CHAPTER 22

NAT

セキュリティ アプライアンスは、発信ホスト セッションごとに一意のグローバル アドレスを提供する Network Address Translation（NAT; ネットワーク アドレス変換）機能と、最大で 64,000 件までの同時に行われる発信または着信ホスト セッションに一意のグローバル アドレスを 1 つ提供する Port Address Translation（PAT; ポート アドレス変換）機能の両方をサポートしています。NAT で使用されるグローバル アドレスは、特にアドレス変換で使用されるアドレス プールから選択されます。PAT で使用される一意のグローバル アドレスには、1 つのグローバル アドレスまたは所定のインターフェイスの IP アドレスのいずれかを指定できます。

セキュリティ アプライアンスは、着信接続と発信接続の両方で NAT または PAT を実行できます。着信アドレスを変換する機能は、外部の、つまり安全性の低いインターフェイスのアドレスが使用可能な内部の IP アドレスに変換されるため、外部 NAT と呼ばれます。外部 NAT 機能では、外部ホストまたはネットワークを内部ホストまたはネットワークに変換するオプションを選択することができ、双方向 NAT と呼ばれることもあります。NAT によって発信トラフィックを変換する場合と同様に、ダイナミック NAT、スタティック NAT、ダイナミック PAT、およびスタティック PAT を選択できます。必要に応じて、外部 NAT を内部 NAT と一緒に使用し、パケットの送信元 IP アドレスと宛先 IP アドレスの両方を変換することも可能です。

NAT

Configuration > Security Policy > NAT

NAT ペインでは、ネットワークに適用されるすべてのアドレス変換ルールまたは NAT 免除ルールを表示できます。

NAT ペインでは、変換免除ルールを作成することもでき、変換または暗号化の対象から免除するトラフィックを指定できます。免除ルールはテーブル内でインターフェイスごとにグループ化され、次いで方向ごとにグループ化されます。変換される IP アドレスのグループがある場合は、免除ルールを使用して、変換されることのないように特定のアドレスを免除することができます。事前に設定したアクセスリストを使用して免除ルールを定義できます。ASDM は、コマンドライン インターフェイスに nat 0 コマンドを書き込みます。免除の表示は、カラム ヘッダーをクリックして再ソートできます。

また、ポリシー NAT を使用してアクセスリストの送信元アドレスと宛先アドレス（またはポート）を指定することにより、アドレス変換するローカル トラフィックを特定することもできます。ポリシー NAT を使用することにより、それぞれの文で送信元 / ポートと宛先 / ポートの組み合せが一意である限り、同じローカル アドレスを特定する複数の NAT 文またはスタティック文を作成できます。その後、異なるグローバル アドレスを各送信元 / ポートと宛先 / ポートのペアに対して照合できます。

前提条件

- ネットワークのアクセス ルールと変換ルールを指定する前に、まずルールを適用する各ホストまたはサーバを定義する必要があります。

注意　ネットワーク グループとサービス グループの命名に関するオブジェクト グループについては、特記事項を確認してください。

制限事項

- ネットワークまたはホストを定義するまでは、使用不可の変換コマンドを使用することはできません。使用不可のコマンドは、メニューでグレー表示されます。
- 変換ルールの適用順序は、ルールの動作に影響する可能性があることに注意してください。ASDM は、まずスタティック変換をリストしてからダイナミック変換をリストします。NAT を処理する場合、セキュリティ アプライアンスは設定されている順序でまずスタティック変換を実行します。Insert または Insert After を使用して、スタティック変換が処理される順序を決定することができます。動的に変換されるルールは最も適合するルールから処理されるため、ダイナミック変換の前後にルールを挿入するオプションはディセーブルになっています。
- セキュア ネットワークにルーティング可能な IP アドレスが存在する場合でも、NAT を実行する必要があります。ルーティング可能な IP アドレスで NAT を実行する場合は、ルーティング可能な IP アドレスを外部にあるそのアドレス自体に変換します。
- 中間（DMZ）インターフェイス宛てのよりセキュアな（内部）インターフェイスが送信元になっているパケットは、安全性の低い（外部）インターフェイスの発信パケットである場合、同じ変換済みアドレスを持つことはできません。さらに、発信インターフェイスのいずれかで 1 つのダイナミック ルールが削除されると、同じインターフェイスで発信される変換のすべての発信ダイナミック ルールが削除されます。
- トラフィックがインターネットまたは安全性の低いインターフェイスに暗号化なしで送信されるように、そのトラフィックの免除ルールを作成することが可能です。この方法は、別のリモート VPN ネットワークへの一部のトラフィックを暗号化し、それ以外の場所宛てのトラフィックは暗号化しないようにするシナリオで役立ちます。

フィールド

- Add : 新しい NAT ルールを追加します。ドロップダウン リストから、追加するルールのタイプを選択します。
- Edit：NAT ルールを編集します。
- Delete：NAT ルールを削除します
- Move Up：ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複するルールがあると順序によって評価が異なります。
- Move Down：ルールを下に移動します。
- Cut：ルールを切り取ります。
- Copy：ルールのパラメータをコピーし、Paste ボタンを使用して、同じパラメータを持つ新しいルールを開始できます。
- Paste : コピーまたは切り取られたルールのパラメータがあらかじめ入力された状態で、Add/Edit Rule ダイアログボックスを開きます。ダイアログボックスで何らかの修正を行い、ルールをテーブルに追加することができます。Paste ボタンをクリックすると、選択したルールの上にルールが追加されます。Paste ドロップダウン リストから Paste After 項目を選択すると、選択したルールの後にルールが追加されます。
- Find : 表示をフィルタリングして、一致するルールのみを表示します。**Find** をクリックすると、Filter フィールドが開きます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter ドロップダウン リスト : Interface、Source、Destination、Service、Action、または Rule Query の中からフィルタの基準を選択します。ルール クエリーは複数の基準の集合であり、保存して繰り返し使用することができます。
  - Filter フィールド : Interface タイプの場合は、このフィールドがドロップダウン リストになります。リストでは、インターフェイス名を選択できます。Action タイプの場合は、ドロップダウン リストに Exempt、Static、および Dynamic が表示されます。Rule Query タイプの場合は、ドロップダウン リストにすべての定義済みルール クエリーが表示されます。Source タイプと Destination タイプの場合には、IP アドレスを指定できます。アドレスを手動で入力するか、または **...** ボタンをクリックして Browse Address ダイアログボックスを開いてアドレスを参照します。Service タイプとしては、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを指定できます。プロトコル タイプを手動で入力するか、または **...** ボタンをクリックして Browse Service Groups ダイアログボックスを開き、プロトコル タイプを参照します。
  - Filter：フィルタリングを実行します。
  - Clear：Filter フィールドをクリアします。
  - Rule Query : Rule Queries ダイアログボックスを開き、名前付きルール クエリーを管理できます。
- Show Rule Flow Diagram：ルール テーブルの下に Rule Flow Diagram 領域を表示します。この図には、ネットワーク、トラフィックのタイプ、インターフェイス名、フロー方向、およびアクションが表示されます。
- Packet Trace：選択したルールの特性を示すパラメータがあらかじめ入力された状態で Packet Tracer ツールが開きます。

次に、NAT Rules テーブルのカラムの概要を説明します。これらのカラムの内容は、テーブル セルをダブルクリックすると編集できます。カラム ヘッダーをダブルクリックすると、選択したカラムをソート キーとして、テーブルの内容がアルファベットの昇順で並べ替えられます。ルールを右クリックすると、上のボタンで示されるオプションすべてとともに、Insert 項目と Insert After 項目が表示されます。これらの項目により、選択したルールの前（Insert）または後（Insert After）に新しいルールを挿入します。

- No：ルールの評価順序を示します。

- Type：dynamic または static のうち、所定の行に適用される変換ルール タイプを表示します。
  - Dynamic：内部 IP アドレスは、グローバル アドレスのプールにある IP アドレスを使用して、あるいは PAT の場合であれば 1 つのアドレスを使用して、動的に変換されます。これらのルールは、セキュリティ レベルの高いインターフェイス上にあるホストのアドレスを、セキュリティ レベルの低いインターフェイスに送信されるトラフィック用のアドレス プールから選択されるアドレスに変換します。多くの場合、ダイナミック変換は、ローカルの RFC 1918 IP アドレスを、インターネットへルーティング可能なアドレスにマッピングするために使用されます。ダイナミック変換はダイナミック アイコンで表示されます。
  - Static：内部 IP アドレスは、グローバル IP アドレスに永続的にマッピングされます。これらのルールは、セキュリティ レベルの低いインターフェイス上のホスト アドレスを、セキュリティ レベルの高いインターフェイス上のグローバル アドレスにマッピングします。たとえば、境界ネットワークの Web サーバのローカル アドレスを、外部インターフェイス上のホストが Web サーバにアクセスするために使用するグローバル アドレスにマッピングする場合には、スタティック ルールを使用します。スタティック変換はスタティック アイコンで表示されます。
- Real：ネットワーク変換が適用される前の元のアドレスと、それに関連付けられていたインターフェイスを表示します。
  - Source Network：ポリシー NAT の場合には、変換対象のトラフィックが常駐する送信元ネットワーク。通常の NAT の場合には、any と表示されます。
  - Destination Network：ポリシー NAT の場合は、変換対象のトラフィックが常駐する宛先ネットワーク。通常の NAT の場合には、any と表示されます。
- Translated：ネットワーク変換が適用された後の変換済みアドレス、および関連付けられたインターフェイスを表示します。
  - Interface：変換済みアドレスが存在するインターフェイス。
  - Address：変換済みのアドレス。
- Options：次の項目を含みます。
  - DNS Rewrite：外部クライアントが内部 DNS サーバを使用して内部ホストの名前を解決したり、またはその逆を行ったりすることができるように、セキュリティ アプライアンスで DNS レコードをリライトできます。たとえば、内部 Web サーバ www.example.com の IP アドレスが 192.168.1.1 のときに、外部インターフェイスの 10.1.1.1 に変換されるとします。この場合、外部クライアントは DNS 要求を内部 DNS サーバに送り、内部 DNS サーバは www.example.com を 192.168.1.1 に名前解決します。DNS Rewrite がイネーブルになっているセキュリティ アプライアンスに応答が返されると、セキュリティ アプライアンスはペイロードの IP アドレスを 10.1.1.1 に変換するため、外部クライアントは正しい IP アドレスを取得することになります。
  - Maximum TCP Connections：スタティックに変換された IP アドレスへの接続を許可される TCP 接続の最大数。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。
  - Embryonic Limit：セキュリティ アプライアンスが接続の拒否を開始するまでの初期接続の許容数。この制限を設定して、初期接続のフラッディングによる攻撃を防止します。初期接続は、3 ウェイ TCP ハンドシェイク状態などのように、開始されてはいても確立されていない接続です。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。正の数を設定すると、TCP 代行受信機能がイネーブルになります。
  - Maximum UDP Connections：スタティックに変換された IP アドレスへの接続を許可される UDP 接続の最大数。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。
  - Randomize Sequence Number：このチェックボックスをオンにすると、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。この機能は、別のインライン セキュリティ アプライアンスもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合にのみディセーブルにしてください。このオプションを使用すると、セキュリティ アプライアンスのセキュリティ ホールが開いた状態になります。デフォルトで選択されています。
- Description（Policy NAT の場合のみ）：ルールの説明がある場合は、このカラムに表示されます。

- Enable traffic through the firewall without address translation：トラフィックがアドレス変換なしでセキュリティ アプライアンスを通過できるようにします。
- Addresses：IP アドレス オブジェクト、IP 名、またはネットワーク オブジェクト グループを追加、編集、削除、または検索するためのタブ。
- Services：サービスを追加、編集、削除、または検索するためのタブ。
- Global Pools：ダイナミック NAT コンフィギュレーションで使用されるグローバル アドレスの NAT プールを管理するためのタブ。Global Pools のアドレスは、そのアドレスが設定されている外部または安全性の低いインターフェイスにセキュリティ アプライアンスが提示する IP アドレスです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Add/Edit Static NAT Rule

Configuration > Security Policy > NAT > Add/Edit Static NAT Rule

Add/Edit Static NAT Rule ダイアログボックスでは、使用するセキュリティ アプライアンスの変換ルールを追加、編集、および貼り付けできます。変換ルールは、NAT Rules テーブルに表示されます。スタティック NAT ルールにより、そのアドレス変換が、プライベート（無効）IP アドレスからグローバル（有効）IP アドレスに対して行われる、1 対 1 の IP アドレス スタティック変換であることを指定します。Static または Dynamic を選択できますが、両方は選択できません。

（注） ネットワーク グループとサービス グループの命名に関するオブジェクト グループについては、特記事項を確認してください。

フィールド

- Real Address：ネットワーク変換が適用される前の元のアドレスと、それに関連付けられていたインターフェイス。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - IP address：ルールを適用するホストまたはネットワークの IP アドレスを指定します。
  - Mask：アドレスのネットワーク マスク（ネットマスク）を選択します。
  - Browse：事前定義済みホストまたはネットワークの Hosts/Networks ツリーから、正しい IP アドレスとマスクを選択できます。
- Static Translation：スタティック インターフェイスと IP アドレスを指定できます。
  - Interface：スタティック変換用のセキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - IP address：スタティック変換用の IP アドレスを選択します。
  - Browse：事前定義済みホストまたはネットワークの Hosts/Networks ツリーから、正しい IP アドレスとマスクを選択できます。

- Enable Port Address Translation (PAT)：このオプションを選択して、PAT 用のプロトコル、元のポート、および変換後のポートを指定します。
  - Protocol：TCP または UDP。
  - Original Port：ポートのリストから選択します。
  - Translated Port：ポートのリストから選択します。
- NAT Options : DNS Rewrite、Maximum Connections、Embryonic Limit、および Randomize Sequence Number を設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Add/Edit Dynamic NAT Rule

Configuration > Security Policy > NAT > Add/Edit Dynamic NAT Rule

Add/Edit Dynamic NAT Rule ダイアログボックスでは、使用するセキュリティ アプライアンスの変換ルールを追加、編集、および貼り付けできます。変換ルールは、NAT Rules テーブルに表示されます。ダイナミック NAT ルールでは、IP アドレスの事前定義済みプールを指定するか、あるいは、PAT をグローバル IP アドレスで、またはよりセキュアなインターフェイス上にある複数のホストの安全性の低いインターフェイスで実行するかを指定します。たとえば、内部ネットワークに複数のホストが存在する場合は、ダイナミック NAT を使用することによってプールまたは PAT アドレスを介した発信アクセスを許可し、発信接続を要求しているホストごとにグローバル IP アドレスをダイナミックに割り当てることができます。Static または Dynamic を選択できますが、両方は選択できません。

（注）　ネットワーク グループとサービス グループの命名に関係するオブジェクト グループについては、特記事項を確認してください。

フィールド

- Real Address : ネットワーク変換が適用される前の元のアドレスと、それに関連付けられていたインターフェイス。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - IP Address：ルールを適用するホストまたはネットワークの IP アドレスを指定します。
  - Mask：アドレスのネットワーク マスク（ネットマスク）を選択します。
  - Browse：事前定義済みホストまたはネットワークの Hosts/Networks ツリーから、正しい IP アドレスとマスクを選択できます。
- Dynamic Translation : ダイナミック インターフェイスとグローバル アドレス プールを指定できます。
  - Interface：ダイナミック変換用のセキュリティ アプライアンスのネットワーク インターフェイスを選択します。

- Add：グローバル プールを追加します。
- Edit：グローバル プールを編集します。
- Delete：グローバル プールを削除します。

- NAT Options : DNS Rewrite、Maximum Connections、Embryonic Limit、および Randomize Sequence Number を設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

NAT Options

Configuration > Security Policy > NAT > Add/Edit NAT Rule> NAT Options

NAT Options ダイアログボックスでは、NAT およびポリシー NAT の DNS Rewrite、Maximum Connections、Embryonic Limit、および Randomize Sequence Number を設定できます。

フィールド

- DNS Rewrite : 外部クライアントが内部 DNS サーバを使用して内部ホストの名前を解決したり、またはその逆を行ったりすることができるように、セキュリティ アプライアンスで DNS レコードをリライトできます。たとえば、内部 Web サーバ www.example.com の IP アドレスが 192.168.1.1 のときに、外部インターフェイスの 10.1.1.1 に変換されるとします。この場合、外部クライアントは DNS 要求を内部 DNS サーバに送り、内部 DNS サーバは www.example.com を 192.168.1.1 に名前解決します。DNS Rewrite がイネーブルになっているセキュリティ アプライアンスに応答が返されると、セキュリティ アプライアンスはペイロードの IP アドレスを 10.1.1.1 に変換するため、外部クライアントは正しい IP アドレスを取得することになります。
- Maximum TCP Connections：スタティックに変換された IP アドレスへの接続を許可される TCP 接続の最大数。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。
- Maximum UDP Connections : スタティックに変換された IP アドレスへの接続を許可される UDP 接続の最大数。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。
- Embryonic Limit : セキュリティ アプライアンスが接続の拒否を開始するまでの初期接続の許容数。この制限を設定して、初期接続のフラッディングによる攻撃を防止します。初期接続は、3 ウェイ TCP ハンドシェイク状態などのように、開始されてはいても確立されていない接続です。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。正の数を設定すると、TCP 代行受信機能がイネーブルになります。
- Randomize Sequence Number : このチェックボックスをオンにすると、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。この機能は、別のインライン セキュリティ アプライアンスもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合にのみディセーブルにしてください。このオプションを使用すると、セキュリティ アプライアンスのセキュリティ ホールが開いた状態になります。デフォルトで選択されています。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Global Pools

Configuration > Security Policy > NAT > Add/Edit Address Translation Rule > Global Pools

Global Pools ダイアログボックスでは、ダイナミック NAT ルールで使用されるグローバル アドレス プールを表示、新規プールを定義、または既存プールを削除できます。ダイナミック NAT ルールとその使用の詳細については、ダイナミック NAT の説明を参照してください。

フィールド

- Interface：ダイナミック　アドレス変換で使用するアドレス　プールに関連付けられたインターフェイス名を特定します。
- Pool ID：アドレス プールの ID 番号を特定します。
- IP Address(es)：プールに含めるアドレスのタイプと値を特定します。次のタイプのいずれか 1 つを指定できます。
  - アドレス範囲
  - PAT アドレス
  - インターフェイスに関連付けられた PAT アドレス

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Add/Edit Global Address Pool

Configuration > Security Policy > NAT > Add/Edit Address Translation Rule > Global Pools > Add/Edit Global Address Pool

Add/Edit Global Address Pool ダイアログボックスでは、新しいグローバル アドレス プールの設定を定義したり、既存プールの設定を編集したりできます。

フィールド

- Interface：インターフェイス名を指定して新しいアドレス　プールに関連付けます。Interface　ドロップダウン リストで名前を選択します。
- Pool ID：このアドレス プールを参照するためにダイナミック NAT ルールが使用する ID 番号を指定します。Pool ID フィールドに番号を入力します。
- Range：このオプションを選択して、IP アドレスの範囲を新しいアドレス プールで使用することを指定します。このオプションを選択する場合は、次の値を指定します。

- 範囲として使用する開始アドレスと終了アドレスを **IP Address** フィールドに入力します。これらのアドレスは、元のアドレスの変換後のアドレスです。セキュリティ アプライアンスがホストまたはネットワークをインターネットのユーザに公開している場合、これらの IP アドレスは American Registry for Internet Numbers に登録された有効な IP アドレスである必要があります。
- **Network Mask** (optional) フィールドにマスクを入力します。この値により、変換後の IP アドレスがメンバーになっているネットワークのマスクを特定します。

- Port Address Translation (PAT) : このオプションを選択して、IP アドレスを PAT で使用することを指定します。このオプションを選択する場合は、次の値を指定します。
  - PAT で使用される IP アドレスを **IP Address** フィールドに入力します。
    この値は、変換済みホストまたはネットワークの元のアドレスの変換先となる、固有の変換済み IP アドレスです。セキュリティ アプライアンスがホストまたはネットワークをインターネットのユーザに公開している場合、この IP アドレスは ARIN に登録された有効な IP アドレスである必要があります。
- Port Address Translation (PAT) using the IP address of the interface : このオプションを選択して、**Interface** ドロップダウン リストで選択したインターフェイスに割り当てられている IP アドレスを、PAT の変換後アドレスとして使用することを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Add/Edit Static Policy NAT Rule

Configuration > Security Policy > NAT > Add/Edit Static Policy NAT Rule

Add/Edit Static Policy NAT Rule ダイアログボックスでは、トラフィックの変換でポリシー NAT が使用するプロトコルとサービスを設定できます。

フィールド

- Real Address : ネットワーク変換が適用される前の元のアドレスと、それに関連付けられていたインターフェイス。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - Source：タイプ、IP アドレス、およびネットマスクを選択します。
  - Destination：タイプ、IP アドレス、およびネットマスクを選択します。
- Protocol and Service：ポリシー NAT で使用するプロトコルとサービスを定義できます。
  - TCP：ポリシー NAT による変換で使用する TCP プロトコル タイプを定義する場合に選択します。
  - UDP : ポリシー NAT による変換で使用する UDP プロトコル タイプを定義する場合に選択します。
  - ICMP : ポリシー NAT による変換で使用する ICMP プロトコル タイプを定義する場合に選択します。
  - IP：ポリシー NAT による変換で使用する IP プロトコル タイプを定義する場合に選択します。

  - IP Protocol：選択するプロトコルに応じて、TCP、UDP、ICMP、または IP プロトコル タイプを表示します。ポートまたはプロトコル番号を入力するか、参照（...）ボタンを使用してドロップダウン リストからプロトコルを選択できます。
- Static Translation：スタティック インターフェイスと IP アドレスを指定できます。
  - Interface：スタティック変換用のセキュリティ　アプライアンスのネットワーク　インターフェイスを選択します。
  - IP address：スタティック変換用の IP アドレスを選択します。
  - Browse：事前定義済みホストまたはネットワークの Hosts/Networks ツリーから、正しい IP アドレスとマスクを選択できます。
- Enable Port Address Translation (PAT)：このオプションを選択して、PAT 用のプロトコル、元のポート、および変換後のポートを指定します。
  - Protocol：TCP または UDP。
  - Original Port：ポートのリストから選択します。
  - Translated Port：ポートのリストから選択します。
- NAT Options : DNS Rewrite、Maximum Connections、Embryonic Limit、および Randomize Sequence Number を設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Add/Edit Dynamic Policy NAT Rule

Configuration > Security Policy > NAT > Add/Edit Dynamic Policy NAT Rule

Add/Edit Dynamic Policy NAT Rule ダイアログボックスでは、トラフィックの変換でポリシー NAT が使用するプロトコルとサービスを設定できます。

フィールド

- Real Address : ネットワーク変換が適用される前の元のアドレスと、それに関連付けられていたインターフェイス。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ　アプライアンスのネットワーク インターフェイスを選択します。
  - Source：タイプ、IP アドレス、およびネットマスクを選択します。
  - Destination：タイプ、IP アドレス、およびネットマスクを選択します。
- Protocol and Service：ポリシー NAT で使用するプロトコルとサービスを定義できます。
  - TCP：ポリシー NAT による変換で使用する TCP プロトコル タイプを定義する場合に選択します。
  - UDP : ポリシー NAT による変換で使用する UDP プロトコル タイプを定義する場合に選択します。
  - ICMP : ポリシー NAT による変換で使用する ICMP プロトコル タイプを定義する場合に選択します。
  - IP：ポリシー NAT による変換で使用する IP プロトコル タイプを定義する場合に選択します。

  - IP Protocol : 選択するプロトコルに応じて、TCP、UDP、ICMP、または IP プロトコル タイプを表示します。ポートまたはプロトコル番号を入力するか、参照（...）ボタンを使用してドロップダウン リストからプロトコルを選択できます。
- Dynamic Translation : ダイナミック インターフェイスとグローバル アドレス プールを指定できます。
- Real Address : ネットワーク変換が適用される前の元のアドレスと、それに関連付けられていたインターフェイス。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - IP Address：ルールを適用するホストまたはネットワークの IP アドレスを指定します。
  - Mask：アドレスのネットワーク マスク（ネットマスク）を選択します。
  - Browse：事前定義済みホストまたはネットワークの Hosts/Networks ツリーから、正しい IP アドレスとマスクを選択できます。
- Dynamic Translation : ダイナミック インターフェイスとグローバル アドレス プールを指定できます。
  - Interface：ダイナミック変換用のセキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - Add：グローバル プールを追加します。
  - Edit：グローバル プールを編集します。
  - Delete：グローバル プールを削除します。
- NAT Options : DNS Rewrite、Maximum Connections、Embryonic Limit、および Randomize Sequence Number を設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Add/Edit NAT Exempt Rule

Configuration > Security Policy > NAT > Add/Edit NAT Exempt Rule

Add/Edit NAT Exempt Rule ダイアログボックスでは、セキュリティ アプライアンスでの NAT 免除ルールを追加および編集できます。Translation Rules メニューで選択したコマンドに応じて、このダイアログボックスのタイトルには、Add Address Exemption Rule または Edit Address Exemption Rule と表示されます。

フィールド

- Action：アクションのドロップダウン リストでは、定義された基準にホスト / ネットワークが一致する場合に免除ルールが実行するアクション（免除する、免除しない）を選択できます。Select an action リストには、次のオプションが表示されます。
  - Exempt：定義されたトラフィックが NAT から免除されることを指定します。
  - Do Not Exempt：定義されたトラフィックが NAT から免除されないことを指定します。

- IP　Address：免除ルールのアクションが適用されるかどうかを決定する、送信元ホストまたはネットワークの IP アドレスのテスト基準を選択します。このオプションを選択すると、次のフィールドが表示されます。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ アプライアンスのネットワーク インターフェイス名を選択します。
  - IP address：ルールを適用するホストまたはネットワークの IP アドレスを指定します。
  - Browse：事前定義済みホストまたはネットワークの Hosts/Networks ツリーから、正しい IP アドレスとマスクを選択できます。
  - Mask：アドレスのネットワーク マスク（ネットマスク）を選択します。
- Name：免除ルールのアクションが適用されるかどうかを決定する、送信元ホストまたはネットワークの名前のテスト基準を選択します。このオプションを選択すると、次のフィールドが表示されます。
  - Name：ルールを適用するホストまたはネットワークについて、事前に定義された名前を選択できます。また、セキュリティ アプライアンスは、内部または外部などのインターフェイス名を使用することにより、インターフェイスごとのホスト名を自動的に生成します。
- Group：免除ルールのアクションが適用されるかどうかを決定する、送信元ホストまたはネットワークのグループのテスト基準を選択します。このオプションを選択すると、次のフィールドが表示されます。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ アプライアンスのネットワーク インターフェイス名を選択します。
  - Group：ルールを適用するホストまたはネットワークのグループを選択します。
- When Connecting To：When Connecting To 領域では、アクションを実行するために満たす必要のある基準を定義できます。基準は、IP アドレス、名前、グループを選択することによって、または事前に定義されたホスト / ネットワークのドロップダウン リストを参照することによって定義できます。
- IP address：免除ルールを適用する宛先ホストまたはネットワークの IP アドレスを指定します。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ アプライアンスのネットワーク インターフェイス名を選択します。
  - IP address：ルールを適用するホストまたはネットワークの IP アドレスを指定します。
  - Browse：事前定義済みホストまたはネットワークの Hosts/Networks ツリーから、正しい IP アドレスとマスクを選択できます。
  - Mask：アドレスのネットワーク マスク（ネットマスク）を選択します。
- Name：免除ルールのアクションが適用されるかどうかを決定する、送信元ホストまたはネットワークの名前のテスト基準を選択します。このオプションを選択すると、次のフィールドが表示されます。
  - Name：ルールを適用するホストまたはネットワークについて、事前に定義された名前を選択できます。また、セキュリティ アプライアンスは、内部または外部などのインターフェイス名を使用することにより、インターフェイスごとのホスト名を自動的に生成します。
- Group：免除ルールのアクションが適用されるかどうかを決定する、送信元ホストまたはネットワークのグループのテスト基準を選択します。このオプションを選択すると、次のフィールドが表示されます。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ アプライアンスのネットワーク インターフェイス名を選択します。
  - Group：ルールを適用するホストまたはネットワークのグループを選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

Add/Edit Identity NAT Rule

Configuration > Security Policy > NAT > Add/Edit Identity NAT Rule

Add/Edit Identity NAT Rule ダイアログボックスでは、アイデンティティ NAT の設定値を設定できます。

フィールド

- Real Address : ネットワーク変換が適用される前の元のアドレスと、それに関連付けられていたインターフェイス。
  - Interface：元のホストまたはネットワークが常駐するセキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - IP address：ルールを適用するホストまたはネットワークの IP アドレスを指定します。
  - Mask：アドレスのネットワーク マスク（ネットマスク）を選択します。
  - Browse：事前定義済みホストまたはネットワークの Hosts/Networks ツリーから、正しい IP アドレスとマスクを選択できます。
- Enable outside NAT：外部 NAT をイネーブルにするにはこのオプションを選択します。
- NAT Options : DNS Rewrite、Maximum Connections、Embryonic Limit、および Randomize Sequence Number を設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—