



NAT ポリシー管理

以下のトピックでは、Firepower システム用の NAT ポリシーを管理する方法について説明します。

- [NAT ポリシーの管理 \(1 ページ\)](#)
- [NAT ポリシーの作成 \(2 ページ\)](#)
- [NAT ポリシーの設定 \(4 ページ\)](#)
- [NAT ポリシーの対象の設定 \(5 ページ\)](#)
- [NAT ポリシーのコピー \(6 ページ\)](#)

NAT ポリシーの管理

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)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

手順

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

ステップ2 NAT ポリシーを管理します。

- コピー：コピーする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 (6 ページ) を参照してください。
 - 作成：[新規ポリシー (New Policy)] をクリックします。NAT ポリシーの作成 (2 ページ) を参照してください。
 - 削除：削除するポリシー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。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。
- 注意** 管理対象デバイスに NAT ポリシーを展開した後は、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 ポリシーを展開して、すでに管理対象デバイスに存在する NAT ルールを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、最後に展開し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展開する必要があります。
- 展開：[展開 (Deploy)] をクリックします (設定変更の導入 を参照)。
 - 編集：編集アイコン (📝) をクリックします。NAT ポリシーの設定 (4 ページ) を参照してください。
 - [レポート (Report)]: レポートアイコン (📄) をクリックします (現在のポリシー レポートの生成 を参照)。

NAT ポリシーの作成

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)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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、ポリシーを展開する前に、この手順を実行する必要があります。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。

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。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカルポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

手順

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

ステップ 2 [新しいポリシー (New Policy)] ドロップダウンリストで、以下のいずれかを選択します。


- 7000 & 8000 シリーズ デバイスの場合は [Firepower NAT]。
- Firepower Threat Defense デバイスの場合は [脅威に対する防御 NAT (Threat Defense NAT)]。

ステップ 3 [名前 (Name)] に一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 必要に応じて、[説明 (Description)] を入力します。

ステップ 5 ポリシーを展開するデバイスを選択します。

- [使用可能なデバイス (Available Devices)] リストでデバイスを選択し、[ポリシーに追加 (Add to Policy)] をクリックします。
- [使用可能なデバイス (Available Devices)] リストから [選択されたデバイス (Selected Devices)] リストに、デバイスをクリックしてドラッグします。
- デバイスの横にある削除アイコン () をクリックして、[選択されたデバイス (Selected Devices)] リストからデバイスを削除します。

ステップ 6 [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 ポリシーの設定

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)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカルポリシーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

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。



- (注) ルール属性は NAT ポリシー タイプによって異なります。ルールを追加または編集する場合、詳細については、ダイアログボックスで [?] をクリックするか、関連する章 [Firepower Threat Defense 用のネットワーク アドレス変換 \(NAT\)](#) または [7000 および 8000 シリーズ デバイス用の NAT](#) を参照してください。

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 ポリシーを設定します。

- ポリシー名や説明を変更するには、[名前 (Name)] または [説明 (Description)] フィールドをクリックし、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。マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システ

ムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

- ポリシーの対象を管理するには、[NAT ポリシーの対象の設定（5 ページ）](#) を参照してください。
- ポリシーの変更を保存するには、[保存 (Save)] をクリックします。
- ポリシーに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、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、[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には、ルールを右クリックして [状態 (State)] を選択し、[無効化 (Disable)] または [有効化 (Enable)] を選択します。
- (Firepower NAT のみ。) 特定のルール属性の設定ページを表示するには、ルールの行にある条件の列で名前、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 Networks)] 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 Networks)] ページが表示されます。

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 ポリシーの対象の設定

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)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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、7000 または 8000 シリーズ スタック、および高可用性ペア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。

異なるバージョンの Firepower システムを実行中のスタック構成デバイスを対象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アップグレードが失敗した場合)。

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。

先祖ドメインの管理者は、NAT ポリシーの対象を子孫ドメインのデバイスにすることができます。子孫ドメインではこの NAT ポリシーを使用するか、カスタマイズされたローカル ポリ

シーに置き換えることができます。NAT ポリシーが異なる子孫ドメインのデバイスを対象とする場合、子孫ドメインの管理者は自分のドメインに属する対象デバイスに関する情報のみを表示できます。

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 [ポリシー割り当て (Policy Assignments)] をクリックします。

ステップ 4 次のいずれかを実行します。

- デバイス、スタック、高可用性ペア、またはデバイスグループをポリシーに割り当てるには、[使用可能なデバイス (Available Devices)] リストで選択し、[ポリシーに追加 (Add to Policy)] をクリックします。ドラッグアンドドロップを使用することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス (Selected Device)] リストのデバイス、スタック、高可用性ペア、またはデバイスグループの横にある削除アイコン (🗑) をクリックします。

ステップ 5 [OK] をクリック

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 ポリシーのコピー


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)
任意 (Any)	Control	7000 & 8000 シリーズ Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

NAT ポリシーのコピーを作成できます。コピーには、ポリシーのすべてのルールと設定が含まれます。

マルチドメイン導入では、現在のドメインおよび先祖ドメインからポリシーをコピーできます。

手順

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

ステップ 2 コピーする 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。

ステップ 3 [名前 (Name)] に、ポリシーの一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 [OK] をクリックします。
