CHAPTER 12

ネットワーク オブジェクト NAT の設定

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、*ネットワーク オブジェクト NAT* ルールと見なされます。ネットワーク オブジェクト NAT は、単一の IP アドレス、アドレス範囲、またはサブネットの NAT を設定するための迅速かつ容易な方法です。ネットワーク オブジェクトを設定したら、このオブジェクトのマッピング アドレスを識別できます。

この章では、ネットワーク オブジェクト NAT を設定する方法について説明します。この章は、次の項で構成されています。

（注） NAT の機能の詳細については、第 11 章「NAT に関する情報」を参照してください。

ネットワーク オブジェクト NAT に関する情報

パケットが ASA 1000V に入ると、送信元 IP アドレスと宛先 IP アドレスの両方がネットワーク オブジェクト NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはありません。したがって、宛先 X に向かう場合は送信元アドレスが A と変換され、宛先 Y に向かう場合は B と変換されるように指定することはできません。この種の機能には、Twice NAT を使用します（Twice NAT を使用すると、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます）。

Twice NAT とネットワーク オブジェクト NAT の違いの詳細については、「NAT の実装方法」（P.11-13）を参照してください。

ネットワーク オブジェクト NAT ルールは、NAT ルール テーブルのセクション 2 に追加されます。NAT の順序の詳細については、「NAT ルールの順序」（P.11-18）を参照してください。

ネットワーク オブジェクト NAT の前提条件

コンフィギュレーションによっては、必要に応じてマッピング アドレスをインラインで設定したり、マッピング アドレスの別のネットワーク オブジェクトまたはネットワーク オブジェクト グループを作成したりできます（**object network** コマンドまたは **object-group network** コマンド）。ネットワーク オブジェクト グループは、非連続的な IP アドレス範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。ネットワーク オブジェクトまたはグループを作成するには、「オブジェクトとグループの設定」（P.8-1）を参照してください。

オブジェクトおよびグループに関する特定のガイドラインについては、設定する NAT タイプの設定の項を参照してください。「ガイドラインと制限事項」の項も参照してください。

ガイドラインと制限事項

- 特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、**object network obj-10.10.10.1-01**、**object network obj-10.10.10.1-02** などのように、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待機せずに新しい NAT コンフィギュレーションを使用する必要がある場合は、**clear xlate** コマンドを使用して変換テーブルを消去できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

（注） ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピング アドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。
- 複数の NAT ルールで同じマッピングされたオブジェクトまたはグループを使用できます。
- マッピング IP アドレス プールは、次のアドレスを含むことができません。
  - マッピング インターフェイスの IP アドレス。ルールに **any** インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT の場合は、IP アドレスの代わりに **interface** キーワードを使用します。
  - （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
- インターフェイス PAT には IP アドレスがないため、内部セキュリティ プロファイル インターフェイスで設定できません。
- NAT または PAT のアプリケーション インスペクションの制限については、第 19 章「アプリケーション レイヤ プロトコル インスペクションの準備」の「デフォルト設定」（P.19-3）を参照してください。

デフォルト設定

- デフォルトの実際のインターフェイスおよびマッピング インターフェイスは Any で、すべてのインターフェイスにルールが適用されます。
- アイデンティティ NAT のデフォルト動作ではプロキシ ARP がイネーブルになっており、他のスタティック NAT ルールと一致します。必要に応じて、プロキシ ARP をディセーブルにできます。詳細については、「NAT パケットのルーティング」（P.11-20）を参照してください。
- 任意のインターフェイスを指定すると、ASA 1000V は NAT コンフィギュレーションを使用して出力インターフェイスを決定します。アイデンティティ NAT では、デフォルトの動作は NAT コンフィギュレーションを使用するようになっていますが、オプションで常にルート ルックアップを代わりに使用することもできます。詳細については、「NAT パケットのルーティング」（P.11-20）を参照してください。

ネットワーク オブジェクト NAT の設定

この項では、ネットワーク オブジェクト NAT を設定する方法について説明します。次の項目を取り上げます。

ダイナミック NAT の設定

この項では、ダイナミック NAT のネットワーク オブジェクト NAT を設定する方法について説明します。詳細については、「ダイナミック NAT」（P.11-9）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	ネットワーク オブジェクト： **object network** *obj_name* 　**range** *ip_address_1 ip_address_2* ネットワーク オブジェクト グループ： **object-group network** *grp_name* 　{**network-object** {**object** *net_obj_name* | 　**host** *ip_address*} | 　**group-object** *grp_obj_name*} **例：** hostname(config)# object network TEST hostname(config-network-object)# range 10.1.1.1 10.1.1.70 hostname(config)# object network TEST2 hostname(config-network-object)# range 10.1.2.1 10.1.2.70 hostname(config-network-object)# object-group network MAPPED_IPS hostname(config-network)# network-object object TEST hostname(config-network)# network-object object TEST2 hostname(config-network)# network-object host 10.1.2.79	（変換先である）**マッピング** アドレスを指定するには、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを設定します。ネットワーク オブジェクト グループは、オブジェクトまたはインライン アドレス、あるいはその両方を含むことができます。 **（注）**　オブジェクトまたはグループは、サブネットを含むことはできません。 マッピングされたネットワーク オブジェクトに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。 拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.12-2）を参照してください。 ネットワーク オブジェクトまたはグループの設定の詳細については、「オブジェクトの設定」（P.8-3）を参照してください。
ステップ 2	**object network** *obj_name* **例：** hostname(config)# object network my-host-obj1	NAT を設定するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address* *netmask* | **range** *ip_address_1 ip_address_2*} **例：** hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	新しいネットワーク オブジェクトを作成している場合、変換する**実際の** IP アドレスを定義します。

	コマンド	目的
ステップ 4	**nat** [**(***real_ifc*,*mapped_ifc*)] **dynamic** *mapped_obj* [**interface**] [**dns**] **例：** hostname(config-network-object)# nat (VM1,outside) dynamic MAPPED_IPS interface	オブジェクト IP アドレスの**ダイナミック NAT** を設定します。 **（注）**　特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「ガイドラインと制限事項」（P.12-2）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。いずれかまたは両方のインターフェイスに **any** キーワードを指定することもできます。 • マッピング IP アドレス：次のものとしてマッピング IP アドレスを指定します。 – 既存のネットワーク オブジェクト（ステップ 1 を参照） – 既存のネットワーク オブジェクト グループ（ステップ 1 を参照） • インターフェイス PAT のフォール バック：（任意）**interface** キーワードは、インターフェイス PAT のフォール バックをイネーブルにします。マッピング IP アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。 • DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.11-23）を参照してください。

例

次の例では、外部アドレス 10.2.2.1 ～ 10.2.2.10 の範囲の背後に 192.168.2.0 ネットワークを隠すダイナミック NAT を設定します。

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (VM1,outside) dynamic my-range-obj
```

次の例では、ダイナミック PAT バックアップを設定したダイナミック NAT を設定します。セキュリティ プロファイル VM1 ネットワーク 10.76.11.0 のホストは、まず nat-range1 プール（10.10.10.10 ～ 10.10.10.20）にマッピングされます。nat-range1 プール内のすべてのアドレスが割り当てられたら、pat-ip1 アドレス（10.10.10.21）を使用してダイナミック PAT が実行されます。PAT 変換もすべて使用されることはほとんどありませんが、このような場合には、外部インターフェイス アドレスを使用してダイナミック PAT が実行されます。

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20
```

```
hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21

hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (VM1,outside) dynamic nat-pat-grp interface
```

ダイナミック PAT（隠蔽）の設定

この項では、ダイナミック PAT（隠蔽）のネットワーク オブジェクト NAT を設定する方法について説明します。詳細については、「ダイナミック PAT」（P.11-11）を参照してください。

ガイドライン

PAT プールの場合：

- 可能な場合は、実際の送信元ポート番号がマッピング ポートに使用されます。ただし、実際のポートが使用できない場合は、デフォルトでマッピング ポートは実際のポート番号と同じポートの範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。
- 2 つの別個のルールで同じ PAT プール オブジェクトを使用する場合は、各ルールに対して同じオプションを指定してください。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールの拡張 PAT の場合：

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションのリストについては、第 19 章「アプリケーション レイヤ プロトコル インスペクションの準備」の「デフォルト設定」（P.19-3）を参照してください。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合、PAT プールのアドレスを、ポート変換ルールを持つ別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート変換ルールを持つスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

PAT プールのラウンド ロビン方式の場合：

- ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。**注**：この「スティッキ性」は、フェールオーバーが発生すると失われます。ASA 1000V がフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。

- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

手順の詳細

	コマンド	目的
ステップ 1	（任意） ネットワーク オブジェクト： **object network** *obj_name* {**host** *ip_address* | **range** *ip_address_1 ip_address_2*} ネットワーク オブジェクト グループ： **object-group network** *grp_name* {**network-object** {**object** *net_obj_name* | **host** *ip_address*} | **group-object** *grp_obj_name*} **例：** hostname(config)# object network PAT_POOL1 hostname(config-network-object)# range 10.5.1.80 10.7.1.80 hostname(config)# object network PAT_POOL2 hostname(config-network-object)# range 10.9.1.1 10.10.1.1 hostname(config)# object network PAT_IP hostname(config-network-object)# host 10.5.1.79 hostname(config-network-object)# object-group network PAT_POOLS hostname(config-network)# network-object object PAT_POOL1 hostname(config-network)# network-object object PAT_POOL2 hostname(config-network)# network-object object PAT_IP	（変換先である）**マッピング** アドレスを指定します。1 つのアドレス、または PAT プールに対して複数のアドレスを設定できます。ネットワーク オブジェクトまたはネットワーク オブジェクト グループを設定できます。ネットワーク オブジェクト グループは、オブジェクトまたはインライン アドレス、あるいはその両方を含むことができます。**nat** コマンドのインライン値として 1 つの IP アドレスを入力する場合や、**interface** キーワードを指定してインターフェイス アドレスを使用する場合は、この手順をスキップすることもできます。 PAT プールとして使用するマッピング アドレスの場合、オブジェクト内または範囲を含むグループ内のすべてのアドレスが PAT アドレスとして使用されます。 **（注）** オブジェクトまたはグループは、サブネットを含むことはできません。 拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.12-2）を参照してください。 ネットワーク オブジェクトまたはグループの設定の詳細については、「オブジェクトの設定」（P.8-3）を参照してください。
ステップ 2	**object network** *obj_name* **例：** hostname(config)# object network my-host-obj1	NAT を設定するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** hostname(config-network-object)# range 10.1.1.1 10.1.1.90	新しいネットワーク オブジェクトを作成している場合、変換する**実際の** IP アドレスを定義します。

	コマンド	目的
ステップ 4	**nat** [**(***real_ifc*,*mapped_ifc*)] **dynamic** {*mapped_inline_host_ip* | *mapped_obj* | **pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] | **interface**} [**interface**] [**dns**] **例：** `hostname(config-network-object)# nat (any,outside) dynamic interface`	オブジェクト IP アドレスの**ダイナミック PAT** を設定します。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「ガイドラインと制限事項」（P.12-2）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。いずれかまたは両方のインターフェイスに **any** キーワードを指定することもできます。 • マッピング IP アドレス：マッピング IP アドレスを次のものとして指定できます。 – インライン ホスト アドレス。 – ホスト アドレスとして定義される既存のネットワーク オブジェクト（ステップ 1 を参照）。 – **pat-pool**：複数のアドレスを含む、既存のネットワーク オブジェクトまたはグループ。 – **interface**：マッピング インターフェイスの IP アドレスがマッピング アドレスとして使用されます。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。このキーワードは、インターフェイスの IP アドレスを使用するときに使用する必要があります。インラインで、またはオブジェクトとして入力することはできません。 • PAT プールについて、次のオプションの 1 つ以上を指定できます。 – ラウンド ロビン：**round-robin** キーワードは、PAT プールのラウンド ロビン アドレス割り当てをイネーブルにします。ラウンド ロビンを指定しなければ、デフォルトで PAT アドレスのすべてのポートは次の PAT アドレスが使用される前に割り当てられます。ラウンド ロビン方式は、最初のアドレス、次に 2 つめのアドレスというように使用するために戻る前にプールの各 PAT アドレスからアドレス / ポートを割り当てます。 （続き）

コマンド	目的
	（続き） – 拡張 PAT：**extended** キーワードは、拡張 PAT をイネーブルにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。 – フラットな範囲：**flat** キーワードは、ポートを割り当てる場合、1024 ～ 65535 ポート範囲全体の使用をイネーブルにします。変換のマッピング ポート番号を選択するときに、ASA 1000V によって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用 *できない* 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、**include-reserve** キーワードも指定します。 • インターフェイス PAT のフォール バック：（任意）**interface** キーワードは、プライマリ PAT アドレスの後に入力されたときにインターフェイス PAT のフォール バックをイネーブルにします。プライマリ PAT アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。 • DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.11-23）を参照してください。

例

次の例では、アドレス 10.2.2.2 の背後に 192.168.2.0 ネットワークを隠すダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (VM1,outside) dynamic 10.2.2.2
```

次の例では、外部インターフェイス アドレスの背後に 192.168.2.0 ネットワークを隠蔽するダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
```

```
hostname(config-network-object)# nat (VM1,outside) dynamic interface
```

スタティック NAT またはポート変換を設定したスタティック NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してスタティック NAT ルールを設定する方法について説明します。詳細については、「スタティック NAT」（P.11-4）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	（任意） ネットワーク オブジェクト： **object network** *obj_name* {**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} ネットワーク オブジェクト グループ： **object-group network** *grp_name* {**network-object** {**object** *net_obj_name* | *subnet_address netmask* | **host** *ip_address*} | **group-object** *grp_obj_name*} **例：** hostname(config)# object network MAPPED_IPS hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	（変換先である）**マッピング** アドレスを指定するには、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを設定します。ネットワーク オブジェクト グループは、オブジェクトまたはインライン アドレス、あるいはその両方を含むことができます。または、**nat** コマンドのインライン値として IP アドレスを入力する場合や、**interface** キーワードを指定してインターフェイス アドレス（ポート変換を設定したスタティック NAT の場合）を使用する場合は、この手順を省略できます。 拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.12-2）を参照してください。 ネットワーク オブジェクトまたはグループの設定の詳細については、「オブジェクトの設定」（P.8-3）を参照してください。
ステップ 2	**object network** *obj_name* **例：** hostname(config)# object network my-host-obj1	NAT を設定するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0	新しいネットワーク オブジェクトを作成している場合、変換する**実際の** IP アドレスを定義します。

	コマンド	目的
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface**} [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] **例：** `hostname(config-network-object)# nat (VM1,outside) static MAPPED_IPS service tcp 80 8080`	オブジェクト IP アドレスの**スタティック NAT** を設定します。 **（注）** 特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「ガイドラインと制限事項」（P.12-2）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。いずれかまたは両方のインターフェイスに **any** キーワードを指定することもできます。 • マッピング IP アドレス：マッピング IP アドレスを次のものとして指定できます。 – インライン IP アドレス。マッピング ネットワークのネットマスクまたは範囲は、実際のネットワークと同じです。たとえば、実際のネットワークがホストの場合、このアドレスは、ホスト アドレスです。範囲の場合、マッピング アドレスには、実際の範囲と同じ数のアドレスが含まれます。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲として定義され、172.20.1.1 をマッピング アドレスとして指定する場合、マッピング範囲には、172.20.1.1 ～ 172.20.1.6 が含まれます。 – 既存のネットワーク オブジェクトまたはグループ（ステップ 1 を参照）。 – **interface**：（ポート変換を設定したスタティック NAT のみ）このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。**service** キーワードも必ず設定します。 通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。詳細については、「スタティック NAT」（P.11-4）を参照してください。 • DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.11-23）を参照してください。**service** キーワードを指定した場合、このオプションは使用できません。 • ポート変換：（ポート変換を設定したスタティック NAT のみ）**tcp** または **udp** および実際のポートとマッピング ポートを指定します。ポート番号または予約済みポートの名前（**ftp** など）のいずれかを入力できます。 • No Proxy ARP：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング」（P.11-20）を参照してください。

例

次の例では、内部にある実際のホスト 10.1.1.1 の、DNS リライトがイネーブルに設定された外部にある 10.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (VM1,outside) static 10.2.2.2 dns
```

次の例では、内部にある実際のホスト 10.1.1.1 の、マッピングされたオブジェクトを使用する外部にある 2.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (VM1,outside) static my-mapped-obj
```

次の例では、10.1.1.1 の TCP ポート 21 の、外部インターフェイスのポート 2121 への、ポート変換を設定したスタティック NAT を設定します。

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (VM1,outside) static interface service tcp 21 2121
```

アイデンティティ NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。詳細については、「アイデンティティ NAT」（P.11-12）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	（任意） **object network** *obj_name* {**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** hostname(config)# object network MAPPED_IPS hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	（実際のアドレスと同じ）**マッピング** アドレスについて、ネットワーク オブジェクトを設定します。または、**nat** コマンドのインライン値として IP アドレスを入力する場合は、この手順を省略できます。 ネットワーク オブジェクトの設定の詳細については、「オブジェクトの設定」（P.8-3）を参照してください。
ステップ 2	**object network** *obj_name* **例：** hostname(config)# object network my-host-obj1	アイデンティティ NAT を実行するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	新しいネットワーク オブジェクトを作成している場合、アイデンティティ NAT を実行する実際の IP アドレスを定義します。ステップ 1 でマッピング アドレスのネットワーク オブジェクトを設定した場合、これらのアドレスは一致する必要があります。
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj*} [**no-proxy-arp**] [**route-lookup**] **例：** hostname(config-network-object)# nat (VM1,outside) static MAPPED_IPS	オブジェクト IP アドレスの**アイデンティティ NAT** を設定します。 **（注）** 特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「ガイドラインと制限事項」（P.12-2）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。いずれかまたは両方のインターフェイスに **any** キーワードを指定することもできます。 • マッピング IP アドレス：マッピング アドレスと実際のアドレスの両方に同じ IP アドレスを設定するようにしてください。次のいずれかを使用します。 – ネットワーク オブジェクト：実際のオブジェクトと同じ IP アドレスを含めます（ステップ 1 を参照）。 – インライン IP アドレス：マッピング ネットワークのネットマスクまたは範囲は、実際のネットワークと同じです。たとえば、実際のネットワークがホストの場合、このアドレスは、ホスト アドレスです。範囲の場合、マッピング アドレスには、実際の範囲と同じ数のアドレスが含まれます。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲で定義されている場合、マッピング アドレスとして 10.1.1.1 を指定するには、マッピングされた範囲に 10.1.1.1 ～ 10.1.1.6 が含まれます。 • No Proxy ARP：マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング」（P.11-20）を参照してください。 • ルート ルックアップ：（インターフェイスを指定）NAT コマンドに指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定するには、**route-lookup** を指定します。詳細については、「出力インターフェイスの決定」（P.11-22）を参照してください。

例

次の例では、インラインのマッピング アドレスを使用して、ホスト アドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (VM1,outside) static 10.1.1.1
```

次の例では、ネットワーク オブジェクトを使用して、ホスト アドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (VM1,outside) static my-host-obj1-identity
```

ネットワーク オブジェクト NAT のモニタリング

オブジェクト NAT をモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show nat	各 NAT ルールのヒットを含む NAT の統計情報を表示します。
show nat pool	割り当てられたアドレスとホスト、および割り当て回数を含む、NAT プールの統計情報を表示します。

コマンド	目的

show running-config nat	NAT コンフィギュレーションを表示します。
	（注） NAT コンフィギュレーションは、**show running-config object** コマンドを使用して表示できません。**nat** コマンドで作成されていないオブジェクトまたはオブジェクト グループを参照することはできません。**show** コマンド出力での転送または循環参照を回避するために、**show running-config** コマンドは **object** コマンドを 2 回表示します。1 回目は、IP アドレスが定義される場所、2 回目は **nat** コマンドが定義される場所で表示されます。このコマンド出力によって、オブジェクト、オブジェクト グループ、NAT の順に定義されることが保証されます。例：
	`hostname# show running-config`
	`...`
	`object network obj1`
	`  range 192.168.49.1 192.150.49.100`
	`object network obj2`
	`  object 192.168.49.100`
	`object network network-1`
	`  subnet <network-1>`
	`object network network-2`
	`  subnet <network-2>`
	`object-group network pool`
	`  network-object object obj1`
	`  network-object object obj2`
	`...`
	`object network network-1`
	`  nat (VM1,outside) dynamic pool`
	`object network network-2`
	`  nat (VM1,outside) dynamic pool`

show xlate	現在の NAT セッション情報を表示します。

ネットワーク オブジェクト NAT の設定例

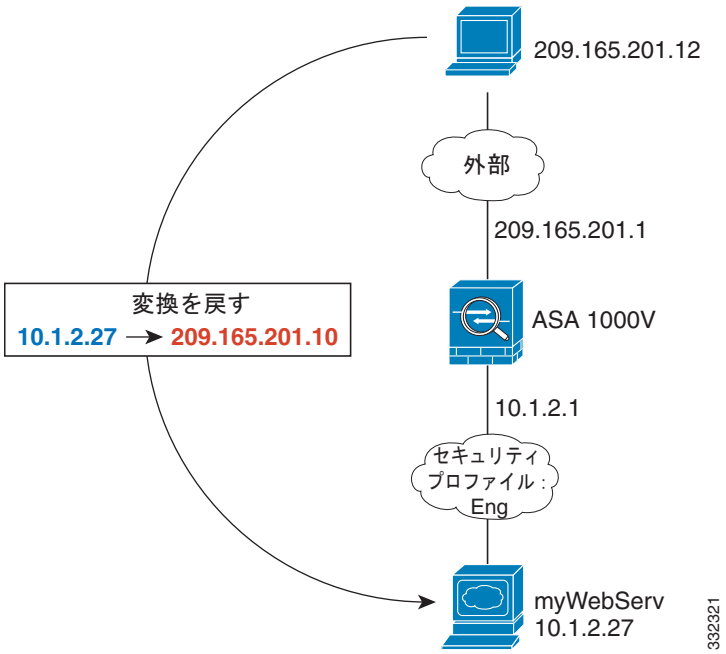
この項では、次の設定例を示します。

- 「内部 Web サーバへのアクセスの提供（スタティック NAT）」（P.12-16）
- 「内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT）」（P.12-16）
- 「複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ」（P.12-18）
- 「FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック NAT）」（P.12-19）
- 「マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT）」（P.12-20）
- 「マッピング インターフェイス上の DNS サーバおよび Web サーバ、Web サーバが変換される（DNS 修正を設定したスタティック NAT）」（P.12-22）

内部 Web サーバへのアクセスの提供（スタティック NAT）

次の例では、内部 Eng サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるので、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です （図 12-1 を参照）。

図 12-1　内部 Web サーバのスタティック NAT



ステップ 1　Eng Web サーバのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
```

ステップ 2　Web サーバのアドレスを定義します。

```
hostname(config-network-object)# host 10.1.2.27
```

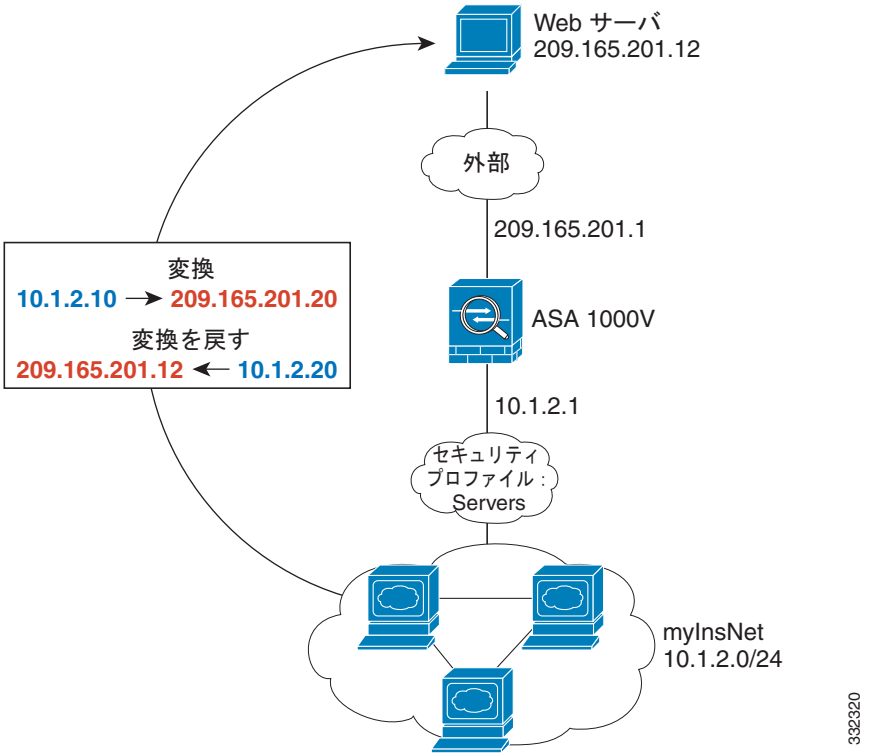
ステップ 3　オブジェクトのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (eng,outside) static 209.165.201.10
```

内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT）

次の例では、プライベート ネットワーク上の内部サーバに対して、このサーバが外部にアクセスする場合のダイナミック NAT を設定します。また、内部サーバが外部 Web サーバに接続する場合、この Web サーバのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます（図 12-2 を参照）。

図 12-2　内部のダイナミック NAT、外部 Web サーバのスタティック NAT



ステップ 1　サーバ アドレスを変換するダイナミック NAT プールのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

ステップ 2　サーバ ネットワークのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 3　サーバ ネットワークのダイナミック NAT をイネーブルにします。

```
hostname(config-network-object)# nat (Servers,outside) dynamic myNatPool
```

ステップ 4　外部 Web サーバのネットワーク オブジェクトを作成します。

```
hostname(config)# object network outWebServ
```

ステップ 5　Web サーバのアドレスを定義します。

```
hostname(config-network-object)# host 209.165.201.12
```

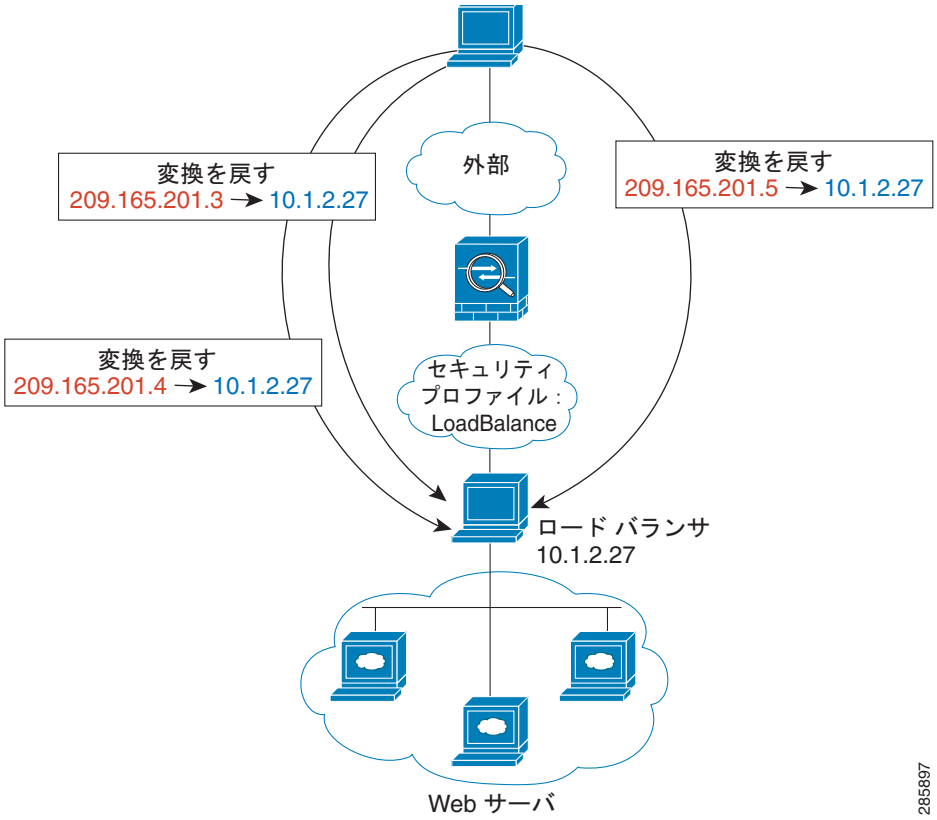
ステップ 6　Web サーバのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (outside,Servers) static 10.1.2.20
```

複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ

次の例では、複数の IP アドレスに変換される内部ロード バランサを示しています。外部ホストがマッピング IP アドレスの 1 つにアクセスする場合、1 つのロード バランサのアドレスには変換されません。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。（図 12-3 を参照）。

図 12-3　内部ロード バランサのスタティック NAT（1 対多）



ステップ 1　ロード バランサをマッピングするアドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.165.201.8
```

ステップ 2　ロード バランサのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myLBHost
```

ステップ 3　ロード バランサのアドレスを定義します。

```
hostname(config-network-object)# host 10.1.2.27
```

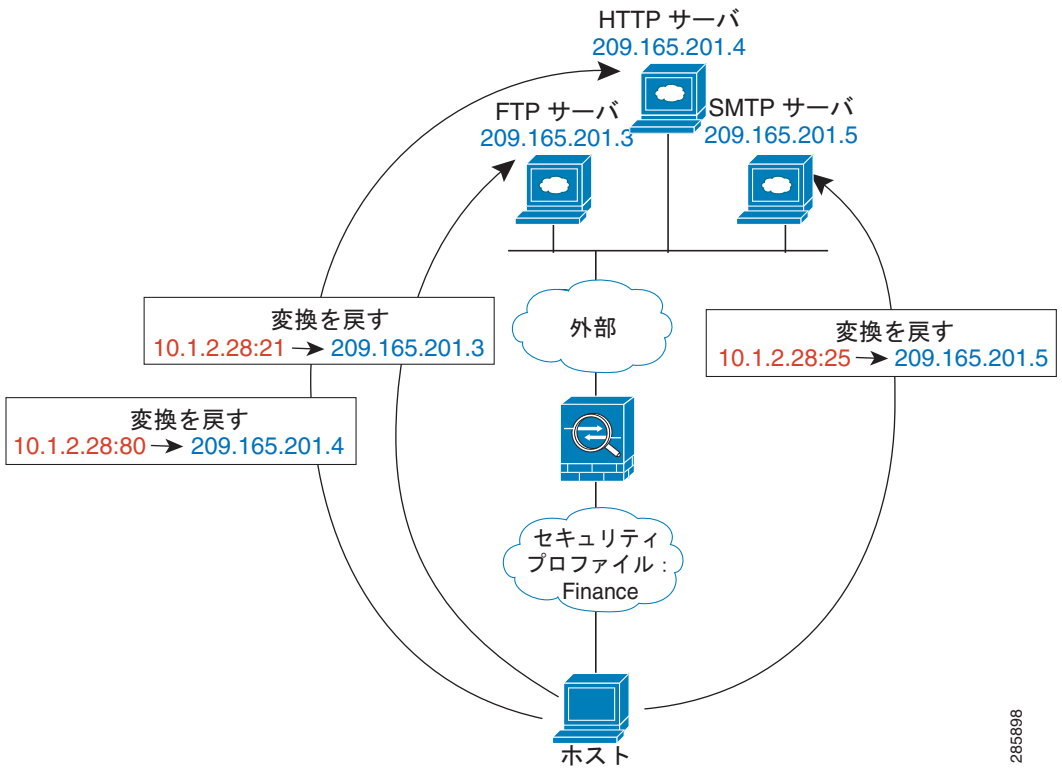
ステップ 4　ロード バランサのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (LoadBalance,outside) static myPublicIPs
```

FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック NAT）

次のポート変換を設定したスタティック NAT の例では、Finance のユーザが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。実際にはこれらのサーバは、実際のネットワーク上の異なるデバイスですが、各サーバに対して、異なるポートでも同じマッピング IP アドレスを使用するというポート変換を設定したスタティック NAT ルールを指定できます。（図 12-4 を参照）。

図 12-4　　ポート変換を設定したスタティック NAT



ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

ステップ 2　FTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を FTP サーバに設定します。

```
hostname(config-network-object)# host 209.165.201.3
hostname(config-network-object)# nat (outside,Finance) static 10.1.2.28 service tcp ftp
ftp
```

ステップ 3　HTTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network HTTP_SERVER
```

ステップ 4　HTTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を HTTP サーバに設定します。

```
hostname(config-network-object)# host 209.165.201.4
hostname(config-network-object)# nat (outside,Finance) static 10.1.2.28 service tcp http
http
```

ステップ 5　SMTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network SMTP_SERVER
```

ステップ 6　SMTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を SMTP サーバに設定します。

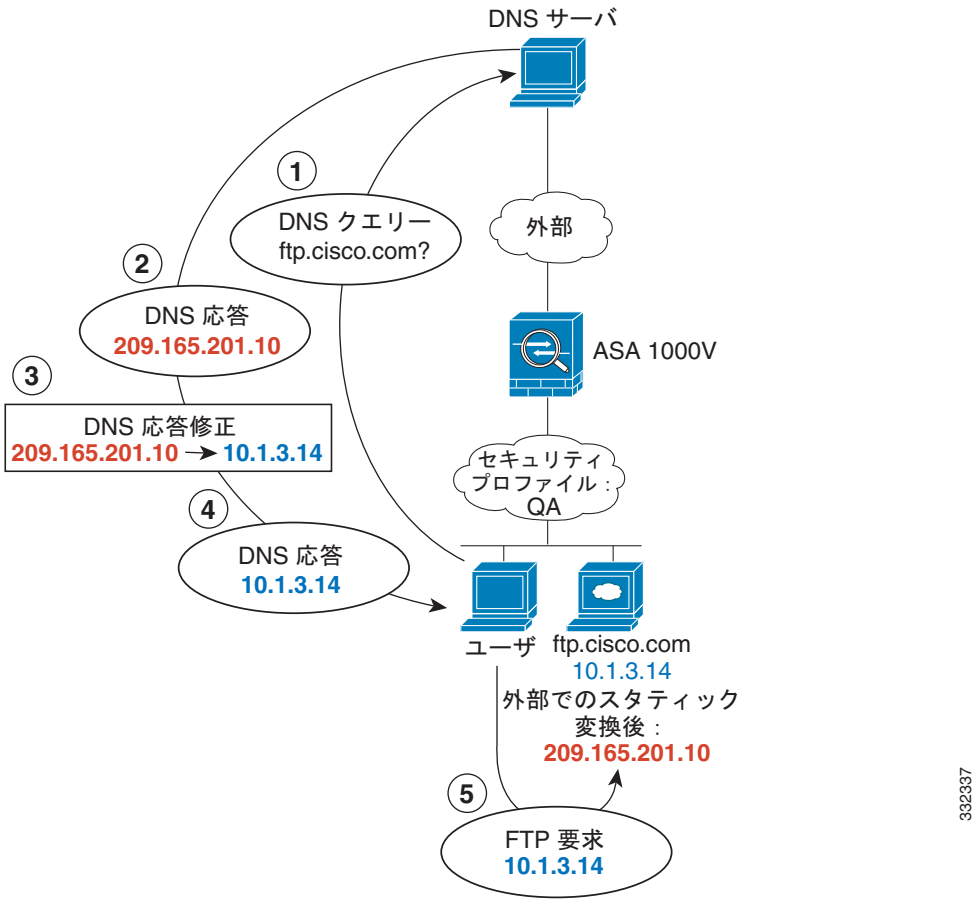
```
hostname(config-network-object)# host 209.165.201.5
hostname(config-network-object)# nat (outside,Finance) static 10.1.2.28 service tcp smtp
smtp
```

マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT）

たとえば、DNS サーバが外部インターフェイスからアクセス可能であるとします。ftp.cisco.com というサーバが内部 QA セキュリティ プロファイル インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、ASA 1000V を設定します （図 12-5 を参照）。この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている QA ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信するようになります。

QA ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。ASA 1000V は、QA サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、QA ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信することを試みます。

図 12-5　　DNS 応答修正



ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

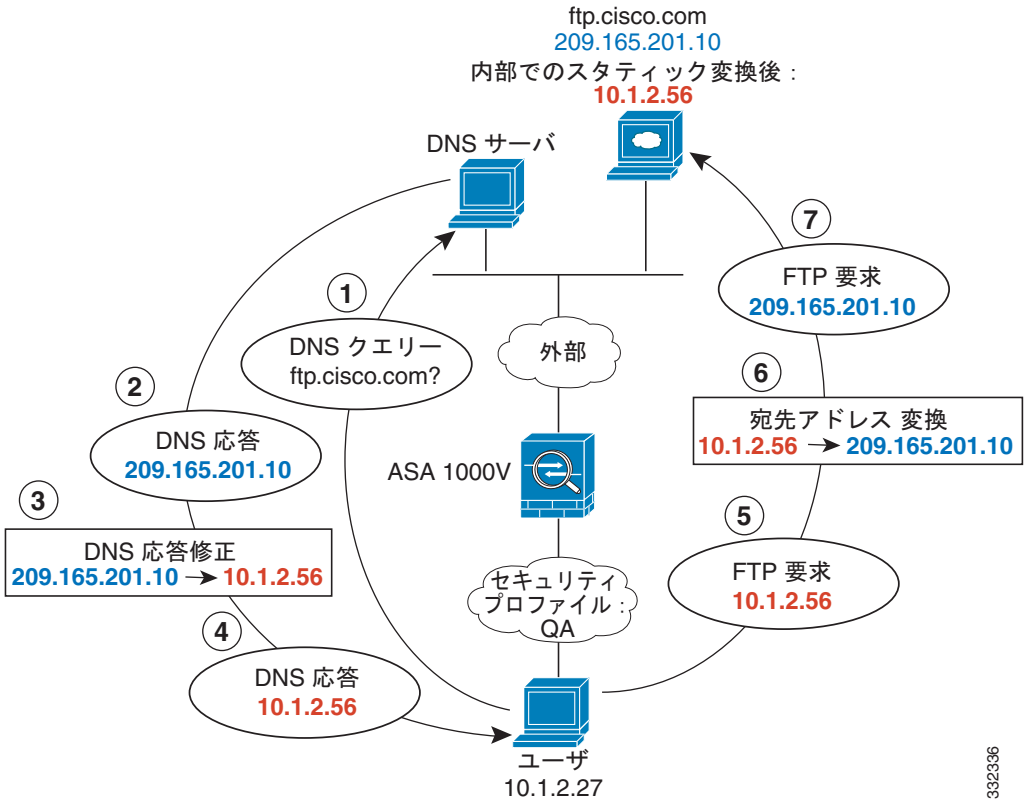
ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。

```
hostname(config-network-object)# host 10.1.3.14
hostname(config-network-object)# nat (QA,outside) static 209.165.201.10 dns
```

マッピング インターフェイス上の DNS サーバおよび Web サーバ、Web サーバが変換される（DNS 修正を設定したスタティック NAT）

図 12-6 に、外部の Web サーバと DNS サーバを示します。ASA 1000V には、外部サーバ用のスタティック変換があります。この場合、内部 QA セキュリティ プロファイル ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を示します。ftp.cisco.com のマッピング アドレス（10.1.2.56）を QA ユーザに使用させる必要があるため、スタティック変換に対して DNS 応答修正を設定する必要があります。

図 12-6　外部 NAT を使用する DNS 応答修正



ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。

```
hostname(config-network-object)# host 209.165.201.10
hostname(config-network-object)# nat (outside,QA) static 10.1.2.56 dns
```

ネットワーク オブジェクト NAT の機能履歴

表 12-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 12-1　ネットワーク オブジェクト NAT の機能履歴

機能名	プラットフォーム リリース	機能情報
ネットワーク オブジェクト NAT	8.3(1)	ネットワーク オブジェクトの IP アドレスの NAT を設定します。 **nat**（オブジェクト ネットワーク コンフィギュレーション モード）、**show nat**、**show xlate**、**show nat pool** コマンドが導入または変更されました。
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	8.4(2)/8.5(1)	アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブルにされ、出力インターフェイスの決定には常にルート ルックアップが使用されていました。これらを設定することはできませんでした。8.4(2) 以降、アイデンティティ NAT のデフォルト動作は他のスタティック NAT コンフィギュレーションの動作に一致するように変更されました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、NAT コンフィギュレーションにより出力インターフェイスが決定されるようになりました（指定されている場合）。これらの設定をそのまま残すこともできますし、個別にイネーブルまたはディセーブルにすることもできます。通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできるようになっています。 8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになっています。 **nat static** [**no-proxy-arp**] [**route-lookup**] コマンドが変更されました。
PAT プールおよびラウンド ロビン アドレス割り当て	8.4(2)/8.5(1)	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになりました。プールの次のアドレスを使用する前に、最初に PAT アドレスのすべてのポートを使用するのではなく、PAT アドレスのラウンド ロビン割り当てを必要に応じてイネーブルにすることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行っている場合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機能により、多数の PAT アドレスを簡単に設定できます。 **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]] コマンドが変更されました。

表 12-1　ネットワーク オブジェクト NAT の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
ラウンドロビン PAT プール割り当てで、既存のホストの同じ IP アドレスを使用する	8.4(3)	ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。 any コマンドを変更できませんでした。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの PAT ポートのフラットな範囲	8.4(3)	使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートには、小さい PAT プールのみがあります。 下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールを使用するときに、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。 **nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] コマンドが変更されました。 *この機能は、8.5(1) または 8.6(1) では使用できません。*

表 12-1　ネットワーク オブジェクト NAT の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
PAT プールの拡張 PAT	8.4(3)	各 PAT IP アドレスでは、最大 65535 個のポートを使用できます。65535 個のポートで変換が不十分な場合は、PAT プールに対して拡張 PAT をイネーブルにすることができます。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。 **nat dynamic** [**pat-pool** *mapped_object* [**extended**]] コマンドが変更されました。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに戻す自動 NAT ルール	8.4(3)	まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。 この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。ルールは **show nat** コマンドを使用して表示できます。 **（注）** ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。ご使用のネットワークとの機能の互換性を確認するには、Cisco TAC にお問い合わせください。次の制限事項を確認してください。 • Cisco IPsec および AnyConnect クライアントのみがサポートされます。 • NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターン トラフィックは ASA 1000V にルーティングされる必要があります。 • ロードバランシングはサポートされません（ルーティングの問題のため）。 • ローミング（パブリック IP 変更）はサポートされません。 次のコマンドが導入されました。 **nat-assigned-to-public-ip** *interface*（トンネル グループ一般属性コンフィギュレーション モード）。