



NAT ポリシーの使用

ネットワーク アドレス変換 (NAT) ポリシーは、システムがネットワーク アドレス変換を使用してルーティングを達成する方法を定めます。1 つ以上の NAT ポリシーを設定して、1 つ以上の管理対象デバイスに適用できます。各デバイスに同時に適用できるポリシーは 1 つです。

ポリシーに NAT ルールを追加して、システムがネットワーク アドレス変換を処理する方法を制御します。各ルールは、変換する特定のトラフィックを識別する、条件のセットを含みます。次のタイプの規則を作成できます。

- **スタティック**。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 変換を提供します。
- **ダイナミック IP**。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 およびポート**。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。

システムはダイナミック変換を検査する前に、スタティック変換に対してトラフィックを照合します。次に、トラフィックはダイナミック NAT ルールに対して順番に照合されます。最初に一致したルールによってトラフィックが処理されます。詳細については、[NAT ポリシー内のルールの編成 \(11-5 ページ\)](#) を参照してください。

展開にアクセス コントロール ポリシーが存在する場合、システムはアクセス制御を通過するまでトラフィックを変換しません。

アプライアンスで NAT ポリシーを設定および適用するには、適用先の各管理対象デバイスで **Control** ライセンスが有効になっている必要があります。また、NAT ポリシーを適用できるのは、仮想ルータまたはハイブリッド インターフェイスが設定された シリーズ 3 デバイスのみです。

NAT ポリシーを設定および展開した後、管理対象デバイスのコマンドライン インターフェイス (CLI) を使用して、展開のトラブルシューティングを行うことができます。CLI には設定、ルール定義、およびアクティブな変換という 3 種類の NAT 情報が表示されます。詳細については、[コマンドライン リファレンス \(D-1 ページ\)](#) を参照してください。

NAT ポリシーの作成および管理の詳細については、次の項を参照してください。

- [NAT ポリシーの計画と実装 \(11-2 ページ\)](#)
- [NAT ポリシーの設定 \(11-2 ページ\)](#)
- [NAT ポリシー内のルールの編成 \(11-5 ページ\)](#)
- [NAT ポリシーの管理 \(11-8 ページ\)](#)
- [NAT ルールの作成と編集 \(11-17 ページ\)](#)
- [NAT ルール タイプについて \(11-18 ページ\)](#)
- [NAT ルール条件と条件のしくみについて \(11-20 ページ\)](#)
- [NAT ルールのさまざまな条件タイプの使用 \(11-25 ページ\)](#)

NAT ポリシーの計画と実装

ライセンス:任意(Any)

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。この項では、NAT ポリシーを展開する方法の一部について説明します。



注意

クラスタ構成で、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、クラスタ 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。

NAT を設定して、内部サーバを外部ネットワークに公開できます。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。

NAT を設定して、内部ホストまたはサーバが外部アプリケーションに接続することを許可できます。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。

NAT を設定して、IP アドレスのブロックを使用することにより、外部ネットワークからプライベート ネットワーク アドレスを隠すことができます。これは内部ネットワーク アドレスをマスクする場合、内部ネットワークのニーズを満たす十分な外部 IP アドレスがある場合に便利です。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。

NAT を設定して、IP アドレスおよびポート変換の限定的なブロックを使用することにより、外部ネットワークからプライベート ネットワーク アドレスを隠すことができます。これは内部ネットワーク アドレスをマスクする場合で、内部ネットワークのニーズを満たす十分な外部 IP アドレスがない場合に便利です。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。

NAT ポリシーの設定

ライセンス:Control

サポートされるデバイス:シリーズ 3

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、ポリシーを適用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適用できます。

スタンドアロン デバイスと同様に、NAT ポリシーをクラスタ スタックを含むデバイス クラスタに適用できます。ただし、個別のクラスタ デバイスまたはクラスタ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クラスタ全体のインターフェイスのみを使用できます。



注意

クラスタ構成で、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、クラスタ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 クラスタでダイナミック NAT を設定した場合、両方のクラスタ 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。詳細については、[HA リンク インターフェイスの設定 \(4-69 ページ\)](#) を参照してください。

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 スタックに適用できます。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適用できますが、ルールは変換を実現しません。詳細については、[スタック構成のデバイスの管理 \(4-47 ページ\)](#) を参照してください。

次の表は、NAT ポリシーの [編集 (Edit)] ページで実行可能な設定アクションを示します。

表 11-1 NAT ポリシーの設定アクション

目的	操作
ポリシーの名前または説明を変更する	[名前 (Name)] フィールドまたは [説明 (Description)] フィールドをクリックして、必要に応じて文字を削除し、新しい名前または説明を入力します。
ポリシーの適用対象を管理する	詳細については、 NAT ポリシー ターゲットの管理 (11-4 ページ) を参照してください。
ポリシーの変更を保存する	[保存 (Save)] をクリックします。
ポリシーを保存し、適用する	[保存して適用 (Save and Apply)] をクリックします。詳細については、 NAT ポリシーの適用 (11-15 ページ) を参照してください。
ポリシーの変更をキャンセルする	[キャンセル (Cancel)] をクリックします。変更を行った場合は、次に [OK] をクリックします。
ポリシーにルールを追加する	[ルールの追加 (Add Rule)] をクリックします。詳細については、 NAT ルールの作成と編集 (11-17 ページ) を参照してください。 ヒント 既存のルールを右クリックし、[新しいルールの挿入 (Insert new rule)] を選択することもできます。
既存のルールを編集する	ルールの横にある編集アイコン (✎) をクリックします。詳細については、 NAT ルールの作成と編集 (11-17 ページ) を参照してください。 ヒント ルールを右クリックして、[編集 (Edit)] を選択することもできます。
ルールを削除する	ルールの横にある削除アイコン (🗑️) をクリックし、[OK] をクリックします。 ヒント 1 つ以上のルールを選択して削除するには、選択したルールの行の空白部分を右クリックし、[削除 (Delete)] を選択して [OK] をクリックします。
既存のルールを有効または無効にする	選択したルールを右クリックして [状態 (State)] を選択した後、[無効 (Disable)] または [有効 (Enable)] を選択します。無効なルールはグレーで表示され、ルール名の下に [(無効) ((disabled))] というマークが付きます。
特定のルール属性の設定ページを表示する	ルールの行で、該当する条件のカラムに示されている名前、値、またはアイコンをクリックします。たとえば、[送信元ネットワーク (Source Network)] 列の名前または値をクリックすると、選択したルールの [送信元ネットワーク (Source Network)] ページが表示されます。詳細については、 NAT ルールのさまざまな条件タイプの使用 (11-25 ページ) を参照してください。

NAT ポリシー ターゲットの管理

ライセンス:Control

サポートされるデバイス:シリーズ 3

NAT ポリシーを適用するには、その前に、ポリシーを適用するデバイス スタック、クラスタ、またはグループなどの管理対象デバイスを識別する必要があります。ポリシーを適用する管理対象デバイスは、ポリシーを作成または編集する際に特定できます。使用可能なデバイス、スタック、およびクラスタのリストを検索して、選択したデバイスのリストに追加できます。また、選択したデバイスをドラッグ アンド ドロップしたり、2つのリスト間のボタンを使用してデバイスを追加したりすることもできます。

異なるバージョンの FireSIGHT システムを実行中のスタック デバイスをターゲットにすることはできません(たとえば、デバイスのいずれかでのアップグレードが失敗します)。詳細については、[スタック構成のデバイスの管理\(4-47 ページ\)](#)を参照してください。

次の表では、対象のデバイスを管理する場合に実行可能な操作の概要を説明しています。



表 11-2 対象のデバイスの管理アクション

目的	操作
使用可能なデバイス、スタック、およびクラスタのリストを検索する	検索フィールド内をクリックして、検索文字列を入力します。検索文字列を入力すると、デバイスのリストが更新されて、検索文字列に一致するデバイス名が表示されます。
使用可能なデバイスの検索をクリアする	検索フィールドのクリア アイコン(✖)をクリックします。
選択されているターゲットのリストに追加するための使用可能なデバイス、スタック、またはクラスタを選択する	デバイス名をクリックします。複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。 ヒント 使用可能なデバイスを右クリックして、[すべて選択 (Select All)] をクリックすることもできます。
選択したデバイス、スタック、またはクラスタを追加する	[ポリシーに追加 (Add to Policy)] をクリックします。 ヒント 選択済みデバイスのリストにドラッグ アンド ドロップするという方法もあります。
[選択されたデバイス (Selected Devices)] リストから単一のデバイス、スタック、またはクラスタを削除する	デバイスの横にある削除アイコン(🗑)をクリックします。 ヒント デバイスを右クリックして、[削除 (Delete)] を選択することもできます。
選択済みデバイスのリストから複数のデバイスを削除する	Ctrl キーまたは Shift キーを押しながら複数のデバイスをクリックして選択したら、選択したデバイスの行を右クリックして強調表示し、次に [選択項目の削除 (Delete Selected)] をクリックします。
設定を保存する	[保存 (Save)] をクリックします。
変更を保存せずに設定を廃棄する	[キャンセル (Cancel)] をクリックします。

次の手順では、対象デバイスを管理するための NAT ポリシーの設定方法について説明します。NAT ポリシーを編集するための詳細な手順については、[NAT ポリシーの編集 \(11-9 ページ\)](#) を参照してください。

NAT ポリシーで対象のデバイスを管理する方法:

アクセス: Admin/Network Admin

-
- 手順 1** [デバイス (Devices)] > [NAT] を選択します。
[NAT] ページが表示されます。
- 手順 2** 設定する NAT ポリシーの横にある編集アイコン(✎)をクリックします。
[NAT ポリシー エディタ (NAT Policy Editor)] ページが表示されます。
- 手順 3** [ターゲット (Targets)] タブをクリックします。
[ターゲット (Targets)] ページが表示されます。
- 手順 4** (任意)[使用可能なデバイス (Available Devices)] リストの上にある [検索 (Search)] プロンプトをクリックして、名前を入力します。
検索文字列を入力すると、リストが更新されて、検索文字列に一致するデバイスが表示されます。クリア アイコン(✕)をクリックすることで、リストをクリアできます。
- 手順 5** 追加するデバイス、スタック、クラスタ、またはデバイス グループをクリックします。複数のデバイスを追加するには、Ctrl キーまたは Shift キーを使用します。
- 
- ヒント** 使用可能なデバイスを右クリックして、[すべて選択 (Select All)] をクリックすることもできます。
-
- 手順 6** [ポリシーに追加 (Add to Policy)] をクリックします。
選択したデバイスが追加されます。
- 
- ヒント** ドラッグ アンド ドロップしてデバイスを追加することもできます。
-
- 手順 7** (任意)削除アイコン(🗑)をクリックして、選択済みデバイスのリストからデバイスを削除します。または、Ctrl キーまたは Shift キーを押しながら複数のデバイスをクリックして選択し、選択したデバイスを右クリックして [選択項目の削除 (Delete Selected)] を選択します。
- 手順 8** [保存 (Save)] をクリックして、設定を保存します。または、[キャンセル (Cancel)] をクリックして、設定を廃棄します。
-

NAT ポリシー内のルールの編成

ライセンス:任意 (Any)

NAT ポリシーの [編集 (Edit)] 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。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。

システムはポリシーの [編集 (Edit)] 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規則はすべて無視します。

オプションで、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。[NAT ルールの作成と編集 \(11-17 ページ\)](#) を参照してください。

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 [静的変換 (Static Translations)] リストにのみ、ダイナミック ルールは [動的変換 (Dynamic Translations)] 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。



(注) スタティック ルールはコピーできますが、切り取ることはできません。

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、説明的な警告メッセージ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、システムはアクセス制御を通過するまでトラフィックを変換しません。

次の表に、ルールを編成するために実行できる操作を要約します。

表 11-3 NAT ルール編成アクション

目的	操作
ルールを選択する	ルールの行の空白部分をクリックします。複数のルールを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。選択したルールが強調表示されます。
ルールの選択をクリアする	ページの右下にある再ロードアイコン (🔄) 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る、またはコピーする	選択したルールの行の空白部分を右クリックし、[切り取り (Cut)] または [コピー (Copy)] を選択します。 ヒント スタティック ルールはコピーできますが、切り取ることはできません。
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	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、[上へ貼り付け (Paste above)] または [下へ貼り付け (Paste below)] を選択します。 ヒント スタティック ルールは [静的変換 (Static Translations)] リストにのみ、ダイナミック ルールは [動的変換 (Dynamic Translations)] リストにのみ貼り付けることができます。
選択したルールを移動する	選択したルールを新しい場所の下にドラッグ アンド ドロップします。ドラッグしたときにポインタの上に青い横線が表示される場所が移動先です。

表 11-3 NAT ルール編成アクション(続き)

目的	操作
ルールを削除する	<p>ルールの横にある削除アイコン()をクリックし、[OK] をクリックします。</p> <p>ヒント 選択したルールの行の空白部分を右クリックして [削除(Delete)] を選択した後、[OK] をクリックして、選択した 1 つ以上のルールを削除するという方法もあります。</p>
警告を表示する	[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の操作(11-7 ページ) を参照してください。

NAT ルールの警告とエラーの操作




ライセンス:任意(Any)


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ブ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ブション処理されません。

次の表に、警告の表示および消去を行うために実行可能なアクションを示します。

表 11-4 プリエンブション処理されたルールの警告アクション

目的	操作
警告を表示する	[警告の表示(Show Warnings)] をクリックします。ページが更新され、プリエンブ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。
ルールの警告を表示する	ルールの横の警告アイコン()の上にポインタを移動します。ルールをプリエンブ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。
警告を消去する	<p>[警告の非表示(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。</p> <p>ヒント ルールの追加または編集など、ページを更新する任意のアクションの実行、またはリロードアイコン()のクリックでも、警告は消えます。</p>

NAT ポリシーの適用が失敗す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。[警告の表示(Show Warnings)] をクリックする必要はありません。

NAT ポリシーの管理

ライセンス:Control

サポートされるデバイス:シリーズ 3

NAT ポリシーのページ([デバイス (Devices)] > [NAT])で、オプションの説明と次のステータス情報と共に、現在のすべての NAT ポリシーを名前別に表示できます。

- ターゲットデバイスに対してポリシーが最新の状態になっている(緑のテキスト)
- ターゲットデバイスに対してポリシーが失効している(赤のテキスト)






このページのオプションを使用して、ポリシーの比較、新しいポリシーの作成、ターゲットデバイスへのポリシーの適用、ポリシーのコピー、各ポリシーで最後に保存されたすべての設定を示すレポートの表示、およびポリシーの編集を行うことができます。



(注) 管理対象デバイスに NAT ポリシーを適用した後は、期限切れであってもポリシーを削除できません。その代わりに、ルールを持たない NAT ポリシーを適用して、適用済みの NAT ルールを管理対象デバイスから削除する必要があります。

次の表に、NAT ポリシーのページでポリシーを管理するために実行可能なアクションについて説明します。

表 11-5 NAT ポリシー管理アクション

目的	操作
新しい NAT ポリシーを作成する	[新しいポリシー (New Policy)] をクリックします。詳細については、 NAT ポリシーの作成 (11-9 ページ) を参照してください。
既存の NAT ポリシーの設定を変更する	編集アイコン() をクリックします。詳細については、 NAT ポリシーの編集 (11-9 ページ) を参照してください。
ポリシーのターゲットであるすべてのデバイスに NAT ポリシーを適用する	ポリシー適用アイコン() をクリックします。詳細については、 NAT ポリシーの適用 (11-15 ページ) を参照してください。
NAT ポリシーをコピーする	コピーアイコン() をクリックします。詳細については、 NAT ポリシーのコピー (11-11 ページ) を参照してください。
NAT ポリシーの現在の設定を示す PDF レポートを表示する	レポートアイコン() をクリックします。詳細については、 NAT ポリシーの表示 (11-11 ページ) を参照してください。
NAT ポリシーを比較する	[ポリシーの比較 (Compare Policies)] をクリックします。詳細については、 2 つの NAT ポリシーの比較 (11-12 ページ) を参照してください。
NAT ポリシーを削除する	削除アイコン() をクリックして [OK] をクリックするか、または、ポリシーを削除しない場合は [キャンセル (Cancel)] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザの未保存の変更が存在するかどうかも通知されます。 (注) 管理対象デバイスに NAT ポリシーを適用した後は、デバイスからそのポリシーを削除できません。その代わりに、ルールを持たない NAT ポリシーを適用して、適用済みの NAT ルールを管理対象デバイスから削除する必要があります。また、どのターゲットデバイスでも、最後に適用されたポリシーは期限切れであっても削除できません。ポリシーを完全に削除する前に、それらのターゲットに異なるポリシーを適用する必要があります。

NAT ポリシーの作成

ライセンス:Control

サポートされるデバイス:シリーズ 3

新しい NAT ポリシーを作成する場合、少なくとも一意の名前を付ける必要があります。ポリシーの作成時にポリシー ターゲットを特定する必要はありませんが、ポリシーを適用する前には、この手順に実行する必要があります。[NAT ポリシー ターゲットの管理\(11-4 ページ\)](#)を参照してください。ルールを持たない NAT ポリシーをデバイスに適用すると、そのデバイスからすべての NAT ルールが削除されます。

NAT ポリシーを作成する方法:

アクセス:Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [NAT] を選択します。
[NAT] ページが表示されます。
 - 手順 2 [新しいポリシー (New Policy)] をクリックします。
[新しい NAT ポリシー (New NAT Policy)] ポップアップ ウィンドウが表示されます。
 - 手順 3 [名前 (Name)] に一意のポリシー名を入力し、オプションで [説明 (Description)] にポリシーの説明を入力します。
スペースや特殊文字を含めて、印刷可能なすべての文字を使用できます。
 - 手順 4 [使用可能なデバイス (Available Devices)] から、ポリシーを適用するデバイスを選択します。
複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックするか、または右クリックをして [すべて選択 (Select All)] を選択します。表示されるデバイスを絞り込むには、[検索 (Search)] フィールドに検索文字列を入力します。検索をクリアするには、クリアアイコン (×) をクリックします。
 - 手順 5 [選択されたデバイス (Selected Devices)] に、選択したデバイスを追加します。それには、クリックしてドラッグするか、[ポリシーに追加 (Add to Policy)] をクリックします。
 - 手順 6 [保存 (Save)] をクリックします。
[NAT ポリシー編集 (NAT policy Edit)] ページが表示されます。ルールの追加を含め、新しいポリシーの設定方法については、[NAT ポリシーの編集\(11-9 ページ\)](#)を参照してください。ポリシーを有効にするには適用する必要があることに注意してください。[NAT ポリシーの適用\(11-15 ページ\)](#)を参照してください。
-

NAT ポリシーの編集

ライセンス:Control

サポートされるデバイス:シリーズ 3

[NAT ポリシー編集 (NAT policy Edit)] ページで、ポリシーを設定できます。詳細については、[NAT ポリシーの設定\(11-2 ページ\)](#)とを参照してください。

設定を変更すると、変更がまだ保存されていないことを通知するメッセージが表示されます。変更を維持するには、[NAT ポリシー編集 (NAT policy Edit)] ページを終了する前にポリシーを保存する必要があります。変更を保存しないでポリシーの [編集 (Edit)] ページを終了しようとすると、変更がまだ保存されていないことを警告するメッセージが表示されます。この場合、変更を破棄してポリシーを終了するか、ポリシーの [編集 (Edit)] ページに戻るかを選択できます。

セッションのプライバシーを保護するために、ポリシーの編集ページが非アクティブになってから 60 分後に、ポリシーの変更は廃棄され、NAT ページに戻ります。非アクティブの最初の 30 分後にメッセージが表示され、変更が廃棄されるまでの残り時間(分)が定期的に更新されます。ページで何らかの操作を行うとタイマーはリセットされます。

2つのブラウザ ウィンドウで同じポリシーを編集しようとすると、新しいウィンドウで編集を再開するか、元のウィンドウでの変更を破棄して新しいウィンドウで編集を続けるか、または2番目のウィンドウをキャンセルしてポリシーの [編集 (Edit)] ページに戻るかを選択するよう求めるプロンプトが出されます。

複数のユーザが同じポリシーを同時に編集する場合、各ユーザに対して、ポリシーの編集ページにメッセージが表示され、他のユーザによる未保存の変更があることが通知されます。変更を保存しようとするすべてのユーザに、変更を保存すると他のユーザの変更が上書きされることが警告されます。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。

インターフェイスのタイプを、そのインターフェイスがあるデバイスを対象とする NAT ポリシーでの使用が無効なタイプに変更した場合、ポリシーはそのインターフェイスに削除済みのラベルを付けます。NAT ポリシーの [保存 (Save)] をクリックすると、インターフェイスはポリシーから自動的に削除されます。

NAT ポリシーを編集する方法:

アクセス: Admin/Network Admin

-
- 手順 1** [デバイス (Devices)] > [NAT] を選択します。
[NAT] ページが表示されます。
- 手順 2** 設定する NAT ポリシーの横にある編集アイコン(✎)をクリックします。
[NAT ポリシー編集 (NAT policy Edit)] ページが表示されます。
- 手順 3** ポリシーを設定するには、[NAT ポリシーの設定 \(11-2 ページ\)](#) で説明しているいずれかの操作を実行します。
- 手順 4** 設定を保存または廃棄します。次の選択肢があります。
- 変更を保存し、編集を続行する場合は、[保存 (Save)] をクリックします。
 - 変更を保存し、ポリシーを適用する場合は、[保存して適用 (Save and Apply)] をクリックします。[NAT ポリシーの適用 \(11-15 ページ\)](#) を参照してください。
変更を有効にするには、ポリシーを適用する必要があります。
 - 変更を廃棄する場合は、[キャンセル (Cancel)] をクリックし、プロンプトが出たら [OK] をクリックします。
変更は廃棄され、[NAT] ページが表示されます。
-

NAT ポリシーのコピー


ライセンス:Control

サポートされるデバイス:シリーズ 3

NAT ポリシーをコピーして、名前を変更できます。ポリシーをコピーすると、そのポリシーのすべてのルールと設定がコピーされます。

NAT ポリシーをコピーする方法:

アクセス:Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [NAT] を選択します。
[NAT] ページが表示されます。
- 手順 2 設定する NAT ポリシーの横にあるコピー アイコン () をクリックします。
[NAT ポリシーのコピー (Copy NAT Policy)] ポップアップ ウィンドウが表示されます。
- 手順 3 [名前 (Name)] に一意のポリシー名を入力します。
スペースや特殊文字を含めてすべての印刷可能な文字を使用できます。
- 手順 4 [OK] をクリックします。
コピーしたポリシーは [NAT] ページに名前のアルファベット順に表示されます。
-

NAT ポリシーの表示

ライセンス:Control

サポートされるデバイス:シリーズ 3

NAT ポリシー レポートは、特定の時点でのポリシーとルール設定の記録です。このレポートは、監査目的や、現行の設定を調べるために使用できます。



ヒント

また、ポリシーを現在適用されているポリシーまたは別のポリシーと比較する NAT 比較レポートを生成することもできます。詳細については、[2つの NAT ポリシーの比較 \(11-12 ページ\)](#) を参照してください。

NAT ポリシー レポートには、次の表で説明するセクションが含まれます。

表 11-6 NAT ポリシー レポートのセクション

セクション	説明
タイトル ページ	ポリシー レポートの名前、ポリシーの最終変更日時、ポリシーの最終変更ユーザ名を示します。
目次	レポートの内容が記載されます。
ポリシー情報 (Policy Information)	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。 NAT ポリシーの編集 (11-9 ページ) を参照してください。

表 11-6 NAT ポリシー レポートのセクション(続き)


セクション	説明
デバイス ターゲット (Device Targets)	ポリシーがターゲットとする管理対象デバイスがリストされます。 NAT ポリシー ターゲットの管理(11-4 ページ) を参照してください。
ルール (Rule)	ポリシーの各ルールのルールタイプと条件を示します。 NAT ルールの作成と編集(11-17 ページ) を参照してください。
参照オブジェクト (Referenced Objects)	ポリシーで使用されているすべての個別オブジェクトとグループオブジェクトの名前および設定を、オブジェクトが設定された条件のタイプ(ゾーン、ネットワーク、およびポート)別に示します。

NAT ポリシー レポートを表示する方法:

アクセス: Admin/Network Admin

手順 1 [デバイス (Devices)] > [NAT] を選択します。

[NAT] ページが表示されます。

手順 2 レポートの生成対象とするポリシーの横にあるレポートアイコン()をクリックします。NAT ポリシー レポートを生成する前に、すべての変更を保存してください。保存された変更のみがレポートに表示されます。

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

2 つの NAT ポリシーの比較

ライセンス: Control

サポートされるデバイス: シリーズ 3

ポリシーの変更を確認するために、2 つの NAT ポリシーの違いを調べることができます。任意の 2 つのポリシーを比較することも、現在適用されているポリシーを別のポリシーと比較することもできます。オプションで、比較した後に PDF レポートを生成することで、2 つのポリシーの間の差異を記録できます。

ポリシーを比較するために使用できるツールは 2 つあります。

- 比較ビューは、2 つのポリシーを左右に並べて表示し、その差異のみを示します。比較ビューの左右のタイトルバーに、それぞれのポリシーの名前が表示されます。ただし、[実行中の設定 (Running Configuration)] を選択した場合、現在アクティブなポリシーは空白のバーで表されます。

このツールを使用すると、Web インターフェイスで 2 つのポリシーを表示してそれらに移動するときに、差異を強調表示することができます。

- 比較レポートは、ポリシー レポートと同様の形式ですが、2 つのポリシーの間の差異だけが、PDF 形式で記録されます。

これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

ポリシーの比較ツールの内容と使用方法の詳細については、次の項を参照してください。

- [NAT ポリシー比較ビューの使用\(11-13 ページ\)](#)
- [NAT ポリシー比較レポートの使用\(11-13 ページ\)](#)

NAT ポリシー比較ビューの使用

ライセンス:Control

サポートされるデバイス:シリーズ 3

比較ビューには、両方のポリシーが左右に並べて表示されます。それぞれのポリシーは、比較ビューの左右のタイトルバーに示される名前で特定されます。現在実行されている設定ではない2つのポリシーを比較する場合、最後に変更された日時とその変更を行ったユーザがポリシー名と共に表示されます。

2つのポリシー間の差異は、次のように強調表示されます。

- 青色は強調表示された設定が2つのポリシーで異なることを示し、差異は赤色で示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

次の表に、実行できる操作を記載します。

表 11-7 NAT ポリシー比較のビューのアクション

目的	操作
変更個別にナビゲートする	タイトルバーの上にある [前へ(Previous)] または [次へ(Next)] をクリックします。 左側と右側の間にある二重矢印アイコン(⇄)が移動し、表示している違いを示す [差異(Difference)] 番号が変わります。
新しいポリシー比較ビューを生成する	[新しい比較(New Comparison)] をクリックします。 [比較の選択(Select Comparison)] ウィンドウが表示されます。詳細については、 NAT ポリシー比較レポートの使用(11-13 ページ) を参照してください。
ポリシー比較レポートを生成する	[比較レポート(Comparison Report)] をクリックします。 ポリシー比較レポートは、2つのポリシーの間の差異だけをリストした PDF ドキュメントです。

NAT ポリシー比較レポートの使用

ライセンス:Control

サポートされるデバイス:シリーズ 3

NAT ポリシー比較レポートは、ポリシー比較ビューによって示される2つの NAT ポリシー間または1つのポリシーと現在適用されているポリシーの間のすべての差異を PDF 形式で表示する記録です。このレポートを使用することで、2つのポリシー設定の間の違いをさらに調べ、調査結果を保存して共有できます。

アクセス可能な任意のポリシーに関して、比較ビューから NAT ポリシー比較レポートを生成できます。ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式は、ポリシー レポートと同様です。唯一異なる点は、ポリシー レポートにはポリシーのすべての設定が記載される一方、ポリシー比較レポートにはポリシー間で異なる設定だけがリストされることです。NAT ポリシー比較レポートには、[NAT ポリシー レポートのセクション](#)の表で説明しているセクションが含まれます。

2 つの NAT ポリシーを比較する方法:

アクセス: Admin/Network Admin

-
- 手順 1** [デバイス (Devices)] > [NAT] を選択します。
[NAT] ページが表示されます。
- 手順 2** [ポリシーの比較 (Compare Policies)] をクリックします。
[比較の選択 (Select Comparison)] ウィンドウが表示されます。
- 手順 3** [比較対象 (Compare Against)] ドロップダウン リストから、比較するタイプを次のように選択します。
- 異なる 2 つのポリシーを比較するには、[他のポリシー (Other Policy)] を選択します。
ページが更新されて、[ポリシー A (Policy A)] と [ポリシー B (Policy B)] という 2 つのドロップダウンリストが表示されます。
 - 2 つのリビジョンを比較するには、[他のリビジョン (Other Revision)] を選択します。
ページが更新され、[ポリシー (Policy)]、[リビジョン A (Revision A)] および [リビジョン B (Revision B)] ドロップダウン リストが表示されます。
 - 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[実行中の設定 (Running Configuration)] を選択します。
ページが更新されて、[ターゲット/実行中の設定 A (Target/Running Configuration A)] と [ポリシー B (Policy B)] という 2 つのドロップダウンリストが表示されます。
- 手順 4** 選択した比較タイプに応じて、次のような選択肢があります。
- 2 つの異なるポリシーを比較する場合は、[ポリシー A (Policy A)] と [ポリシー B (Policy B)] ドロップダウンリストから比較するポリシーを選択します。
 - 2 つの異なるリビジョンを比較する場合、[リビジョン A (Revision A)] ドロップダウン リストと [リビジョン B (Revision B)] ドロップダウン リストから比較するリビジョンを選択します。
 - 現在実行されている設定を別のポリシーと比較する場合は、[ポリシー B (Policy B)] ドロップダウンリストから 2 目目のポリシーを選択します。
- 手順 5** ポリシー比較ビューを表示するには、[OK] をクリックします。
比較ビューが表示されます。
- 手順 6** オプションで、[比較レポート (Comparison Report)] をクリックして、NAT ポリシー比較レポートを生成します。
NAT ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。
-

NAT ポリシーの適用

ライセンス:Control

サポートされるデバイス:シリーズ 3

NAT ポリシーに変更を加えたら、ポリシーを1つ以上のデバイスに適用し、デバイスによって監視するネットワーク上に設定変更を実装する必要があります。ポリシーを適用するには、その前に、ポリシーを適用するターゲット デバイスを指定する必要があります。[NAT ポリシー ターゲットの管理\(11-4 ページ\)](#)を参照してください。

NAT ポリシーを適用する場合は、次の点に注意してください。

- Defense Center では複数の NAT ポリシーを設定および保持できますが、1つのデバイスに一度に適用可能なポリシーは1つだけです。
- デバイスがいずれも複数のポリシーのターゲットであっても、2つの異なる NAT ポリシーを異なるデバイスに適用できます。
- 複数の異なるバージョンの FireSIGHT システムを実行中のスタック デバイスに NAT ポリシーを適用することはできません(たとえば、一方のデバイスでアップグレードに失敗した場合など)。詳細については、[スタック構成のデバイスの管理\(4-47 ページ\)](#)を参照してください。
- 適用が保留されているポリシーがある場合、新しい NAT ポリシーを適用できません。
- NAT ポリシーのインターフェイスに影響するデバイス設定を適用すると、インターフェイスの変更を含め、デバイスの NAT ポリシーが再適用されます。ただし、ポリシーは DC で変更されず、インターフェイスにはエラー アイコン(❗)が表示されます。



(注) 空の NAT ポリシーを適用すると、デバイスからすべての NAT ルールが削除されます。

詳細については、次の各項を参照してください。

- [完全な NAT ポリシーの適用\(11-15 ページ\)](#)ではクイック適用オプションを使用して NAT ポリシーを適用する方法について説明します。
- [選択したポリシーの設定の適用\(11-16 ページ\)](#)では NAT ポリシー内の設定を選択して適用する方法について説明します。

完全な NAT ポリシーの適用

ライセンス:Control

サポートされるデバイス:シリーズ 3

NAT ポリシーはいつでも適用できます。NAT ポリシーを適用すると、関連するルール設定、オブジェクト、およびポリシーの変更もポリシーの対象となるデバイスに適用されます。ポップアップ ウィンドウを使用し、すべての変更を1つのクイック適用アクションとして適用できます。

完全な NAT ポリシーをクイック適用する方法:

アクセス:Admin/Network Admin

- 手順 1 [デバイス(Devices)] > [NAT] を選択します。
[NAT] ページが表示されます。
- 手順 2 適用するポリシーの横にある適用アイコン(✔)をクリックします。

[NAT ルールの適用 (Apply NAT Rules)] ポップアップ ウィンドウが表示されます。

または、ポリシーの [編集 (Edit)] ページで [保存して適用 (Save and Apply)] をクリックするという方法もあります。[NAT ポリシーの編集 \(11-9 ページ\)](#) を参照してください。

手順 3 [すべて適用 (Apply All)] をクリックします。

ポリシー適用タスクがキューに入れられます。[OK] をクリックして、[NAT] ページに戻ります。



ヒント

ポリシー適用タスクの進行状況は、[タスク ステータス (Task Status)] ページ ([システム (System)] > [モニタリング (Monitoring)] > [タスク ステータス (Task Status)]) でモニタできます。

選択したポリシーの設定の適用

ライセンス: Control

サポートされるデバイス: シリーズ 3

詳細なポリシー適用ページを使用して、NAT ポリシーおよび任意の指定ターゲット デバイスに変更を適用できます。詳細ページには、ポリシーのターゲットである各デバイスが表示され、デバイス別に NAT ポリシーを表す列が含まれます。期限切れの各ターゲット デバイスに対して、NAT ポリシーに変更を適用するかどうかを指定できます。

選択した NAT ポリシー設定を適用する方法:

アクセス: Admin/Network Admin

手順 1 [デバイス (Devices)] > [NAT] を選択します。

[NAT] ページが表示されます。

手順 2 適用するポリシーの横にある適用アイコン (✓) をクリックします。

[NAT ルールの適用 (Apply NAT Rules)] ポップアップ ウィンドウが表示されます。

または、ポリシーの [編集 (Edit)] ページで [保存して適用 (Save and Apply)] をクリックするという方法もあります。[NAT ポリシーの編集 \(11-9 ページ\)](#) を参照してください。

手順 3 [詳細 (Details)] をクリックします。

詳細な [NAT ルールの適用 (Apply NAT Rules)] ポップアップ ウィンドウが表示されます。



ヒント

[NAT] ページ ([デバイス (Devices)] > [NAT]) で、ポリシーの [ステータス (Status)] 列の期限切れメッセージをクリックして、ポップアップ ウィンドウを開くこともできます。

手順 4 デバイス名の横の [NAT ポリシー (NAT policy)] チェック ボックスをオンまたはオフにして、ターゲット デバイスに NAT ポリシーを適用するかどうかを指定します。

手順 5 [選択した設定の適用 (Apply Selected Configurations)] をクリックします。

ポリシー適用タスクがキューに入れられます。[OK] をクリックして、[NAT] ページに戻ります。



ヒント

ポリシー適用タスクの進行状況は、[タスク ステータス (Task Status)] ページ ([システム (System)] > [モニタリング (Monitoring)] > [タスク ステータス (Task Status)]) でモニタできます。

NAT ルールの作成と編集

ライセンス:Control

サポートされるデバイス:シリーズ 3

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)]

各ルールに一意的な名前を付けます。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。スペースや特殊文字(「:」は除く)など、印刷可能文字を使用できます。

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。

ルールタイプとそれらが変換およびトラフィック フローに与える影響の詳細については、[NAT ルールタイプについて\(11-18 ページ\)](#)を参照してください。

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。詳細については、[NAT ポリシー内のルールの編成\(11-5 ページ\)](#)を参照してください。

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。

条件の追加の詳細については、[NAT ルール条件と条件のしくみについて\(11-20 ページ\)](#)および [NAT ルールのさまざまな条件タイプの使用\(11-25 ページ\)](#)を参照してください。

NAT ルールを作成または編集する方法:

アクセス: Admin/Network Admin

-
- 手順 1** [デバイス (Devices)] > [NAT] を選択します。
[NAT] ページが表示されます。
- 手順 2** ルールを追加する SSL ポリシーの横にある編集アイコン(✎)をクリックします。
[NAT ポリシー編集 (NAT policy Edit)] ページが表示されます。
- 手順 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。
- [ルールの追加 (Add Rule)] ページまたは [ルールの編集 (Editing Rule)] ページが表示されます。

**ヒント**

右クリック コンテキスト メニューを使用して、さまざまなルール作成/管理操作を実行することができます([コンテキスト メニューの使用 \(2-5 ページ\)](#) を参照)。また、ルールをドラッグ アンド ドロップして順序を変更することもできます。

-
- 手順 4** 前述の方法で、ルールのコンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。
- ルールに一意の名前 [名前 (Name)] を付ける必要があります。
 - ルールを有効にするかどうかを指定します。
 - ルールタイプを [タイプ (Type)] から選択します。
 - 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。
 - 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。
- 手順 5** [追加 (Add)] または [保存 (Save)] をクリックします。
- 変更が保存されます。変更内容を有効にするには、NAT ポリシーを適用する必要があります。 [NAT ポリシーの適用 \(11-15 ページ\)](#) を参照してください。
-

NAT ルールタイプについて

ライセンス: 任意 (Any)

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 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。

必要に応じて、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

クラスタ デバイスのスタティック NAT ルールに関して、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(無効)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、適用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 が完全に無効(デッド)ではありません。

必要に応じて、元の宛先ポートだけを指定できます。変換後の宛先ポートは指定できません。

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ある場合、優先度の低いルールはデッド(無効)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すると、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、適用することは可能ですが、ルールは変換を実現できません。

必要に応じて、元の宛先ポートだけを指定できます。変換後の宛先ポートは指定できません。



(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。

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 11-8 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 ルール条件と条件のしくみについて

ライセンス:任意 (Any)

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、シスコから直接提供された条件と、他の FireSIGHT 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。

ルール条件の指定については、次の項を参照してください。

- [NAT ルール条件について \(11-21 ページ\)](#) に、さまざまなタイプのルール条件の定義を示します。
- [NAT ルールへの条件の追加 \(11-22 ページ\)](#) に、ルール条件を選択および追加するためのコントロールを示しています。
- [NAT ルール条件リストの検索 \(11-24 ページ\)](#) では、使用可能な条件の検索方法を説明します。入力した名前や値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。
- [NAT ルールへのリテラル条件の追加 \(11-24 ページ\)](#) に、リテラル条件をルールに追加する方法の説明を示します。
- [NAT ルール条件でのオブジェクトの使用 \(11-25 ページ\)](#) では、該当する条件タイプの設定ページから個別のオブジェクトをシステムに追加する方法について説明します。

NAT ルール条件について

ライセンス:任意 (Any)

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 11-9 NAT ルールの条件タイプ

条件	説明	サポートされる Defense Center	サポートされる デバイス
ゾーン	NAT ポリシーを適用できる 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。オブジェクト マネージャを使ってゾーンを作成する方法については、 セキュリティ ゾーン の操作 (3-44 ページ) を参照してください。	Any	シリーズ 3
ネットワーク	明示的に指定された、またはネットワーク オブジェクトとグループ (ネットワーク オブジェクトの操作 (3-4 ページ) を参照) を使って指定された、個別の IP アドレス、CIDR ブロック、およびプレフィックス長からなる任意の組み合わせ。NAT ルールに送信元ネットワークおよび宛先ネットワークの条件を追加できます。	Any	シリーズ 3
宛先ポート (Destination Ports)	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。オブジェクト マネージャを使用して個別のトランスポートプロトコル オブジェクトとグループ トランスポートプロトコル オブジェクトを作成する方法については、 ポート オブジェクトの操作 (3-13 ページ) を参照してください。	Any	シリーズ 3

NAT ルールへの条件の追加

ライセンス:任意(Any)

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。

次の表に、条件を選択してルールに追加する際に実行できる操作の説明を示します。

表 11-10 NAT ルールへの条件の追加

目的	操作
使用可能な条件を選択して、選択済み条件のリストに追加する	使用可能な条件をクリックします。複数の条件を選択するには Ctrl キーと Shift キーを使用します。
リストされたすべての使用可能な条件を選択する	いずれかの使用可能な条件の行を右クリックし、[すべて選択 (Select All)] をクリックします。
使用可能な条件またはフィルタのリストを検索する	検索フィールド内をクリックし、検索文字列を入力します。詳細については、 NAT ルール条件リストの検索 (11-24 ページ) を参照してください。
使用可能な条件やフィルタを検索しているときに検索内容をクリアする	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。
使用可能な条件のリストから選択したゾーン条件を、選択した送信元または宛先の条件のリストに追加する	[送信元に追加 (Add to Source)] または [送信先に追加 (Add to Destination)] をクリックします。詳細については、 NAT ルールへのゾーン条件の追加 (11-26 ページ) を参照してください。
使用可能な条件のリストから選択したネットワークとポートの条件を、選択した元または変換後の条件のリストに追加する	[オリジナルに追加 (Add to Original)] または [変換後に追加 (Add to Translated)] をクリックします。詳細については、 ダイナミック NAT ルールへの送信元ネットワーク条件の追加 (11-28 ページ) 、 NAT ルールへの宛先ネットワーク条件の追加 (11-29 ページ) 、または NAT ルールへのポート条件の追加 (11-31 ページ) を参照してください。
選択した使用可能な条件を、選択済み条件リストにドラッグアンドドロップする	選択した条件をクリックし、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。
リテラルフィールドを使用して、選択済み条件リストにリテラル条件を追加する	クリックしてリテラルフィールドからプロンプトを除去し、リテラル条件を入力して、[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。

表 11-10 NAT ルールへの条件の追加(続き)

目的	操作
ドロップダウンリストを使用して、選択済み条件リストにリテラル条件を追加する	ドロップダウンリストから条件を選択して、[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。詳細については、 NAT ルールへのポート条件の追加(11-31 ページ) を参照してください。
個々のオブジェクトまたは条件フィルタを追加して、使用可能条件リストからそれを選択できるようにする	追加アイコン(+) をクリックします。オブジェクトマネージャを使ってオブジェクトを追加する方法については、 再利用可能なオブジェクトの管理(3-1 ページ) を参照してください。
選択済み条件リストから単一の条件を削除する	条件の横にある削除アイコン(🗑️) をクリックします。
選択済み条件リストから 1 つの条件を削除する	1 つの選択済み条件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。
選択済み条件リストから複数の条件を削除する	Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックして [すべて選択(Select All)] を選択します。次に、いずれかの選択済み条件の行を右クリックして強調表示し、[選択項目の削除(Delete Selected)] をクリックします。

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。

新しいルールに条件を追加する基本的な手順を次に示します。ルールの追加と変更に関する詳しい説明は、[NAT ルールの作成と編集\(11-17 ページ\)](#) を参照してください。

使用可能な条件を選択済み条件リストに追加する方法:

アクセス: Admin/Network Admin

-
- 手順 1 [デバイス(Devices)] > [NAT] を選択します。
[NAT] ページが表示されます。
 - 手順 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。
ポリシーの [編集(Edit)] ページが表示されます。
 - 手順 3 [ルールの追加(Add Rule)] をクリックします。
[ルールの追加(Add Rule)] ページが表示されます。
 - 手順 4 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。
選択した条件のタイプに対応する条件ページが表示されます。
 - 手順 5 [NAT ルールへの条件の追加](#)表に含まれているいずれかのアクションを実行します。
 - 手順 6 設定を保存するには、[追加(Add)] をクリックします。
ルールが追加され、ポリシー編集ページが表示されます。
-

NAT ルール条件リストの検索

ライセンス:任意(Any)

使用可能な NAT ルール条件のリストをフィルタして、リストに表示される項目の数を制限できます。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。

オプションで、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することができます。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。

新しいルールでリストをフィルタ処理する基本的な手順を次に示します。ルールの追加と変更に関する詳しい説明は、[NAT ルールの作成と編集\(11-17 ページ\)](#)を参照してください。

使用可能な条件のリストを検索する方法:

アクセス:Admin/Network Admin

-
- 手順 1** [デバイス (Devices)] > [NAT] を選択します。
[NAT] ページが表示されます。
- 手順 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。
ポリシーの [編集 (Edit)] ページが表示されます。
- 手順 3** [ルールの追加 (Add Rule)] をクリックします。
[ルールの追加 (Add Rule)] ページが表示されます。
- 手順 4** リストを検索するには、検索フィールド内部をクリックしてプロンプトをクリアした後、検索文字列を入力します。
入力していくとリストが更新され、一致する項目とクリアアイコン(✕)が検索フィールドに表示されます。検索文字列に一致する項目がない場合、リストが更新されて、リストには何も表示されません。
- 手順 5** オプションで、[検索 (Search)] フィールドの上のリロードアイコン(🔄)をクリックするか、[検索 (Search)] フィールド内のクリア アイコン(✕)をクリックして、検索文字列を消去します。
完全なリストが表示されます。
- 手順 6** 設定を保存するには、[追加 (Add)] をクリックします。
ルールが追加され、ポリシー編集ページが表示されます。
-

NAT ルールへのリテラル条件の追加

ライセンス:任意(Any)

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 [すべて (All)] の場合、またオプションでプロトコルが [TCP] または [UDP] の場合、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。

それぞれのタイプのリテラル値を追加する詳しい方法については、次を参照してください。

- [ダイナミック NAT ルールへの送信元ネットワーク条件の追加\(11-28 ページ\)](#)
- [NAT ルールへの宛先ネットワーク条件の追加\(11-29 ページ\)](#)
- [NAT ルールへのポート条件の追加\(11-31 ページ\)](#)

NAT ルール条件でのオブジェクトの使用

ライセンス:任意(Any)

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。詳細については、[再利用可能なオブジェクトの管理\(3-1 ページ\)](#)を参照してください。

NAT ポリシーからオブジェクトを直接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 ルールのさまざまな条件タイプの使用

ライセンス:任意(Any)

トラフィックを 1 つまたは複数のルール条件と照合できます。詳細については、次の各項を参照してください。

- [NAT ルールへのゾーン条件の追加\(11-26 ページ\)](#)ではオブジェクト マネージャを使用して作成したセキュリティゾーンにより、トラフィックを照合する方法について説明します。
- [ダイナミック NAT ルールへの送信元ネットワーク条件の追加\(11-28 ページ\)](#)および [NAT ルールへの宛先ネットワーク条件の追加\(11-29 ページ\)](#)では IP アドレスまたはアドレス ブロックによりトラフィックを照合する方法について説明します。
- [NAT ルールへのポート条件の追加\(11-31 ページ\)](#)では指定した転送プロトコル ポートにより、トラフィックを照合する方法について説明します。

NAT ルールへのゾーン条件の追加

ライセンス:任意(Any)

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で構成されます。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へのルールをターゲットにします。NAT ルールの条件として、ルーテッド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。オブジェクト マネージャを使ってセキュリティ ゾーンを作成する方法については、[セキュリティ ゾーン の操作 \(3-44 ページ\)](#) を参照してください。

仮想ルータに現在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。デバイス設定が適用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、適用済みのゾーンおよびインターフェイスのみ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クラスタ 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、クラスタ内の他のインターフェイスがクラスタ内のアクティブな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、クラスタ 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適用できますが、インターフェイスが有効になるまでルールは変換を実現できません。

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のゾーンです。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適用できますが、ルールは変換を実現しません。

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。割り当てられてい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、ゾーン内のインターフェイスを追加できます。これらの個別に選択されたインターフェイスは、削除して別のゾーンに追加した場合でも、ゾーンに対する変更に影響されません。インターフェイスがクラスタのプライマリ メンバーであり、ダイナミック ルールを設定する場合、プライマリ インターフェイスのみ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、送信元ゾーンのリストに個別のクラスタ メンバー インターフェイスを追加できます。プライマリ クラスタ 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だけ、リストに追加できます。また、個別のクラスタ 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だけ追加できます。

ゾーンを追加すると、ルールはゾーンに関連付けられた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適用されるまで、ルールはゾーンの更新バージョンを使用しません。



(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。

次の手順では、NAT ルールの追加または編集の際に、送信元と宛先のゾーン条件を追加する方法について説明します。詳細については、[NAT ルール条件と条件のしくみについて\(11-20 ページ\)](#)を参照してください。

ゾーン条件を NAT ルールに追加する方法:

アクセス: Admin/Network Admin

- 手順 1 ルール編集ページの [ゾーン(Zones)] タブを選択します。
[ゾーン(Zones)] ページが表示されます。
- 手順 2 必要に応じて、[使用可能なゾーン(Available Zones)] リストの上にある [名前を検索(Search by name)] プロンプトをクリックし、名前か値を入力します。
入力していくと、リストが更新されて一致する条件が表示されます。詳細については、[NAT ルール条件リストの検索\(11-24 ページ\)](#)を参照してください。
- 手順 3 [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。Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックして [すべて選択(Select All)] をクリックします。
選択した条件が強調表示されます。
- 手順 4 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、[送信先に追加(Add to Destination)] をクリックします。オプションで、選択した条件を [送信元ゾーン(Source Zones)] リストまたは [宛先ゾーン(Destination Zones)] リストにドラッグアンドドロップできます。
選択した条件が追加されます。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せんが、ルールは変換を実現しないことに注意してください。



(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。

- 手順 5 ルールを保存するか、編集を続けます。
変更内容を有効にするには、NAT ポリシーを適用する必要があります。[NAT ポリシーの適用\(11-15 ページ\)](#)を参照してください。

ダイナミック NAT ルールへの送信元ネットワーク条件の追加

ライセンス:任意(Any)

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
オブジェクト マネージャを使用して個別のネットワーク オブジェクトとグループ ネットワーク オブジェクトを作成する方法については、[ネットワーク オブジェクトの操作 \(3-4 ページ\)](#) を参照してください。
- 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
詳細については、[NAT ルール条件でのオブジェクトの使用 \(11-25 ページ\)](#) を参照してください。
- リテラル、単一 IP アドレス、範囲、またはアドレス ブロック
詳細については、[NAT ルールへのリテラル条件の追加 \(11-24 ページ\)](#) を参照してください。

次の手順では、ダイナミック NAT ルールの追加または編集の際に、送信元ネットワーク条件を追加する方法について説明します。詳細については、[NAT ルール条件と条件のしくみについて \(11-20 ページ\)](#) を参照してください。

ネットワーク条件をダイナミック NAT ルールに追加する方法:

アクセス:Admin/Network Admin

- 手順 1 ルールの編集ページの [送信元ネットワーク (Source Networks)] タブを選択します。
[送信元ネットワーク (Source Network)] ページが表示されます。
- 手順 2 必要に応じて、[使用可能なネットワーク (Available Networks)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、名前か値を入力します。
入力していくと、リストが更新されて一致する条件が表示されます。詳細については、[NAT ルール条件リストの検索 \(11-24 ページ\)](#) を参照してください。
- 手順 3 [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。Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックして [すべて選択 (Select All)] をクリックします。
選択した条件が強調表示されます。

手順 4 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、[オリジナルに追加(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。

または、選択した条件を [オリジナルの送信元ネットワーク (Original Source Network)] リストまたは [変換後の送信元ネットワーク (Translated Source Network)] リストにドラッグ アンド ドロップできます。

選択した条件が追加されます。

手順 5 オプションで、[使用可能なネットワーク (Available Networks)] リストの上にある追加アイコン (+) をクリックし、個別のネットワーク 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、およびプレフィックス長を追加できます。

その後、オプションで、追加済みのオブジェクトを選択できます。詳細については、[ネットワーク オブジェクトの操作\(3-4 ページ\)](#)と [NAT ルール条件でのオブジェクトの使用\(11-25 ページ\)](#)を参照してください。

手順 6 オプションで、[オリジナルの送信元ネットワーク (Original Source Network)] リストまたは [変換後の送信元ネットワーク (Translated Source Network)] リストの下の [IP アドレスを入力してください(Enter an IP address)] プロンプトをクリックします。次に、IP アドレス、範囲、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。

範囲は、「下位の IP アドレス-上位の IP アドレス」という形式で追加します。例：
179.13.1.1-179.13.1.10.

リストが更新されて、それらのエントリが表示されます。詳細については、[NAT ルールへのリテラル条件の追加\(11-24 ページ\)](#)を参照してください。

手順 7 ルールを保存するか、編集を続けます。



(注) 適用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。

変更内容を有効にするには、NAT ポリシーを適用する必要があります。[NAT ポリシーの適用\(11-15 ページ\)](#)を参照してください。

NAT ルールへの宛先ネットワーク条件の追加

ライセンス:任意(Any)

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 ルールの変換後の宛先ネットワークを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、[使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。スタティック変換用に、単一のオブジェクトまたはリテラル値のみを [オリジナルの宛先ネットワーク (Original Destination Network)] リストと [変換後の宛先ネットワーク (Translated Destination Network)] リストの両方に追加できます。



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。

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
オブジェクト マネージャを使用して個別のネットワーク オブジェクトとグループ ネットワーク オブジェクトを作成する方法については、[ネットワーク オブジェクトの操作 \(3-4 ページ\)](#)を参照してください。
- 宛先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
詳細については、[NAT ルール条件でのオブジェクトの使用 \(11-25 ページ\)](#)を参照してください。
- リテラル、単一 IP アドレス、範囲、あるいはアドレス 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。
詳細については、[NAT ルールへのリテラル条件の追加 \(11-24 ページ\)](#)を参照してください。

次の手順では、NAT ルールの追加または編集の際に、宛先ネットワーク条件を追加する方法について説明します。詳細については、[NAT ルール条件と条件のしくみについて \(11-20 ページ\)](#)を参照してください。

宛先ネットワーク条件を NAT ルールに追加する方法:

アクセス: Admin/Network Admin

-
- 手順 1** ルールの編集ページの [接続先ネットワーク (Destination Network)] タブを選択します。
[接続先ネットワーク (Destination Network)] ページが表示されます。
- 手順 2** 必要に応じて、[使用可能なネットワーク (Available Networks)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、名前か値を入力します。
入力していくと、リストが更新されて一致する条件が表示されます。詳細については、[NAT ルール条件リストの検索 \(11-24 ページ\)](#)を参照してください。
- 手順 3** [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。Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックして [すべて選択 (Select All)] をクリックします。
選択した条件が強調表示されます。
- 手順 4** 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、[オリジナルに追加 (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。
- または、選択した条件を [オリジナル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)] リストにドラッグアンドドロップできます。

選択した条件が追加されます。

- 手順 5** オプションで、[使用可能なネットワーク (Available Networks)] リストの上にある追加アイコン (+) をクリックし、個別のネットワーク 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、およびプレフィッ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。その後、オプションで、追加済みのオブジェクトを選択できます。詳細については、[ネットワーク オブジェクトの操作\(3-4 ページ\)](#)と [NAT ルール条件でのオブジェクトの使用\(11-25 ページ\)](#)を参照してください。
- 手順 6** オプションで、[オリジナル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 アドレスを入力してください (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。
- リストが更新されて、それらのエントリが表示されます。詳細については、[NAT ルールへのリテラル条件の追加\(11-24 ページ\)](#)を参照してください。
- 手順 7** ルールを保存するか、編集を続けます。



(注) 適用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。

変更内容を有効にするには、NAT ポリシーを適用する必要があります。[NAT ポリシーの適用\(11-15 ページ\)](#)を参照してください。

NAT ルールへのポート条件の追加

ライセンス:任意 (Any)

ルールにポート条件を追加し、元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に一致します。パケットが NAT ルールに一致し、変換後の宛先ポートが設定されている場合、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。スタティック変換用に、単一のオブジェクトまたはリテラル値のみを [オリジナルのポート (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、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、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
オブジェクト マネージャを使用して個別のポート オブジェクトとグループ ポート オブジェクトを作成する方法については、[ポート オブジェクトの操作\(3-13 ページ\)](#)を参照してください。
- 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
詳細については、[NAT ルール条件でのオブジェクトの使用\(11-25 ページ\)](#)を参照してください。
- 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
詳細については、[NAT ルールへのリテラル条件の追加\(11-24 ページ\)](#)を参照してください。

次の手順では、NAT ルールの追加または編集の際に、ポート条件を追加する方法について説明します。詳細については、[NAT ルール条件と条件のしくみについて\(11-20 ページ\)](#)を参照してください。

宛先ポート条件を NAT ルールに追加する方法:

アクセス:Admin/Network Admin

-
- 手順 1** ルールの編集ページの [接続先ポート (Destination Port)] タブを選択します。
[接続先ポート (Destination Port)] ページが表示されます。
- 手順 2** 必要に応じて、[利用可能なポート (Available Ports)] リストの上にある [名前または値で検索 (Search by name or value)] プロンプトをクリックし、名前または値を入力します。
入力していくと、リストが更新されて一致する条件が表示されます。詳細については、[NAT ルール条件リストの検索\(11-24 ページ\)](#)を参照してください。
- 手順 3** [利用可能なポート (Available Ports)] リスト内の条件をクリックします。Shift キーまたは Ctrl キーを押しながら複数の条件をクリックして選択するか、右クリックしてすべての条件を選択します。なお、最大で 50 個の条件を追加できます。
選択した条件が強調表示されます。
- 手順 4** 次の選択肢があります。
- [オリジナルに追加 (Add to Original)] をクリックして、選択したポートを [オリジナルのポート (Original Ports)] リストに追加します。
 - [変換後に追加 (Add to Translated)] をクリックして、選択したポートを [変換済みポート (Translated Ports)] リストに追加します。
 - 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。
- 手順 5** オプションで、個別のポート オブジェクトを作成して追加するには、[利用可能なポート (Available Ports)] リストの上の追加アイコン(+)をクリックします。
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。詳細については、[NAT ルール条件でのオブジェクトの使用\(11-25 ページ\)](#)を参照してください。
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。

- 手順 6** (任意)リテラル ポートを追加するには、[オリジナルのポート(Original Port)] リストまたは [変換済みポート(Translated Port)] リストの [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。
- ポートを入力し、[追加(Add)] をクリックします。0 から 65535 までのポート番号を指定できます。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。
- リストが更新され、選択内容が表示されます。詳細については、[NAT ルールへのリテラル条件の追加\(11-24 ページ\)](#)を参照してください。
- 選択した条件が追加されます。
- 手順 7** ルールを保存するか、編集を続けます。
- 変更内容を有効にするには、NAT ポリシーを適用する必要があります。[NAT ポリシーの適用\(11-15 ページ\)](#)を参照してください。
-

