタート

---

**作業内容とコマンドの例**

---

8. レイヤ 7 ロード バランシングのポリシー マップを設定し、クラス マップをポリシー マップに関連付けます。

```
host1/C1(config)# policy-map type loadbalance http first-match  
L7_POLICY  
host1/C1(config-pmap-lb)# class L7_CLASS  
host1/C1(config-pmap-lb-c)#
```

---

9. レイヤ 7 ロード バランシング ポリシーのポリシー マップ アクションとして、サーバファーム ベースのダイナミック NAT を設定します。各プライマリおよびバックアップのサーバファーム、および発信側サーバ VLAN ごとに、このコマンドの複数のインスタンスを設定できます。

```
host1/C1(config-pmap-lb-c)# nat dynamic 1 vlan 200 serverfarm  
primary  
host1/C1(config-pmap-lb-c)# exit  
host1/C1(config-pmap-lb)# exit  
host1/C1(config)#
```

---

10. レイヤ 3 および レイヤ 4 のクラス マップを設定し、一致基準を定義します。

```
host1/C1(config)# class-map match-any SLB_CLASS  
host1/C1(config-cmap)# match virtual-address 172.16.27.52 tcp eq  
http  
host1/C1(config-cmap)# exit
```

---

11. レイヤ 3 およびレイヤ 4 のポリシー マップを設定し、クラス マップをポリシー マップに関連付けます。

```
host1/C1(config)# policy-map multi-match SLB_POLICY  
host1/C1(config-pmap)# class SLB_CLASS  
host1/C1(config-pmap-c)#
```

---

12. レイヤ 3 およびレイヤ 4 のポリシー マップ アクションを設定します。

```
host1/C1(config-pmap-c)# loadbalance policy L7_POLICY  
host1/C1(config-pmap-c)# loadbalance vip inservice  
host1/C1(config-pmap-c)# exit  
host1/C1(config-pmap)# exit  
host1/C1(config)#
```

---

13. サービス ポリシーを使用して、インターフェイス上でポリシーを起動します。ACE がワンアーム モードで動作している場合、ステップ 14 で指定したインターフェイスに **service-policy** コマンドを使用します。

```
host1/C1(config)# interface vlan 100  
host1/C1(config-if)# service-policy input SLB_POLICY  
host1/C1(config-if)# exit
```

---

表 5-2 サーバファーム ベースのダイナミック NAT 設定のクイック スタート

---

**作業内容とコマンドの例**

---

14. サーバ インターフェイスに NAT プールを設定します。

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.26.49
255.255.255.0
host1/C1(config-if)# Ctrl-Z
```

---

15. (任意) 設定の変更内容をフラッシュ メモリに保存します。

```
host1/Admin# copy running-config startup-config
```

---

16. サーバファーム ベースのダイナミック NAT の設定を表示して、確認します。

```
host1/C1# show running-config class-map
host1/C1# show running-config policy-map
host1/C1# show running-config service-policy
```

---



## サーバファーム ベースのダイナミック NAT への ACL の設定

アクセス制御リスト (ACL) を使用して、NAT を必要とするトラフィックを許可します。ACL の設定については、第 1 章「セキュリティ アクセス コントロール リストの設定」を参照してください。

ダイナミック NAT に ACL を設定するには、コンフィギュレーション モードで **access-list** コマンドを使用します。このコマンドの構文は次のとおりです。

```
access-list name [line number] extended {deny | permit}
    {protocol} {src_ip_address netmask | any | host src_ip_address}
    [operator port1 [port2]] {dest_ip_address netmask | any | host
    dest_ip_address} [operator port3 [port4]]
```

たとえば、次のように入力します。

```
host1/C1(config)# access-list NAT_ACCESS extended permit tcp
192.168.12.0 255.255.255.0 172.27.16.0 255.255.255.0 eq 80
```

設定から ACL を削除するには、次のように入力します。

```
host1/C1(config)# no access-list nat_access
```

## サーバファーム ベースのダイナミック NAT へのインターフェイスの設定

クライアントのインターフェイスと、実サーバのインターフェイスを設定します。ACE がワンアーム モードで動作している場合は、クライアントインターフェイスは省略します。インターフェイスの設定の詳細については『Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide』を参照してください。

## ダイナミック NAT のグローバル IP アドレス プールの作成

ダイナミック NAT は指定したグローバル IP アドレスのプールを使用します。ダイナミック NAT を使用する場合、グローバル IP アドレスの範囲を定義することができます。アドレス範囲を使用するには、アドレス プールに ID を割り当てます。次に、NAT プールと サーバの VLAN インターフェイスを関連付けます。



(注) パケットが、NAT 用に設定していないインターフェイスを出力する場合、ACE はパケットを変換せずに送信します。

ダイナミック NAT の IP アドレスのプールを作成するには、インターフェイス コンフィギュレーション モードで **nat-pool** コマンドを使用します。このコマンドの構文は次のとおりです。

```
nat-pool pool_id ip_address1 ip_address2 netmask mask
```

キーワード、引数、およびオプションは次のとおりです。

- *pool\_id* - グローバル IP アドレスの NAT プールの ID。1 ~ 2147483647 の整数を入力します。



(注) 同じ ID の NAT プールを複数設定する場合、ACE は最後に設定された NAT プールを使用してから、他の NAT プールを使用します。

- *ip\_address1* - NAT に使用する単一の IP アドレス。または *ip\_address2* 引数を使用する場合は、グローバルアドレス範囲の最初の IP アドレス。ドット付き 10 進表記で IP アドレスを入力します (たとえば、172.27.16.10)。
- *ip\_address2* - NAT に使用するグローバル IP アドレス範囲の最上位 IP アドレス。ドット付き 10 進表記で IP アドレスを入力します (たとえば、172.27.16.26)。NAT プールで最大 64 K アドレスを設定できます。

サブネット上で IP アドレス範囲は設定できません。たとえば、次のコマンド (**nat-pool 2 10.0.6.1 10.0.7.20 netmask 255.255.255.0**) は許可されず、無効な IP アドレス エラーが生成されます。



(注) ACE では、ダイナミック NAT に使用する NAT プールで仮想 IP (VIP) アドレスを設定することができます。このアクションは、VIP アドレスを使用して NAT の実サーバを起点とする接続 (クライアントに接続) を使用する場合に利用できます。この機能は、クライアント側ネットワークの実 IP アドレスの数に制限がある場合に特に便利です。

- **netmask mask** - IP アドレス プールのサブネット マスクを指定します。ドット付き 10 進表記でマスクを入力します（たとえば、255.255.255.255）。ネットワーク マスク 255.255.255.255 では、ACE に指定された範囲の IP アドレスが使用できます。

32 のグローバル IP アドレスを含む範囲からなる NAT プールを設定するには、次のように入力します。

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.41 netmask
255.255.255.255
```



(注)

インターフェイスから NAT プールを削除する前に、NAT プールに関連付けられたサービス ポリシーとポリシー マップを削除する必要があります。

設定から NAT プールを削除するには、次のように入力します。

```
host1/C1(config-if)# no nat-pool 1
```

## 実サーバとサーバファームの設定

実サーバとサーバファームの設定については、『Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide』を参照してください。

## サーバファーム ベースのダイナミック NAT へのレイヤ 7 ロード バランシングのクラス マップの設定

コンフィギュレーション モードで **class-map** コマンドを使用すると、サーバファーム ベースのダイナミック NAT にレイヤ 7 トラフィック クラスを設定できます。このコマンドの構文は次のとおりです。

```
class-map type http loadbalance match-any name
```

*name* 引数には、クラス マップに対する UID を指定します（64 文字までの英数字で、引用符が含まれないテキスト文字列により指定）。

たとえば、次のように入力します。

```
host1/C1(config)# class-map type http loadbalance match-any L7_CLASS
host1/C1(config-cmap-http-lb)#
```

設定からクラス マップを削除するには、次のように入力します。

```
host1/C1(config)# no class-map type http loadbalance match-any  
L7_CLASS
```

必要に応じて、クラス マップ ロード バランシング コンフィギュレーション モードで **match** コマンドを使用して一致基準を入力します。たとえば、次のように入力します。

```
host1/C1(config-cmap-http-lb)# match http content .*cisco.com
```

クラス マップから一致ステートメントを削除するには、次のように入力します。

```
host1/C1(config-cmap-http-lb)# no match http content .*cisco.com
```

## サーバファーム ベースのダイナミック NAT へのレイヤ 7 ロード バランシングのポリシー マップの設定

コンフィギュレーション モードで **policy-map** コマンドを使用すると、レイヤ 7 ロード バランシングのポリシー マップを設定できます。このコマンドの構文は次のとおりです。

**policy-map type loadbalance http first-match *name***

*name* 引数には、既存のポリシー マップに対する UID を指定します (64 文字までの英数字で、引用符が含まれないテキスト文字列により指定)。

たとえば、次のように入力します。

```
host1/C1(config)# policy-map type loadbalance http first-match  
L7_POLICY  
host1/C1(config-pmap-lb)#
```

設定からポリシー マップを削除するには、次のように入力します。

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```

事前に作成されたクラス マップとポリシー マップを関連付けます。たとえば、次のように入力します。

```
host1/C1(config-pmap-lb)# class L7_CLASS  
host1/C1(config-pmap-lb-c)#
```

ポリシー マップとクラス マップの関連付けを解除するには、次のように入力します。

```
host1/C1(config-pmap-lb)# no class L7_CLASS
```

## サーバファーム ベースのダイナミック NAT のレイヤ 7 ポリシー アクションとしての設定

ポリシー マップ ロード バランシング クラスのコンフィギュレーション モードで **nat** コマンドを使用すると、サーバファーム ベースのダイナミック NAT をレイヤ 7 ロード バランシング ポリシー マップのアクションとして設定できます。通常、ダイナミック NAT は SNAT 用に使用します。ダイナミック NAT を使用すると、クラス マップのトラフィック分類の一部として参照される拡張 ACL の送信元および宛先アドレスを指定することで、アドレス変換を行うローカルトラフィックを特定できます。ACE は、トラフィック ポリシーが適用されるインターフェイスのダイナミック NAT を、(**service-policy** インターフェイス コンフィギュレーション コマンドを介して)、**nat dynamic** コマンドで指定されたインターフェイスに適用します。

このコマンドの構文は次のとおりです。

```
nat dynamic pool_id vlan number serverfarm {primary | backup}
```

キーワードと引数は次のとおりです。

- **pool\_id** - グローバル IP アドレスの NAT プールの ID。1 ~ 2147483647 の整数を入力します。



(注) 同じ ID の NAT プールを複数設定する場合、ACE は最後に設定された NAT プールを使用してから、他の NAT プールを使用します。

- **vlan number** - グローバル IP アドレスのサーバインターフェイスを指定します。このインターフェイスは、ネットワーク デザインがワンアーム モードで動作している場合を除き、NAT が必要なトラフィックのフィルタリングおよび受信を行う場合に ACE で使用するインターフェイスとは別のものでなければなりません。この場合、VLAN 番号は同じになります。
- **serverfarm** - サーバファーム ベースのダイナミック NAT を指定します。

- **primary | backup** - プライマリ サーバファーム、またはバックアップサーバファームのいずれかにダイナミック NAT を適用します。



(注)

パケットが、NAT 用に設定していないインターフェイスを出力する場合、ACE はパケットを変換せずに送信します。

次の SNAT サーバファームベースのダイナミック NAT の例では、**nat** コマンドをレイヤ 7 ポリシー マップのアクションとして指定します。

```
host1/C1(config)# policy-map type loadbalance http first-match
L7_POLICY
host1/C1(config-pmap-lb)# class L7_CLASS
host1/C1(config-pmap-lb-c)# nat dynamic serverfarm primary 1 vlan 200
```

ポリシー マップからサーバファームベースダイナミック NAT アクションを削除するには、次のように入力します。

```
host1/C1(config-pmap-lb-c) no nat dynamic serverfarm primary 1
vlan 200
```

## サーバファームベースのダイナミック NAT へのレイヤ 3 およびレイヤ 4 クラス マップの設定

コンフィギュレーションモードで **class-map** コマンドを使用すると、サーバファームベースのダイナミック NAT にレイヤ 3 およびレイヤ 4 トラフィック クラスを設定できます。クラス マップの詳細については、『Cisco 4700 Series Application Control Engine Appliance Administration Guide』を参照してください。このコマンドの構文は次のとおりです。

**class-map match-any name**

**name** 引数には、クラス マップに対する UID を指定します (64 文字までの英数字で、引用符が含まれないテキスト文字列により指定)。

たとえば、次のように入力します。

```
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)#
```

設定からクラス マップを削除するには、次のように入力します。

```
host1/C1(config)# no class-map match-any NAT_CLASS
```

必要に応じて、クラス マップ コンフィギュレーション モードで **match** コマンドを使用して一致基準を入力します。たとえば、次のように入力します。

```
host1/C1(config-cmap)# match access-list NAT_ACCESS
```

または

```
host1/C1(config-cmap)# match source address 192.168.12.15
```

クラス マップから一致ステートメントを削除するには、次のように入力します。

```
host1/C1(config-cmap)# no match access-list NAT_ACCESS
```

## サーバファーム ベースのダイナミック NAT へのレイヤ 3 およびレイヤ 4 ポリシー マップの設定

コンフィギュレーション モードで **policy-map** コマンドを使用すると、レイヤ 3 およびレイヤ 4 トラフィック ポリシーを設定できます。ポリシー マップの詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

このコマンドの構文は次のとおりです。

### **policy-map multi-match name**

**name** 引数は、ポリシー マップに割り当てられた名前です。「"」記号で囲わずに、最大 64 文字までの英数字でスペースを入れずにテキスト文字列を入力します。

たとえば、次のように入力します。

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)#
```

設定からポリシー マップを削除するには、次のように入力します。

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```

事前に作成されたクラス マップとポリシー マップを関連付けます。たとえば、次のように入力します。

```
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

ポリシー マップとクラス マップの関連付けを解除するには、次のように入力します。

```
host1/C1(config-pmap)# no class NAT_CLASS
```

必要に応じてポリシー マップ アクションを設定します。たとえば、次のように設定します。

```
host1/C1(config-pmap-c)# loadbalance policy L7_POLICY
host1/C1(config-pmap-c)# loadbalance VIP inservice
```

## サービス ポリシーを使用したレイヤ 3 およびレイヤ 4 ポリシー マップのインターフェイスへの適用

インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用すると、サーバファーム ベース ダイナミック NAT ポリシーを起動して、インターフェイスに割り当てることができます。**service-policy** コマンドの詳細については、『Cisco 4700 Series Application Control Engine Appliance Administration Guide』を参照してください。



(注)

ダイナミック NAT は、入力サービス ポリシーとしてのみ設定できます。出力サービス ポリシーとしては設定できません。同じ NAT ポリシーを、ローカルおよびグローバルの両方には適用できません。

このコマンドの構文は次のとおりです。

```
service-policy input policy_name
```

キーワードと引数は次のとおりです。

- **input** - VLAN インターフェイスの入力方向に接続する（適用する）トラフィック ポリシーを指定します。トラフィック ポリシーは、インターフェイスが受信するすべてのトラフィックを評価します。
- **policy\_name** - 事前に定義されたポリシー マップの名前。名前には、64 文字までの英数字を指定できます。

たとえば、次のように入力します。

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1700
host1/C1(config-if)# ip address 192.168.12.100 255.255.255.0
host1/C1(config-if)# service-policy input NAT_POLICY
```

インターフェイスからサービス ポリシーを削除するには、次のように入力します。

```
host1/C1(config-if)# no service-policy input NAT_POLICY
```





(注)

サービス ポリシーを適用した最後の VLAN インターフェイスからトラフィック ポリシーを削除すると、ACE は関連するサービス ポリシーの統計情報を自動的にリセットします。ACE は、次にトラフィック ポリシーを特定の VLAN インターフェイスに適用するときに、サービス ポリシー統計情報の新しい開始ポイントを提供するため、このアクションを実行します。

## スタティック NAT とスタティック ポート リダイレクションの設定

ここでは、DNAT の ACE でスタティック NAT およびスタティック ポート リダイレクションを設定する方法について説明します。スタティック NAT およびスタティック ポート リダイレクションの概要については、「[NAT の概要](#)」を参照してください。このセクションの内容は、次のとおりです。

- [スタティック NAT の設定のクイック スタート](#)
- [スタティック NAT とスタティック ポート リダイレクション用 ACL の設定](#)
- [クラス マップの設定](#)
- [ポリシー マップの設定](#)
- [ポリシー アクションとしてのスタティック NAT およびスタティック ポート リダイレクションの設定](#)
- [サービス ポリシーを使用したスタティック NAT およびスタティック ポート リダイレクション ポリシー マップのインターフェイスへの適用](#)

### スタティック NAT の設定のクイック スタート

表 5-3 に、スタティック NAT およびスタティック ポート リダイレクションの設定に必要なステップの概要を示します。各ステップには CLI、または作業を完了するのに必要な手順の参照が含まれます。CLI コマンドに関連した各機能すべてのオプションの詳細については、次の表 5-3 を参照してください。

表 5-3 スタティック NAT の設定のクイック スタート

---

**作業内容とコマンドの例**


---

1. 複数のコンテキストで操作している場合、対象のコンテキストで操作しているかどうかを CLI プロンプトを確認します。必要に応じて、正しいコンテキストに変更します。

```
host1/Admin# changeto C1
host1/C1#
```

他に特に指定がなければ、この表の残りの例では C1 ユーザ コンテキストを使用します。コンテキストの作成方法の詳細については、『Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide』を参照してください。

---

2. コンフィギュレーション モードを開始します。

```
host1/C1# config
host1/C1(config)#
```

---

3. NAT を必要とするトラフィックを許可するよう ACL を設定します。

```
host1/C1(config)# access-list ACL1 line 10 extended permit tcp
10.0.0.0 255.0.0.0 eq 8080 any
host1/C1(config-acl)# exit
```

---

4. NAT を必要とするトラフィックをフィルタリングして受信するようローカル インターフェイスを設定します。

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1500
host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit
```

---

5. NAT を実行する 2 番目のインターフェイス（グローバル インターフェイス）を設定します。

```
host1/C1(config)# interface vlan 101
host1/C1(config-if)# mtu 1500
host1/C1(config-if)# ip address 172.27.16.100 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit
```

---

6. クラス マップを設定し、一致基準を定義します。

```
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)# match access-list ACL1
host1/C1(config-cmap)# exit
```

---

表 5-3 スタティック NAT の設定のクイック スタート (続き)

---

**作業内容とコマンドの例**

---

7. ポリシー マップを設定し、クラス マップをポリシー マップに関連付けます。

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

---

8. スタティック NAT をポリシー マップ アクションとして設定します。

```
host1/C1(config-pmap-c)# nat static 192.0.0.0 netmask 255.0.0.0
vlan 101
host1/C1(config-pmap-c)# exit
host1/C1(config-pmap)# exit
host1/C1(config)#
```

---

9. サービス ポリシーを使用して、インターフェイス上でポリシーを起動します。

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# service-policy input NAT_POLICY
host1/C1(config-if)# Ctrl-Z
```

---

10. (任意) 設定の変更内容をフラッシュ メモリに保存します。

```
host1/Admin# copy running-config startup-config
```

---

11. スタティック NAT とスタティック ポート リダイレクションの設定を表示し、確認します。

```
host1/C1# show running-config class-map
host1/C1# show running-config policy-map
```

---

## スタティック NAT とスタティック ポート リダイレクション用 ACL の設定

ACL を使用して、スタティック NAT とポート リダイレクションを必要とするトラフィックを許可します。ACL の設定については、第 1 章「セキュリティ アクセス コントロール リストの設定」を参照してください。

スタティック NAT に ACL を設定するには、コンフィギュレーション モードで **access-list** コマンドを使用します。このコマンドの構文は次のとおりです。

```
access-list name [line number] extended {deny | permit}
  {protocol} {src ip_address netmask | any | host src ip_address}
  [operator port1 [port2]] {dest ip_address netmask | any | host
  dest_ip_address} [operator port3 [port4]]
```

たとえば、次のように入力します。

```
host1/C1(config)# access-list acl1 line 10 extended permit tcp
10.0.0.0 255.0.0.0 eq 8080 any
```

設定から ACL を削除するには、次のように入力します。

```
host1/C1(config)# no access-list nat_access
```

## スタティック NAT とスタティック ポート リダイレクションへのインターフェイスの設定

クライアントのインターフェイスと、実サーバのインターフェイスを設定します。詳細については、『Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide』を参照してください。

## クラス マップの設定

コンフィギュレーション モードで **class-map** コマンドを使用すると、スタティック NAT およびポート リダイレクションにトラフィック クラスを設定できます。クラス マップの詳細については、『Cisco 4700 Series Application Control Engine Appliance Administration Guide』を参照してください。

このコマンドの構文は次のとおりです。

```
class-map match-any name
```

*name* 引数には、クラス マップに対する UID を指定します（64 文字までの英数字で、引用符が含まれないテキスト文字列により指定）。

たとえば、次のように入力します。

```
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)#
```

設定からクラス マップを削除するには、次のように入力します。

```
host1/C1(config)# no class-map match-any NAT_CLASS
```

必要に応じて、クラス マップ コンフィギュレーション モードで **match** コマンドを使用して一致基準を入力します。たとえば、次のように入力します。

```
host1/C1(config-cmap)# match access-list NAT_ACCESS
```

または

```
host1/C1(config-cmap)# match source address 192.168.12.15
```

クラス マップから一致ステートメントを削除するには、次のように入力します。

```
host1/C1(config-cmap)# no match access-list NAT_ACCESS
```

## ポリシー マップの設定

コンフィギュレーション モードで **policy-map** コマンドを使用すると、NAT にトラフィック ポリシーを設定できます。ポリシー マップの詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

このコマンドの構文は次のとおりです。

### **policy-map multi-match name**

*name* 引数は、ポリシー マップに割り当てられた名前です。「"」記号で囲わずに、最大 64 文字までの英数字でスペースを入れずにテキスト文字列を入力します。

たとえば、次のように入力します。

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)#
```

設定からポリシー マップを削除するには、次のように入力します。

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```

## ■ スタティック NAT とスタティック ポート リダイレクションの設定

事前に作成されたクラス マップとポリシー マップを関連付けます。たとえば、次のように入力します。

```
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

ポリシー マップとクラス マップの関連付けを解除するには、次のように入力します。

```
host1/C1(config-pmap)# no class NAT_CLASS
```

## ポリシー アクションとしてのスタティック NAT およびスタティック ポート リダイレクションの設定

ポリシー マップ クラス コンフィギュレーション モードで **nat static** コマンドを使用すると、スタティック NAT およびスタティック ポート リダイレクションをポリシー マップのアクションとして設定できます。一般的に、DNAT 用にスタティック NAT とポート リダイレクションを使用します。スタティック NAT を使用すると、拡張 ACL で送信元および宛先アドレスを指定することにより、アドレス変換を行うローカルトラフィックを特定できます。これは、クラス マップトラフィック分類の一部として参照されます。ACE は、トラフィック ポリシーに適用するインターフェイスから (**service-policy** インターフェイス コンフィギュレーション コマンドを介して)、**nat static** コマンドで指定されたインターフェイスへスタティック NAT を適用します。

このコマンドの構文は次のとおりです。

```
nat static ip_address netmask mask {port1 | tcp eq port2 | udp eq port3}
vlan number
```

キーワードと引数は次のとおりです。

- **static ip\_address** - 単一のスタティック変換を設定します。*ip\_address* 引数は、外部のような、グローバルに一意的なホストの IP アドレスを確立します。ポリシー マップは、ACL で指定された送信元 IP アドレスのグローバル IP アドレス変換を実行します (クラス マップトラフィック分類の一部として)。
- **netmask mask** - スタティック IP アドレス プールのサブネット マスクを指定します。ドット付き 10 進表記でマスクを入力します (たとえば、255.255.255.0)。
- *port1* - スタティック ポート リダイレクションのグローバル TCP または UDP ポート。0 ~ 65535 の整数を入力します。

- **tcp eq port2** - TCP ポートの名前または番号を指定します。0 ~ 65535 の整数を入力します。0 に設定すると、ACE はいずれのポートとも一致します。または、TCP ポート番号に相当するプロトコル キーワードを入力できます。サポートされている well-known TCP ポートの名前と番号のリストについては、表 5-4 を参照してください。

表 5-4 Well-known TCP ポート番号およびキーワード

キーワード	ポート番号	説明
ftp	21	File Transfer Protocol (FTP; ファイル転送プロトコル)
http	80	Hypertext Transfer Protocol (HTTP; ハイパーテキスト転送プロトコル)
https	443	HTTP over TLS/SSL
irc	194	Internet Relay Chat (IRC; インターネットリレー チャット)
matip-a	350	Mapping of Airline Traffic over Internet Protocol (MATIP) タイプ A
nntp	119	ネットワーク ニュース トランスポート プロトコル
pop2	109	POP v2
pop3	110	POP v3
rtsp	554	Real Time Streaming Protocol
smtp	25	Simple Mail Transfer Protocol (SMTP; シンプル メール転送プロトコル)
telnet	23	Telnet

- **udp eq port3** - UDP ポートの名前または番号を指定します。0 ~ 65535 の整数を入力します。0 に設定すると、ACE はいずれのポートとも一致します。または、UDP ポート番号に相当するプロトコル キーワードを入力できます。サポートされている well-known UDP ポートの名前と番号のリストについては、表 5-5 を参照してください。

表 5-5 Well-known UDP ポート番号およびキーワード

キーワード	ポート番号	説明
dns	53	Domain Name System (DNS; ドメイン ネーム システム)
wsp	9200	Connectionless Wireless Session Protocol (WSP)
wsp-wtls	9202	セキュアなコネクショレス型 WSP
wsp-wtp	9201	接続ベースの WSP
wsp-wtp-wtls	9203	セキュアな接続ベースの WSP

- **vlan number** - グローバル IP アドレスのインターフェイスを指定します。



(注)

パケットが、NAT 用に設定していないインターフェイスを出力する場合、ACE はパケットを変換せずに送信します。

次の DNAT スタティック ポート リダイレクションの例では、**nat static** コマンドをスタティック NAT ポリシー マップのアクションとして指定します。

```
host1/C1(config)# policy-map multi-action NAT_POLICY
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)# nat static 192.168.12.0 255.255.255.0 80
vlan 101
```

ポリシー マップから NAT アクションを削除するには、次のように入力します。

```
host1/C1(config-pmap-c) no nat static 192.168.12.15 255.255.255.0
vlan 200
```



## サービス ポリシーを使用したスタティック NAT およびスタティック ポート リダイレクション ポリシー マップのインターフェイスへの適用

インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用すると、スタティック NAT およびポート リダイレクション ポリシーを起動して、インターフェイスに割り当てることができます。 **service-policy** コマンドの詳細については、『Cisco 4700 Series Application Control Engine Appliance Administration Guide』を参照してください。



(注)

スタティック NAT は、入力サービス ポリシーとしてのみ設定できます。出力サービス ポリシーとしては設定できません。

このコマンドの構文は次のとおりです。

```
service-policy input policy_name
```

キーワードと引数は次のとおりです。

- **input - VLAN** インターフェイスの入力方向に接続する (適用する) トラフィック ポリシーを指定します。トラフィック ポリシーは、インターフェイスが受信するすべてのトラフィックを評価します。
- **policy\_name** - 事前に定義されたポリシー マップの名前。名前には、64 文字までの英数字を指定できます。

たとえば、次のように入力します。

```
host1/C1(config)# interface vlan 100  
host1/C1(config-if)# mtu 1700  
host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0  
host1/C1(config-if)# service-policy input NAT_POLICY
```

インターフェイスからサービス ポリシーを削除するには、次のように入力します。

```
host1/C1(config-if)# no service-policy input NAT_POLICY
```



(注)

サービス ポリシーを適用した最後の VLAN インターフェイスからトラフィック ポリシーを削除すると、ACE は関連するサービス ポリシーの統計情報を自動的にリセットします。ACE は、次にトラフィック ポリシーを特定の VLAN インターフェイスに適用するときに、サービス ポリシー統計情報の新しい開始ポイントを提供するため、このアクションを実行します。

# NAT の設定と統計情報の表示

ここでは、ダイナミックおよびスタティック NAT と PAT の設定および統計情報を表示する場合に使用するコマンドについて説明します。

- [NAT および PAT の設定の表示](#)
- [IP アドレスとポート変換の表示](#)

## NAT および PAT の設定の表示

EXEC モードで **show running-config class-map** コマンドおよび **show running-config policy-map** コマンドを使用すると、NAT および PAT の設定を表示できます。

たとえば、次のように入力します。

```
host1/C1# show running-config class-map
host1/C1# show running-config policy-map
```

## IP アドレスとポート変換の表示

EXEC モードで **show xlate** コマンドを使用すると、IP アドレスとポート変換 (Xlate) 情報を表示できます。このコマンドの構文は次のとおりです。

```
show xlate [global {ip_address1 [ip_address2 [netmask mask1]]}] [local
{ip_address3 [ip_address4 [netmask mask2]]}] [gport port1 [port2]]
[lport port1 [port2]]
```

キーワード、引数、およびオプションは次のとおりです。

- **global *ip\_address1 ip\_address2*** - (任意) ACE によるスタティックおよびダイナミック NAT の送信元アドレスの変換先のグローバル IP アドレス情報またはグローバル IP アドレス範囲の情報を表示します。単一のグローバル IP アドレスの場合、ドット付き 10 進表記でアドレスを入力します (たとえば、192.168.12.15)。IP アドレスの範囲を指定するには、2 番目の IP アドレスを入力します。
- **netmask *mask*** - (任意) 指定された IP アドレスのサブネット マスクを表示します。

- **local ip\_address3 ip\_address4** - (任意) ローカル IP アドレスまたはローカル IP アドレス範囲を表示します。単一のローカル IP アドレスの場合、ドット付き 10 進表記でアドレスを入力します (たとえば、192.168.12.15)。ローカル IP アドレスの範囲を指定するには、2 番めの IP アドレスを入力します。
- **gport port1 port2** - (任意) ACE によるスタティック ポートリダイレクションとダイナミック PAT それぞれの送信元ポートの変換先のグローバルポート情報またはグローバルポート範囲の情報を表示します。ポート番号として 0 ~ 65535 の整数を入力します。ポート番号の範囲を指定するには、2 番めのポート番号を入力します。
- **lport port3 port4** - (任意) ローカルポートおよびローカルポート範囲の情報を表示します。ポート番号として 0 ~ 65535 の整数を入力します。ポート番号の範囲を指定するには、2 番めのポート番号を入力します。

たとえば、次のように入力します。

```
host1/Admin# show xlate global 172.27.16.3 172.27.16.10 netmask  
255.255.255.0 gport 100 200
```

**show conn** コマンドを使用して NAT 情報を表示することもできます。次の例を参照してください。

このセクションの内容は、次のとおりです。

- [ダイナミック NAT の例](#)
- [ダイナミック PAT の例](#)
- [スタティック NAT の例](#)
- [スタティック ポートリダイレクション \(スタティック PAT\) の例](#)

## ダイナミック NAT の例

次の **show xlate** コマンドの出力例は、ダイナミック NAT を示します (この例では SNAT)。VLAN 2020 の 172.27.16.5 から Telnet を使用する場合、ACE はこれを VLAN 2021 の 192.168.100.1 に変換します。

```
host1/Admin# show xlate global 192.168.100.1 192.168.100.10  
NAT from vlan2020:172.27.16.5 to vlan2021:192.168.100.1 count:1
```

## ダイナミック PAT の例

次に、ダイナミック PAT の例を示します。VLAN 2020 の 172.27.16.5 から Telnet を使用する場合、ACE はこれを VLAN 2021 の 192.168.201.1 に変換します。

```
host1/Admin# show xlate
TCP PAT from vlan2020:172.27.16.5/38097 to vlan2021:192.168.201.1/1025
```

## スタティック NAT の例

次に、スタティック NAT の例を示します。ACE は実 IP アドレス (172.27.16.5) を 192.168.210.1 にマッピングします。

```
host1/Admin# show xlate
NAT from vlan2020:172.27.16.5 to vlan2021:192.168.210.1 count:1
```

```
host1/Admin# show conn
```

```
total current connections : 2
```

conn-id	dir	prot	vlan	source	destination	state
7	in	TCP	2020	172.27.16.5	192.168.100.1	ESTAB
6	out	TCP	2021	192.168.100.1	192.168.210.1	ESTAB

## スタティック ポート リダイレクション (スタティック PAT) の例

次に、スタティック ポート リダイレクション (この例では DNAT) の例を示します。192.168.0.10:37766 のホストは Telnet を使用して、ACE の VLAN 2021 の 192.168.211.1:3030 に接続します。ACE は、VLAN 2020 の 172.27.0.5:23 を VLAN 2021 の 192.168.211.1:3030 にマッピングします。

```
host1/Admin# show xlate
TCP PAT from vlan2020:172.27.0.5/23 to vlan2021:192.168.211.1/3030
Mar 24 2006 20:05:41 : %ACE-7-111009: User 'admin' executed cmd: show
xlate
```

```
host1/Admin# show conn
```

```
total current connections : 2
```

conn-id	dir	prot	vlan	source	destination	state
6	in	TCP	2021	192.168.0.10:37766	192.168.211.1:3030	ESTAB
7	out	TCP	2020	172.27.0.5:23	192.168.0.10:1025	ESTAB

## Clearing Xlates のクリア

EXEC モードで **clear xlate** コマンドを使用すると、グローバルアドレス、グローバルポート、ローカルアドレス、ローカルポート、グローバルアドレスとしてのインターフェイスアドレス、および NAT タイプに基づいたグローバルアドレス/ローカルアドレス マッピング情報をクリアできます。このコマンドを入力する場合、ACE は変換 (Xlates) を使用するセッションを解放します。このコマンドの構文は次のとおりです。

```
clear xlate [{global | local} start_ip [end_ip [netmask netmask]]] [{gport | lport} start_port [end_port]] [interface vlan number] [state static] [portmap]
```

キーワード、引数、およびオプションは次のとおりです。

- **global** - (任意) グローバル IP アドレスによるアクティブな変換をクリアします。
- **local** - (任意) ローカル IP アドレスによるアクティブな変換をクリアします。
- **start\_ip** - グローバルまたはローカル IP アドレス範囲のグローバルまたはローカル IP アドレス。ドット付き 10 進表記で IP アドレスを入力します (たとえば、172.27.16.10)。
- **end\_ip** - (任意) グローバルまたはローカル IP アドレス範囲の最後の IP アドレス。ドット付き 10 進表記で IP アドレスを入力します (たとえば、172.27.16.10)。
- **netmask netmask** - (任意) グローバルまたはローカル IP アドレスのネットワーク マスクを指定します。ドット付き 10 進表記でマスクを入力します (たとえば、255.255.255.0)。
- **gport** - (任意) グローバルポートによるアクティブな変換をクリアします。
- **lport** - (任意) ローカルポートによるアクティブな変換をクリアします。
- **start\_port** - グローバルまたはローカルポート番号。
- **end\_port** - (任意) グローバルまたはローカルポート範囲の最後のポート番号。
- **interface vlan number** - (任意) VLAN 番号によるアクティブな変換をクリアします。

- **state static** - (任意) ステートによるアクティブな変換をクリアします。
- **portmap** - (任意) ポート マップによるアクティブな変換をクリアします。



(注)

冗長性を設定した場合は、アクティブ側とスタンバイ側の両方の ACE 上で Xlate を明示的にクリアする必要があります。アクティブ アプライアンス でのみ Xlate をクリアすると、スタンバイ アプライアンス の Xlate が古いマッピングのまま残ります。

たとえば、すべてのスタティックな変換をクリアするには、次のように入力します。

```
host1/Admin# clear xlate state static
```

## NAT 設定の例

ここでは、ダイナミックおよびスタンバイな NAT ソリューションを使用する一般的なシナリオについて説明します。

- [ダイナミック NAT および PAT \(SNAT\) の設定例](#)
- [サーバファーム ベースのダイナミック NAT \(SNAT\) の設定例](#)
- [スタティック ポート リダイレクション \(DNAT\) の設定例](#)
- [クッキー ロード バランシングが設定された SNAT の例](#)

## ダイナミック NAT および PAT (SNAT) の設定例

次の SNAT の設定例では、ACE にダイナミック NAT および PAT を設定するのに使用するコマンドを示します。この SNAT の例では、192.168.12.0 ネットワークから ACE を入力するパケットは、**nat-pool** コマンドによって VLAN 200 で定義された NAT プールの IP アドレスの 1 つに変換されます。**pat** キーワードは、1024 より大きいポートも変換されたことを示します。

ACE がワンアーム モードで動作している場合、インターフェイス VLAN 100 を省略し、インターフェイス VLAN 200 にサービス ポリシーを設定します。

```
access-list NAT_ACCESS line 10 extended permit tcp 192.168.12.0
255.255.255.0 172.27.16.0 255.255.255.0 eq http

class-map match-any NAT_CLASS
  match access-list NAT_ACCESS

policy-map multi-match NAT_POLICY
  class NAT_CLASS
    nat dynamic 1 vlan 200

interface vlan 100
  mtu 1500
  ip address 192.168.1.100 255.255.255.0
  service-policy input NAT_POLICY
  no shutdown

interface vlan 200
  mtu 1500
  ip address 172.27.16.2 255.255.255.0
  nat-pool 1 172.27.16.15 172.27.16.24 netmask 255.255.255.0 pat
  no shutdown
```

## サーバファームベースのダイナミック NAT (SNAT) の設定例

次の SNAT の設定例では、ACE にサーバファームベースのダイナミック NAT を設定する場合に使用するコマンドを示します。この SNAT の例では、172.27.16.0 ネットワークの実サーバアドレスが、**nat-pool** コマンドで VLAN 200 に定義された NAT プール内の IP アドレスの 1 つに変換されます。

ACE がワンアームモードで動作している場合、インターフェイス VLAN 100 を省略し、インターフェイス VLAN 200 にサービスポリシーを設定します。

```
access-list NAT_ACCESS line 10 extended permit tcp 192.168.12.0
255.255.255.0 172.27.16.0 255.255.255.0 eq http

rserver SERVER1
  ip address 172.27.16.3
  inservice
rserver SERVER2
  ip address 172.27.16.4
  inservice

serverfarm SFARM1
  rserver SERVER1
```

```

    inservice
  rserver SERVER2
    inservice
class-map type http loadbalance match-any L7_CLASS
  match http content .*cisco.com
class-map match-any NAT_CLASS
  match access-list NAT_ACCESS

policy-map type loadbalance http first-match L7_POLICY
  class L7_CLASS
    serverfarm SFARM1
  nat dynamic 1 vlan 200 serverfarm primary
policy-map multi-match NAT_POLICY
  class NAT_CLASS
    loadbalance policy L7_POLICY
    loadbalance vip inservice

interface vlan 100
  mtu 1500
  ip address 192.168.1.100 255.255.255.0
  service-policy input NAT_POLICY
  no shutdown

interface vlan 200
  mtu 1500
  ip address 172.27.16.2 255.255.255.0
  nat-pool 1 172.27.16.15 172.27.16.24 netmask 255.255.255.0
  no shutdown

```

## スタティック ポート リダイレクション (DNAT) の設定例

次の DNAT の設定例では、ACE でスタティック ポート リダイレクションを設定するのに必要なコマンドに関連した実行コンフィギュレーションを示します。一般に、このコンフィギュレーションは DNAT に使用します。宛先が 192.0.0.0/8 で、VLAN 101 上の ACE に入る HTTP パケットは 10.0.0.0/8 とポート 8080 に変換されます。この例では、サーバがカスタム ポート 8080 で HTTP をホスティングします。

```

access-list acl1 line 10 extended permit tcp 10.0.0.0 255.0.0.0
eq 8080 any

class-map match-any NAT_CLASS
  match access-list acl1

policy-map multi-match NAT_POLICY

```





