7000 および 8000 シリーズ デバイス用の NAT

以下のトピックでは、7000 および 8000 シリーズ デバイス用に NAT を設定する方法を示します。

- NAT ポリシーの設定 （1 ページ）
- NAT ポリシー内のルール編成 （3 ページ）
- NAT ルールの編成 （4 ページ）
- NAT ポリシー規則のオプション （5 ページ）

NAT ポリシーの設定

特定のネットワーク ニーズを管理するためにさまざまな方法で NAT ポリシーを設定できます。次の操作を実行できます。

- 外部ネットワークに内部サーバを公開します。

  この設定では、外部 IP アドレスから内部 IP アドレスへのスタティック変換を定義するため、システムはネットワーク外部から内部サーバにアクセスできます。サーバに送信されるトラフィックは、外部 IP アドレスまたは IP アドレスとポートを対象とし、内部 IP アドレスまたは IP アドレスとポートに変換されます。サーバからのリターン トラフィックは、外部アドレスに再度変換されます。

- 内部ホスト/サーバが外部アプリケーションに接続できるようにします。

  この設定では、内部アドレスから外部アドレスへのスタティック変換を定義します。この定義により、内部ホストまたはサーバは、内部ホストまたはサーバが特定の IP アドレスおよびポートを持っていると予期する外部アプリケーションへの接続を開始できます。したがって、システムは内部ホストまたはサーバのアドレスを動的に割り当てることはできません。

- 外部ネットワークに対してプライベート ネットワーク アドレスを隠します。

  以下のいずれかの設定を使用して、内部ネットワーク アドレスをわかりにくくすることができます。

  - 内部ネットワークの必要に十分対応できるだけの数の外部 IP アドレスがある場合は、IP アドレスのブロックを使用できます。この設定では、すべての発信トラフィックの

送信元 IP アドレスを、外部に面する IP アドレスのうち未使用の IP アドレスに自動的に変換するダイナミック変換を作成します。

- 内部ネットワークの必要に対応できるだけの数の外部 IP アドレスがない場合は、限定した数の IP アドレスのブロックとポート変換を使用できます。この設定では、発信トラフィックの送信元 IP アドレスとポートを、外部に面する IP アドレスのうち未使用の IP アドレスとポートに自動的に変換するダイナミック変換を作成します。

⚠

注意 7000 または 8000 シリーズ デバイスの高可用性ペアでは、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、ペアを構成するデバイス上でのスタティック NAT ルールに対して個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールには、この設定を使用しないでください。

NAT ポリシーの設定ガイドライン

NAT ポリシーを設定するには、ポリシーに一意の名前を付け、ポリシーを展開するデバイスつまりターゲットを特定する必要があります。また、NAT ルールを追加、編集、削除、有効化、および無効化することができます。NAT ポリシーを作成または変更した後、ターゲット デバイスのすべてまたは一部にポリシーを展開できます。

スタンドアロン デバイスと同様に、NAT ポリシーをペアリングされたスタックを含む 7000 または 8000 シリーズ デバイス高可用性ペアに展開できます。ただし、個別のペアリングされたデバイスまたは高可用性ペア全体でインターフェイスのスタティック NAT ルールを定義し、送信元ゾーン内でインターフェイスを使用できます。ダイナミック ルールの場合、送信元ゾーンまたは宛先ゾーンで高可用性ペア全体のインターフェイスのみを使用できます。

⚠

注意 7000 または 8000 シリーズ デバイス高可用性ペアで、NAT 変換により影響を受けるすべてのネットワークがプライベートの場合、ペアリングされたデバイスのスタティック NAT ルールに対して、個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用**しない**でください。

HA リンク インターフェイスが確立されていないデバイス高可用性ペアでダイナミック NAT を設定した場合、両方のペアリングされたデバイスは別々にダイナミック NAT エントリを割り当て、システムはデバイス間でエントリを同期できません。

スタンドアロン デバイスと同様に、NAT ポリシーをデバイス スタックに展開できます。NAT ポリシーに含まれ、スタックのメンバーであるセカンダリ デバイスのインターフェイスに関連付けられているルールを持ったデバイスからデバイス スタックを確立した場合、セカンダリ デバイスのインターフェイスは NAT ポリシーに残ります。インターフェイスを持つポリシーを保存および展開できますが、ルールは変換を実現しません。

先祖ドメインのマルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。管理者は、NAT ポリシーのターゲットを子孫ドメインのデバイスに設定できます。こうすることで、子孫ドメインではカスタマイズされたローカルポリシーを使用または置き換えることができます。

NAT ポリシー内のルール編成

NAT ポリシーの編集ページにはスタティックな NAT ルールとダイナミックな NAT ルールが別々に表示されます。このシステムでは、スタティック ルールは名前のアルファベット順に並べ替えられ、表示順序を変更できません。同一の照合値を持つスタティック ルールは作成できません。システムの照合では、ダイナミック変換を検査する前に、スタティック変換を検査します。

ダイナミック ルールは番号順に処理されます。各ダイナミック ルールの番号位置は、ページ左側のルールの横に表示されます。ダイナミック ルールは移動または挿入したり、ルールの順序を変更したりすることができます。たとえば、ダイナミック ルール 10 をダイナミック ルール 3 の下に移動した場合、ルール 10 がルール 4 になり、後に続くすべての番号が順次繰り上がります。

このシステムでは、ポリシーの編集ページ上のルールの番号順にパケットとダイナミック ルールを比較するので、ダイナミック ルールの位置は重要です。パケットがダイナミック ルールのすべての条件を満たすと、システムはパケットにそのルール条件を適用し、そのパケットに対する後続のルールはすべて無視します。

ダイナミック ルールを追加または編集する際、ダイナミック ルールの番号の位置を指定できます。新しいダイナミック ルールを追加する前にダイナミック ルールを強調表示して、強調表示したルールの下に新しいルールを挿入することもできます。

ルールの行内の空白部分をクリックすることにより、1つ以上のダイナミック ルールを選択できます。選択したダイナミック ルールを新しい場所にドラッグ アンド ドロップできます。これにより、移動したルールと後続のすべてのルールの位置が変更されます。

選択したルールを既存のルールの上または下にカット アンド ペーストできます。スタティック ルールはスタティック変換リストにのみ、ダイナミック ルールはダイナミック変換リストにのみ貼り付けることができます。また、選択したルールを削除したり、既存のルール リスト内の任意の場所に新しいルールを挿入したりすることもできます。

先行ルールが優先して適用されるために決して一致することがないルールを示す、説明的な警告を表示することもできます。

展開にアクセス コントロール ポリシーが存在する場合、このシステムではアクセス制御を通過するまでトラフィックを変換することありません。

NAT ルールの編成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）] > [NAT]**を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 NAT ルールを編成します。

- ルールを選択するには、ルールの行の空白部分をクリックします。
- ルールの選択をクリアするには、ページの右下にあるリロード アイコン（）をクリックします。個別のルールをクリアするには、Ctrl キーを押しながら各ルールの行内の空白部分をクリックします。
- 選択したルールを切り取りまたはコピーするには、選択したルールの行の空白部分を右クリックして、[切り取り（Cut）] または [コピー（Copy）] を選択します。
- 切り取ったルールまたはコピーしたルールをルール リストに貼り付けるには、選択したルールを貼り付けるルールの行の空白部分を右クリックして、[上に貼り付け（Paste above）] または [下に貼り付け（Paste below）] を選択します。
- 選択したルールを移動するには、選択したルールを新しい位置の下にドラッグ アンド ドロップします。この移動先の位置は、ドラッグ時にポインタの上に表示される青い横線で示されます。
- ルールを削除するには、ルールの横にある削除アイコン（）をクリックして、[OK] をクリックします。
- 警告を表示するには、[警告の表示（Show Warnings）] をクリックします。

NAT ルールの警告とエラー

NAT ルールの条件が後続のルールによるトラフィックの照合をプリエンプション処理する場合があります。どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。いずれかの条件が異なっていた場合、後続のルールはプリエンプション処理されません。

NAT ポリシーの展開失敗の原因となるルールを作成した場合、ルールの横にエラー アイコン（）が表示されます。スタティック ルールに矛盾がある場合、または現時点で無効となるポリシーで使用されるネットワーク オブジェクトを編集した場合、エラーが発生します。たとえば、IPv6 アドレスのみを使用するようにネットワーク オブジェクトを変更した結果、少なくとも 1 つのネットワークが必要な状況で、そのオブジェクトを使用するルールに有効なネットワークがなくなると、エラーが発生します。エラー アイコンは自動的に表示されます。[警告を表示（Show Warnings）] をクリックする必要はありません。

NAT ルール警告の表示と非表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）] > [NAT]**を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 警告を表示するには、[警告を表示（Show Warnings）] をクリックします。

ページが更新され、プリエンプション処理された各ルールの横に警告アイコン（）が表示されます。

ステップ 4 ルールの警告を表示するには、ルールの横にある警告アイコン（）の上にポインタを合わせます。

ルールをプリエンプション処理するルールを示すメッセージが表示されます。

ステップ 5 警告をクリアするには、[警告を非表示（Hide Warnings）] をクリックします。

ページが更新され、警告が消えます。

NAT ポリシー規則のオプション

NAT ルールは次の働きを持つ設定および条件のセットです。

- ネットワーク トラフィックを限定する

- 条件に一致するトラフィックの変換方法を指定する

既存の NAT ポリシーから NAT ルールを作成および編集します。各ルールは 1 つのポリシーにのみ属します。

ルールの追加と編集は同様の Web インターフェイスで行います。ページの上部でルールの名前、状態、タイプ、および位置（ダイナミックの場合）を指定します。ページの左側のタブを使用して、条件を構築します。条件タイプごとに独自のタブがあります。

次のリストは、NAT ルールの設定可能なコンポーネントを示しています。

[名前（Name）]

各ルールに一意の名前を付けます。スタティック NAT ルールでは、最大 22 文字を使用します。ダイナミック NAT ルールでは、最大 30 文字を使用します。印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン（:）は使用できません。

ルール状態（Rule State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、変換用のネットワーク トラフィックの評価に使用されません。NAT ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。

タイプ（Type）

ルールのタイプによって、ルールの条件に一致するトラフィックの処理方法が決まります。NAT ルールを作成および編集する際、設定可能なコンポーネントはルール タイプによって異なります。

位置（Position）（ダイナミック ルールのみ）

NAT ポリシーのダイナミック ルールには 1 から始まる番号が付いています。システムは、ルール番号の昇順で、NAT ルールを上から順にトラフィックと照合します。

ルールをポリシーに追加する際、参照ポイントとしてルール番号を使用し、特定のルールの**上**または**下**に配置することによって位置を指定します。既存のルールを編集するときには、同様の方法でルールを**移動**できます。

条件（Conditions）

ルール条件は変換する特定のトラフィックを識別します。条件はセキュリティ ゾーン、ネットワーク、および転送プロトコルのポートなど、複数の属性を任意に組み合わせてトラフィックと照合できます。

関連トピック

NAT ルールの作成および編集 （7 ページ）

NAT ルールの作成および編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

マルチドメイン導入では、現在のドメインで作成されたポリシーとルールが表示されます。これは編集できます。先祖ドメインで作成されたポリシーとルールも表示されますが、これは編集できません。下位のドメインで作成されたルールを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]**を選択します。

ステップ 2 ルールを追加する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 新しいルールを追加するか、既存のルールを編集します。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（）をクリックします。

ステップ 4 [名前（Name）] に一意のルール名を入力します。

ステップ 5 次のルール コンポーネントを設定します。

- ルールを**有効**にするかどうかを指定します。
- [タイプ（Type）] で、ルール タイプを指定します。
- ルールの位置（ダイナミック ルールのみ）を指定します。
- ルールの条件を設定します。

（注） スタティック ルールは元の宛先ネットワークを含む必要があります。ダイナミック ルールは変換された送信元ネットワークを含む必要があります。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

NAT ルールのタイプ

すべての NAT ルールには次の働きを持つタイプが関連付けられています。

- ネットワーク トラフィックを限定する
- 条件に一致するトラフィックの変換方法を指定する

次に、NAT ルール タイプの概要を示します。

静的

スタティック ルールは宛先ネットワークと任意選択のポートおよびプロトコルで 1 対 1 の変換を提供します。スタティック変換を設定する場合、送信元ゾーン、宛先ネットワーク、および宛先ポートを設定できます。宛先ゾーンまたは送信元ネットワークを設定できません。

元の宛先ネットワークを指定する**必要**があります。宛先ネットワークでは、単一の IP アドレスを含むネットワーク オブジェクトおよびグループを選択するか、または単一の IP アドレスを表すリテラル IP アドレスを入力することのみが可能です。元の宛先ネットワークと変換後の宛先ネットワークはそれぞれ 1 つのみ指定できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

元の宛先ポートと変換後の宛先ポートをそれぞれ 1 つ指定できます。元の宛先ポートを指定するには、その前に、元の宛先ネットワークを指定する必要があります。さらに、元の宛先ポートを指定しない場合は、変換後の宛先ポートを指定できません。また、変換後の値は、元の値のプロトコルと一致する必要があります。

注意 高可用性ペアとして構成されている 7000 または 8000 シリーズ デバイスのスタティック NAT ルールについては、NAT 変換で影響を受けるすべてのネットワークがプライベートの場合、個別のピア インターフェイスのみを選択します。パブリック ネットワークとプライベート ネットワーク間のトラフィックに影響するスタティック NAT ルールに対してこの設定を使用**しない**でください。

ダイナミック IP 専用

ダイナミック IP 専用ルールは多対多の送信元ネットワークを変換しますが、ポートおよびプロトコルを維持します。ダイナミック IP 専用変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも1つ指定する**必要**があります。変換後の送信元ネットワーク値の数が元の送信元ネットワークの数よりも小さい場合、元のアドレスがすべて照合される前に変換後のアドレスが不足する可能性があるという警告がルールに表示されます。

同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッドルールとなり、トリガーされなくなります。デッドルールにも警告が表示されます。ツールチップを表示して、デッドルールに代わるルールを判別できます。

（注） デッドルールを持つポリシーを保存し、展開することは可能ですが、ルールは変換を実現できません。

場合によっては、範囲の広いルールよりも優先される、範囲が限定されたルールを作成することをお勧めします。次に例を示します。

```
Rule 1: Match on address A and port A/Translate to address B
Rule 2: Match on address A/Translate to Address C
```

この例で、ルール1はルール2にも一致するいくつかのパケットに一致します。したがって、ルール2は完全に無効ではありません。

元の宛先ポートだけを指定した場合、変換後の宛先ポートを指定することはできません。

ダイナミック IP およびポート

ダイナミック IP およびポート ルールは多対 1 または多対多の送信元ネットワークとポートおよびプロトコルを変換します。ダイナミック IP およびポート変換を設定する場合、ゾーン、送信元ネットワーク、元の宛先ネットワーク、および元の宛先ポートを設定できます。変換後の宛先ネットワークまたは変換後の宛先ポートは設定できません。

変換後の送信元ネットワークを少なくとも1つ指定する**必要**があります。同じパケットに一致する条件を持つルールが複数個ある場合、優先度の低いルールはデッドルールとなり、トリガーされなくなります。デッドルールにも警告が表示されます。ツールチップを表示して、デッドルールに代わるルールを判別できます。

（注） デッドルールを持つポリシーを保存し、展開することは可能ですが、ルールは変換を実現できません。

元の宛先ポートだけを指定した場合、変換後の宛先ポートを指定することはできません。

（注） ダイナミック IP およびポート ルールを作成し、システムがポートを使用しないトラフィックを渡す場合、そのトラフィックに対して変換は発生しません。たとえば、送信元ネットワークに一致する IP アドレスからの ping（ICMP）は、ICMP がポートを使用しないため、マッピングされません。

NAT ルールの条件タイプ

次の表に、指定された NAT ルール タイプに基づいて設定可能な NAT ルールの条件タイプをまとめています。

表 *1: NAT* ルール タイプごとに使用可能な *NAT* ルールの条件タイプ

条件	静的	ダイナミック（IP 専用または IP およびポート）
送信元ゾーン（Source Zones）	オプション	オプション
宛先ゾーン（Destination Zones）	不可	オプション
元の送信元ネットワーク	不可	オプション
変換後の送信元ネットワーク	不可	**必須（Required）**
元の宛先ネットワーク	**必須（Required）**	オプション
変換後の宛先ネットワーク	任意。単一アドレスのみ	不可
元の宛先ポート	任意。単一ポートでのみ、元の宛先ネットワークを定義する場合のみ可能	オプション
変換後の宛先ポート	任意。単一ポートでのみ、元の宛先ポートを定義する場合のみ可能	不可

NAT ルールの条件と条件の仕組み

ルールに一致するトラフィックのタイプを識別するために NAT ルールに条件を追加できます。それぞれの条件タイプごとに、使用可能条件リストから、ルールに追加する条件を選択します。条件フィルタを適用できる場合は、条件フィルタを使って使用可能な条件を限定できます。使用可能な条件リスト、および選択した条件リストは、1 つの条件だけを含む場合も、数ページに及ぶ場合もあります。使用可能な条件は検索することができ、名前や値を入力するとそれに一致する条件だけが表示され、入力していくにつれてそのリストが更新されます。

条件のタイプに応じて、使用可能条件リストには、Cisco から直接提供された条件と、他の Firepower システム機能を使って設定された条件が一緒に含まれることがあります。その中には、オブジェクト マネージャ（**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**）を使って作成されたオブジェクト、個別の条件ページから直接作成されたオブジェクト、およびリテラル条件が含まれます。

NAT ルールの条件

次の表で説明されている条件のいずれかを満たすトラフィックを照合するための NAT ルールを設定できます。

表 *2 : NAT* ルールの条件タイプ

条件	説明
ゾーン	NAT ポリシーを展開できる 1 つ以上のルーテッド インターフェイスの設定。ゾーンは、送信元インターフェイスと宛先インターフェイスでトラフィックを分類するメカニズムであり、ルールに送信元のゾーン条件と宛先のゾーン条件を追加することができます。
ネットワーク	明示的に指定した、またはネットワーク オブジェクトとグループを使用した、個々の IP アドレス、CIDR ブロック、およびプレフィックス長の組み合わせ。NAT ルールに送信元ネットワーク条件と宛先ネットワーク条件を追加できます。
宛先ポート	トランスポート プロトコルに基づいて作成される、個別のポート オブジェクトとグループ ポート オブジェクトを含むトランスポート プロトコル ポート。

NAT ルールへの条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

NAT ルールへの条件の追加は基本的にどの条件のタイプでも同じです。左側の使用可能な条件のリストから選択して、右側で選択した条件の 1 つまたは 2 つのリストに、選択した条件を追加します。

すべての条件タイプで、使用可能な個々の条件を 1 つまたは複数クリックすると、それが強調表示され、選択状態になります。2 つのタイプのリスト間にあるボタンをクリックして選択した使用可能な条件を選択した条件のリストに追加するか、または選択した使用可能な条件を選択した条件のリストにドラッグ アンド ドロップします。

選択済み条件リストには、タイプごとに最大 50 個までの条件を追加できます。たとえばアプライアンスの上限に達するまで、最大 50 個の送信元ゾーン条件、最大 50 個の宛先ゾーン条件、最大 50 個の送信元ネットワーク条件などを追加できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 ルールに追加する条件タイプに対応したタブをクリックします。

ステップ 7 次のいずれかの操作を行います。

- 表示されている条件を、すでに選択済みの条件のリストに追加するには、表示されている条件をクリックします。
- 表示されている条件をすべて選択するには、条件のいずれかの行を右クリックし、[すべて選択（Select All）] をクリックします。
- 表示されている条件の一部またはフィルタされた条件を選択するには、[検索（Search）] フィールド内をクリックし、検索のための文字列を入力します。入力していくと、リストが更新されて一致する項目が表示されます。

  オブジェクト名およびオブジェクトに設定されている値を検索対象にできます。たとえば `Texas Office` という名前の個別ネットワーク オブジェクトがあり、`192.168.3.0/24` という値が設定されていて、`US Offices` というグループ オブジェクトに含まれる場合、`Tex` などの部分的または完全な検索文字列を入力するか、または `3` などの値を入力することにより、両方のオブジェクトを表示できます。

- 表示されている条件を検索中、またはフィルタ中に検索文字列をクリアするには、検索フィールドの上のリロード アイコン（  ）または検索フィールド内のクリア アイコン（）をクリックします。
- 表示されている条件リストからゾーンの条件を選択し、選択済みの送信元または宛先の条件リストに追加するには、[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックします。
- 表示されている条件リストからネットワークとポートの条件を選択し、選択済みの元または変換済みの条件リストに追加するには、[元に追加（Add to Original）] または [変換済みに追加（Add to Translated）] をクリックします。
- 表示されている条件を選択済み条件のリストにドラッグ アンド ドロップするには、選択済み条件をクリックし、選択済み条件のリストにドラッグ アンド ドロップします。
- リテラルフィールドを使用し、選択済み条件のリストにリテラル条件を追加するには、クリックしてリテラルフィールドからのプロンプトを削除し、リテラル条件を入力し、[追加（Add）] をクリックします。ネットワーク条件は、リテラル条件を追加するためのフィールドを提供します。
- ドロップダウン リストを使用し、選択済み条件のリストにリテラル条件を追加するには、ドロップダウン リストから条件を選択し、[追加（Add）] をクリックします。ポート条件には、リテラル条件を追加するためのドロップダウン リストがあります。
- 個々のオブジェクトまたは条件フィルタを追加して、条件リストからそれを選択できるよう表示させるには、追加アイコン（  ）をクリックします。

- 選択済み条件のリストから条件を 1 つだけ削除するには、条件の横にある削除アイコン（）をクリックします。
- 選択済み条件のリストから条件を削除するには、選択済み条件のリストの行を右クリックして強調表示し、[削除（Delete）] をクリックします。

ステップ 8 設定を保存するには、[追加（Add）] をクリックします。

NAT ルールのリテラル条件

次の条件タイプについて、元のおよび変換後の条件のリストにリテラル値を追加できます。

- ネットワーク
- ポート

ネットワーク条件の場合、元のまたは変換後の条件リストの下にある設定フィールドにリテラル値を入力します。

ポート条件では、ドロップダウン リストからプロトコルを選択します。プロトコルが `All`、または `TCP` または `UDP` である場合、設定フィールドにポート番号を入力します。

該当するそれぞれの条件ページには、リテラル値を追加するために必要なコントロールがあります。設定フィールドに入力した値が無効である場合や、まだ有効と認識されていない場合は、赤いテキストとして表示されます。入力時に有効と認識された値は青色に変わります。有効な値が認識されると、グレー表示の [追加（Add）] ボタンがアクティブになります。追加したリテラル値は、選択済み条件リストにただちに表示されます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

NAT ルールの条件のオブジェクト

オブジェクト マネージャ（**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**）で作成されたオブジェクトは、使用可能な NAT ルール条件の関連リストからすぐに選択可能になります。

NAT ポリシーから直接オブジェクトを作成することもできます。該当する条件ページ上のコントロールでは、オブジェクト マネージャでの設定コントロールと同じ機能を利用できます。

直接作成された個別のオブジェクトは使用可能なオブジェクトのリストにすぐに表示されます。それらを現在のルールと他の既存および将来のルールに追加できます。該当する条件ページとポリシー編集ページで、ポインタを 1 つの個別オブジェクトの上に置くとそのオブジェク

トの内容が表示され、グループ オブジェクトの上に置くと、グループ内の個々のオブジェクトの数が表示されます。

NAT ルール内のゾーン条件

システムのセキュリティ ゾーンは、管理対象デバイス上のインターフェイスから構成されています。NAT ルールに追加するゾーンは、それらのゾーン内にルーテッド インターフェイスまたはハイブリッド インターフェイスを持つ、ネットワーク上のデバイスにそのルールをターゲットします。NAT ルールの条件として、ルーテッド インターフェイスまたはハイブリッド インターフェイスを持つセキュリティ ゾーンのみを追加できます。

現在仮想ルータに割り当てられているゾーンまたはスタンドアロンインターフェイスのどちらかをNATルールに追加できます。デバイス設定が展開されていないデバイスがある場合、[ゾーン（Zones）] ページの使用可能なゾーン リストの上に警告アイコン（⚠）が表示され、展開済みのゾーンとインターフェイスだけが表示されることが示されます。ゾーンの横にある矢印アイコン（▷）をクリックして、ゾーンを縮小または展開し、そのインターフェイスを非表示または表示することができます。

インターフェイスがハイ アベイラビリティペアの 7000 または 8000 シリーズ デバイス上にある場合、使用可能なゾーンのリストに、そのインターフェイスからの追加のブランチが表示されると共に、そのハイ アベイラビリティ ペアの他のインターフェイスがそのハイ アベイラビリティ ペアのアクティブ デバイスのプライマリ インターフェイスの子として表示されます。矢印アイコン（▷）をクリックして、ペアになったデバイスインターフェイスを縮小または展開し、そのインターフェイスを非表示または表示することもできます。

（注） 無効にされたインターフェイスを持つポリシーを保存して展開できますが、ルールではそれらのインターフェイスが有効になるまで変換を提供できません。

右側の 2 つのリストは、NAT ルールによって照合目的に使用される送信元ゾーンと宛先ゾーンです。すでにルールに値が設定されている場合、ルールを編集する際、これらのリストには既存の値が表示されます。送信元ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイスからのトラフィックを照合します。宛先ゾーンのリストが空の場合、ルールは任意のゾーンまたはインターフェイス宛てのトラフィックを照合します。

対象のデバイスでトリガーされることがないゾーンの組み合わせを持つルールに対しては警告が表示されます。

（注） これらのゾーンの組み合わせを持つポリシーを保存して展開できますが、ルールでは変換を提供しません。

ゾーン内の項目を選択するか、またはスタンドアロンインターフェイスを選択することによって、個別のインターフェイスを追加できます。ゾーン内のインターフェイスを追加できるのは、それらのインターフェイスが割り当てられるゾーンがまだ送信元ゾーンまたは宛先ゾーン

のリストに追加されていない場合のみです。これらの個別に選択されたインターフェイスは、それらのインターフェイスを削除して別のゾーンに追加した場合でも、各ゾーンに対する変更の影響を受けません。インターフェイスがハイ アベイラビリティ ペアのプライマリ メンバーで、ダイナミック ルールを設定する場合、そのプライマリ インターフェイスだけを送信元ゾーンまたは宛先ゾーンのリストに追加できます。スタティック ルールの場合、個別のハイ アベイラビリティ ペアのメンバー インターフェイスを送信元ゾーンのリストに追加できます。ハイ アベイラビリティ ペアのプライマリ インターフェイスは、その子がまったく追加されていない場合にだけ、リストに追加できます。また、個別のハイ アベイラビリティ ペアのインターフェイスは、プライマリが追加されていない場合にだけ追加できます。

ゾーンを追加すると、ルールではそのゾーンに関連付けられているすべてのインターフェイスを使用します。ゾーンに対してインターフェイスを追加または削除すると、インターフェイスが存在するデバイスにデバイス設定が再度展開されるまで、ルールでは更新されたバージョンのゾーンを使用しません。

（注） スタティック NAT ルールでは、送信元ゾーンのみを追加できます。ダイナミック NAT ルールでは、送信元ゾーンと宛先ゾーンの両方を追加できます。

NAT ルールへのゾーン条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）] > [NAT]**を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 [ゾーン（Zones）] タブをクリックします。

ステップ 7 [使用可能なゾーン（Available Zones）] リスト内のゾーンまたはインターフェイスをクリックします。

ステップ 8 次の選択肢があります。

- 送信元ゾーンによりトラフィックを照合するには、[送信元に追加（Add to Source）] をクリックします。
- 宛先ゾーンによりトラフィックを照合するには、[宛先に追加（Add to Destination）] をクリックします。

（注） スタティック NAT ルールには送信元ゾーンのみを追加できます。さらに、無効になっているインターフェイスを NAT ルールに追加できますが、ルールは変換を実現しません。

ステップ 9 [追加（Add）] をクリックして新しいルールを保存します。

ステップ 10 [保存（Save）] をクリックして、変更したポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

ダイナミック NAT ルールの送信元ネットワーク条件

パケットの送信元 IP アドレスの照合値と変換値を設定します。元の送信元ネットワークが設定されていない場合、すべての送信元 IP アドレスがダイナミック NAT ルールに一致します。スタティック NAT ルールの送信元ネットワークは設定できないことに注意してください。パケットが NAT ルールに一致すると、システムは変換後の送信元ネットワークの値を使用して、送信元 IP アドレスの新しい値を割り当てます。ダイナミック ルール用に少なくとも 1 つの値を持つ変換後の送信元ネットワークを設定する必要があります。

⚠

注意 ネットワーク オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

ダイナミック NAT ルールに、次の種類の送信元ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト
- 送信元ネットワーク条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ネットワーク条件のダイナミック NAT ルールへの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

展開されているポリシーで使用中のダイナミック ルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]**を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールのダイナミック [タイプ（Type）] を指定します。

- **ダイナミック IP 専用**
- **ダイナミック IP およびポート**

ステップ 6 [送信元ネットワーク（Source Network）] タブをクリックします。

ステップ 7 必要に応じて、リストの上にある追加アイコン（）をクリックし、[使用可能なネットワーク（Available Networks）] リストへ個々のネットワーク オブジェクトを追加します。

各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。

ステップ 8 [使用可能なネットワーク（Available Networks）] リスト内の条件をクリックします。

ステップ 9 次の選択肢があります。

- 元の送信元ネットワークによりトラフィックを照合するには、[元に追加（Add to Original）] をクリックします。

- 変換後の送信元ネットワークと照合するトラフィックの変換値を指定するには、[変換後に追加（Add to Translated）] をクリックします。

ステップ 10 リテラル IP アドレス、範囲、アドレスブロックを追加するには、

a) [元の送信元ネットワーク（Original Source Network）] または [変換後の送信元ネットワーク（Translated Source Network）] リストの下にある [IP アドレス入力（Enter an IP address）] プロンプトをクリックします。

b) IP アドレス、範囲、アドレスブロックを入力します。

範囲は、下位の IP アドレス - 上位の IP アドレスの形式で追加します。たとえば、`179.13.1.1-179.13.1.10` です。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

c) 入力した値の横にある [追加（Add）] をクリックします。

ステップ 11 [追加（Add）] をクリックしてルールを保存します。

ステップ 12 [保存（Save）] をクリックして、変更したポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

NAT ルールの宛先ネットワーク条件

パケットの宛先 IP アドレスの照合値と変換値を設定します。ダイナミック NAT ルールでは変換済み宛先ネットワークは設定できないことに注意してください。

スタティック NAT ルールは 1 対 1 変換であるため、[利用可能なネットワーク（Available Networks）] リストには単一の IP アドレスのみを含むネットワーク オブジェクトおよびグループのみが含まれます。スタティック変換では、[元の宛先ネットワーク（Original Destination Network）] リストと [変換済み宛先ネットワーク（Translated Destination Network）] リストにそれぞれ追加できるオブジェクトまたはリテラル値は 1 つのみです。

⚠

注意 ネットワーク オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールに、次の種類の宛先ネットワーク条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのネットワーク オブジェクト
- [宛先ネットワーク（Destination Network）] 条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のネットワーク オブジェクト
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック

  スタティック NAT ルールでは、リストにまだ値がない場合に限り、CIDR とサブネット マスク /32 のみを追加できます。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

NAT ルールへの宛先ネットワーク条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

展開されているポリシーで使用中のダイナミック ルールのネットワーク条件を更新すると、既存の変換済みアドレス プールを使用しているネットワーク セッションがドロップされます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]**を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 [宛先ネットワーク（Destination Network）] タブをクリックします。

ステップ 7 必要に応じて、リストの上にある追加アイコン（）をクリックし、[使用可能なネットワーク（Available Networks）] リストへ個々のネットワーク オブジェクトを追加します。

ダイナミック ルールの場合、各ネットワーク オブジェクトに複数の IP アドレス、CIDR ブロック、およびプレフィクス長を追加できます。スタティック ルールの場合、単一の IP アドレスのみを追加できます。

ステップ 8 [使用可能なネットワーク（Available Networks）] リスト内の条件またはオブジェクトをクリックします。

ステップ 9 次の選択肢があります。

- 元の宛先ネットワークによりトラフィックを照合するには、[元に追加（Add to Original）] をクリックします。
- 変換後の宛先ネットワークと照合するトラフィックの変換値を指定するには、[変換後に追加（Add to Translated）] をクリックします。

ステップ 10 オプションで、[元の宛先ネットワーク（Original Destination Network）] リストまたは [変換後の宛先ネットワーク（Translated Destination Network）] リストの下の [IP アドレス入力（Enter an IP address）] プロンプトをクリックし、次に、IP アドレスまたはアドレス ブロックを入力して、[追加（Add）] をクリックします。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックし、ポリシーの変更内容を保存します。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

NAT ルールでのポート条件

ルールにポート条件を追加することで、元の宛先ポートと変換後の宛先ポートおよび変換用の転送プロトコルに基づいてネットワーク トラフィックを照合できます。元のポートが設定されていない場合、すべての宛先ポートがルールと照合されます。パケットを NAT ルールと照合し変換後の宛先ポートが設定されていた場合、システムはその値にポートを変換します。ダイナミック ルールでは元の宛先ポートのみを指定できることに注意してください。スタティック ルールの場合、変換後の宛先ポートを定義できますが、元の宛先ポート オブジェクトまたはリテラル値と同じプロトコルを持つオブジェクトでのみ可能です。

システムは宛先ポートを、スタティック ルールの元の宛先ポート リスト内のポート オブジェクトまたはリテラル ポートの値、またはダイナミック ルールの複数の値と照合します。

スタティック NAT ルールは 1 対 1 変換であるため、[利用可能なポート（Available Ports）] リストには単一のポートのみを含むポート オブジェクトおよびグループのみが含まれます。スタティック変換では、単一のオブジェクトまたはリテラル値のみを [元のポート（Original Port）] リストと [変換済みポート（Translated Port）] リストの両方に追加できます。

ダイナミック ルールの場合は、ポートの範囲を追加できます。たとえば、元の宛先ポートを指定する場合、リテラル値として `1000-1100` を追加できます。

⚠

注意 ポート オブジェクトまたはオブジェクト グループが NAT ルールで使用されている場合に、オブジェクトまたはグループを変更または削除すると、ルールが無効になる可能性があります。

NAT ルールには、次の種類のポート条件を追加できます。

- オブジェクト マネージャを使って作成した個別およびグループのポート オブジェクト
- 宛先ポート条件のページから追加し、ユーザのルールと他の既存および将来のルールに追加可能な個別のポート オブジェクト
- TCP、UDP、またはすべて（TCP および UDP）の転送プロトコルとポートから構成されるリテラル ポート値

NAT ルールへのポートの条件の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	Control	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）] > [NAT]**を選択します。

ステップ 2 変更する NAT ポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を入力します。

ステップ 5 ルールの [タイプ（Type）] を指定します。

ステップ 6 [宛先ポート（Destination Port）] タブをクリックします。

ステップ 7 必要に応じて、[使用可能なポート（Available Ports）] リストの上にある追加アイコン（）をクリックし、リストに個別のポートオブジェクトを追加します。

追加する各ポート オブジェクトの 1 つのポートまたはポート範囲を指定できます。その後、ルールの条件として追加するオブジェクトを選択できます。スタティック ルールの場合、単一のポートを持つポート オブジェクトのみを使用できます。

ステップ 8 [使用可能なポート（Available Ports）] リスト内の条件をクリックします。

ステップ 9 次の選択肢があります。

- [元に追加（Add to Original）] をクリックします。

- [変換後に追加（Add to Translated）] をクリックします。
- 使用可能なポートをリストにドラッグ アンド ドロップします。

ステップ 10 リテラルポートを追加するには、次の手順を実行します。

a) [元のポート（Original Port）] または [変換後のポート（Translated Port）] リストの下にある [プロトコル（Protocol）] ドロップダウンリストからエントリを選択します。

b) ポートを入力します。

c) [追加（Add）] をクリックします。

ダイナミック ルールの場合、単一のポートまたは範囲を指定できます。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックし、ポリシーの変更内容を保存します。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。