

Cisco Start Firewall

Cisco ASA 5506-X PAT (Port Address Translation) の設定

2016年3月23日
第1.1版



www.networld.co.jp

株式会社ネットワールド





Cisco Start Firewall

Cisco ASA 5506-X

PAT (Port Address Translation) の設定



改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016年2月9日	ネットワーク	● 新規
1.1	2016年3月23日	ネットワーク	● 誤記修正
			●
			●



Cisco Start Firewall

Cisco ASA 5506-X

PAT (Port Address Translation) の設定



免責事項

- 本書のご利用は、お客様ご自身の責任において行われるものとします。本書に記載する情報については、株式会社ネットワーク（以下 弊社）が慎重に作成および管理いたしますが、弊社がすべての情報の正確性および完全性を保証するものではありません。
- 弊社は、お客様が本書からご入手された情報により発生したあらゆる損害に関して、一切の責任を負いません。また、本書および本書にリンクが設定されている他の情報元から取得された各種情報のご利用によって生じたあらゆる損害に関しても、一切の責任を負いません。
- 弊社は、本書に記載する内容の全部または一部を、お客様への事前の告知なしに変更または廃止する場合がございます。なお、弊社が本書を更新することをお約束するものではありません。



表記規則

表記	表記の意味
「」 (括弧記号)	キー、テキストボックス、ラジオボタンなどのオブジェクト
bold (ボールド文字)	入力または選択するシステム定義値
<i><italic></i> (イタリック文字)	入力または選択するユーザー定義値
□ (囲み線)	入力または選択するオブジェクト
"" (二重引用符記号)	表示されるメッセージ
[] (蛍光マーカー)	確認するメッセージ

表記の例)

(1) 「Exec」ラジオボタンを選択します。

(2) テキストボックスに以下のコマンドを入力します。

copy running-config <file name>

(3) 「コマンドを実行」ボタンをクリックします。正常に実行されれば、画面に"[OK]"が表示されます。

Destination filename [startup-config]?

Building configuration...

[OK]

- 1
- 2
- 3

CLIによる設定

CLI機能はルータのコマンドプロンプトで実行可能な設定や、全てのIOS CLIコマンドを入力できます

1 Exec
 Configure

2

3

Destination filename [startup-config]?
Building configuration...

[OK]



目次

1. はじめに.....	1
1.1 対象機器.....	1
1.2 PATとは.....	1
3. PATの設定.....	3
3.1 初期設定.....	3
3.2 PATの設定（全てのトラフィックを対象）	5
3.3 PATの設定（対象のトラフィックを指定）	8
3.4 PATの確認	12



1. はじめに

本書では Cisco ASA 5506-X における PAT (Port Address Translation) の設定手順について説明します。

1.1 対象機器

本書で対象としている機器は以下になります。

表 1 本書の対象機器

ASA 5506-X (ASA5506-K9)	ASA 5506W-X (ASA5506W-Q-K9)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1.2 PAT とは

PATとは、複数の IP アドレスを単一の IP アドレスに変換する機能です。この機能によって、プライベートアドレスを持つ複数のクライアント端末に対して、一つのグローバルアドレスを使用したインターネットへのアクセスを提供することなどができます。



2. システム構成

2.1 システム構成

本書での設定手順は以下のシステム構成に基づいて行われます。設定状態は別紙「Cisco ASA 5506-X クイックスタートガイド」および「Cisco ASA 5506-X Network Object と Service Group の設定」に基づいた設定の完了後となり、管理 PC の ASDM から ASA に接続でき、Network Object Group が作成された状態を想定しています。

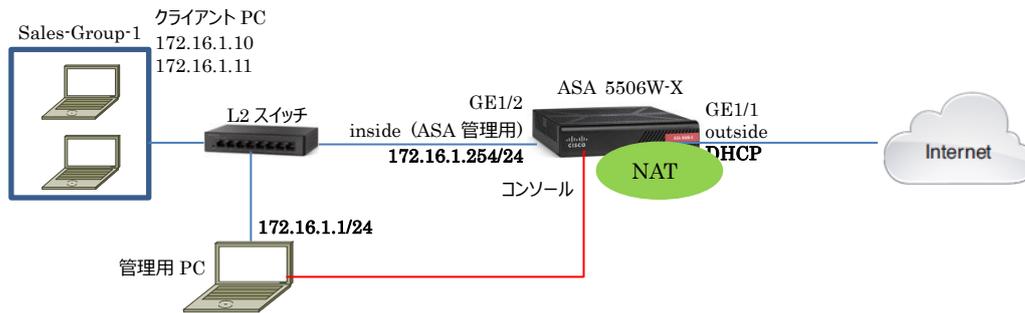


図 1 システム構成図

表 2 本書で使用した機材およびそれらのシステム環境

機器	機器名	OS およびアプリケーション	ネットワーク設定
Firewall	ASA 5506W-X	OS Version 9.5(2) ASDM Version 7.5(2)153	GE1/1 nameif:outside (デフォルト) IP アドレス:DHCP (デフォルト) security level:0(デフォルト) GE1/2 nameif:inside (デフォルト) IP アドレス:172.16.1.254/24 Security level:100(デフォルト)
L2 スイッチ	SG-110D		
管理用 PC		OS : Windows 7 ターミナルアプリケーション (Tera Term) Web ブラウザ(Internet Explorer11)	インタフェース IP アドレス:172.16.1.1/24

表 3 ASA 5506-X のネットワーク設定

ルーティング	DHCP によりインターネット側へのデフォルトルートを取得	
Object	Network Object	Sales-PC-01(172.16.1.10), Sale-PC-02(172.16.1.11)
	Network Object Group	Sales-Group-1(Sales-PC-01, Sale-PC-02)
	Service Group	Sales-Group-1-Service(http,https,imap4,smtp)
NAT	inside(すべてのトラフィック)→outside への PAT または inside(Sales-PC-01 からのトラフィック)→outside への PAT	



3. PAT の設定

3.1 初期設定

本製品にデフォルトで設定されている NAT ルールを削除します。

- 1) 管理 PC から ASDM により ASA にアクセスし、「Configuration」>「Firewall」>「NAT Rules」を開き、デフォルトで設定されている NAT ルールを削除します。

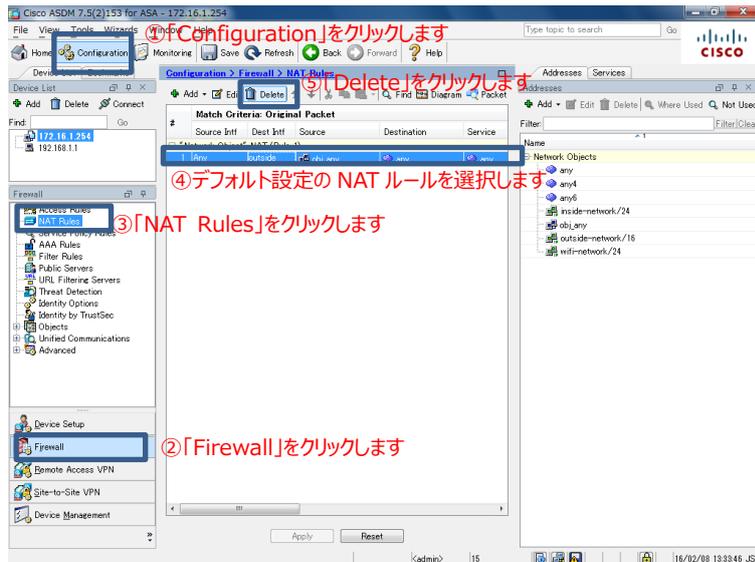


図 2 デフォルト設定の NAT ルールを削除

- 2) NAT ルールの削除後、「Apply」をクリックして ASA に設定を適用します。

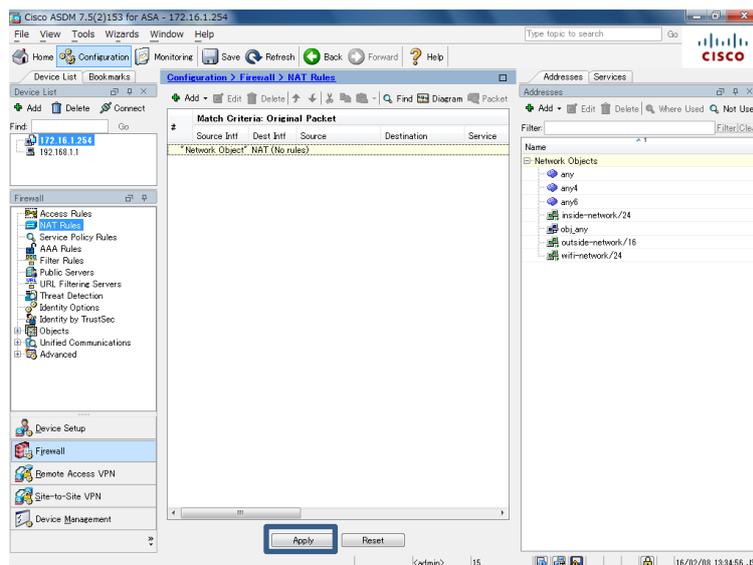


図 3 設定の適用



- 3) NAT テーブルの clear の確認がありますので、「Yes」をクリックします。

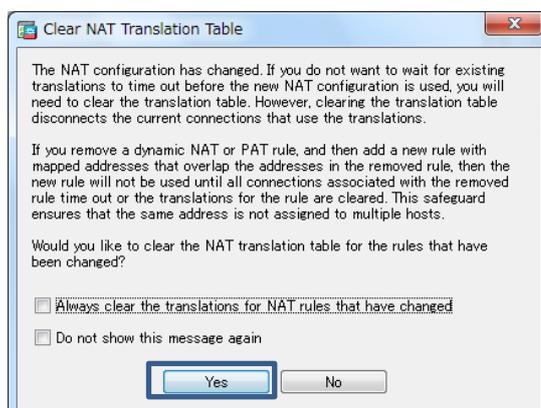


図 4 NAT テーブルの clear

- 4) ASA に実行されるコマンドのプレビューが表示されるので、「Send」をクリックして実行します。

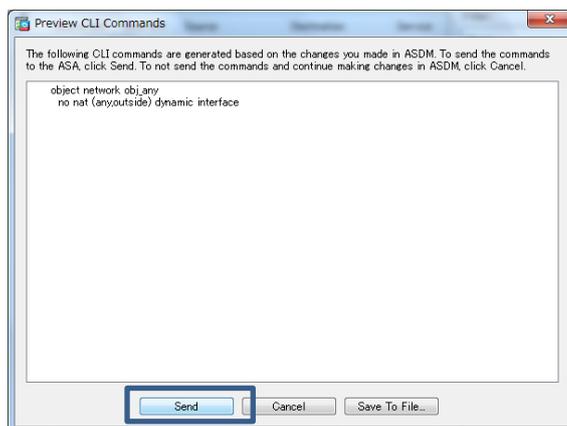


図 5 コマンドのプレビュー



3.2 PAT の設定 (全てのトラフィックを対象)

本節では inside から outside への全てのトラフィックを対象とした PAT の設定手順について説明します。

- 1) 「Configuration」>「Firewall」>「NAT Rules」を開き、「Add」をクリックして「Add NAT Rule Before "Network Object" NAT Rules」を開きます。

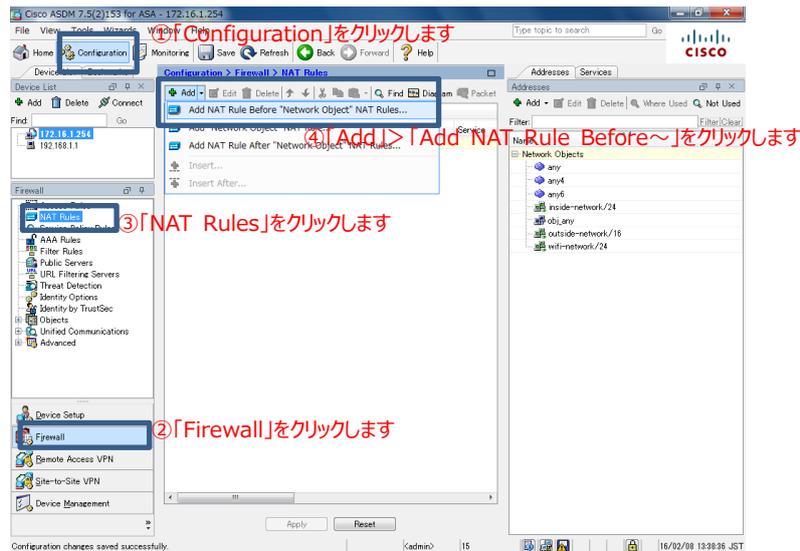


図 6 NAT ルールの設定に移動

- 2) 「Source Interface」を「inside」、「Destination Interface」を「outside」とし、「Source NAT Type」は「Dynamic PAT (Hide)」を選択し、「Source Address」の「…」をクリックします。

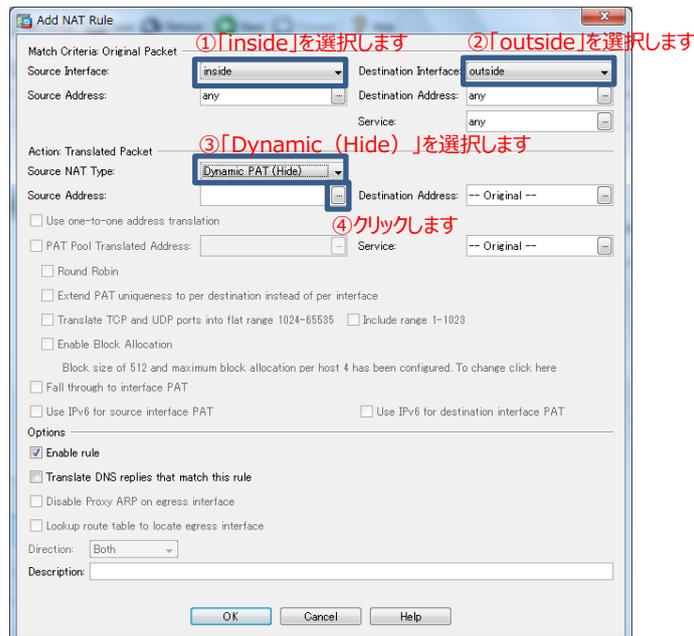


図 7 NAT ルールの設定



- 3) 変換後の Source address となるインタフェースを指定します。「Original Translated Source Address」を「outside」に設定します。

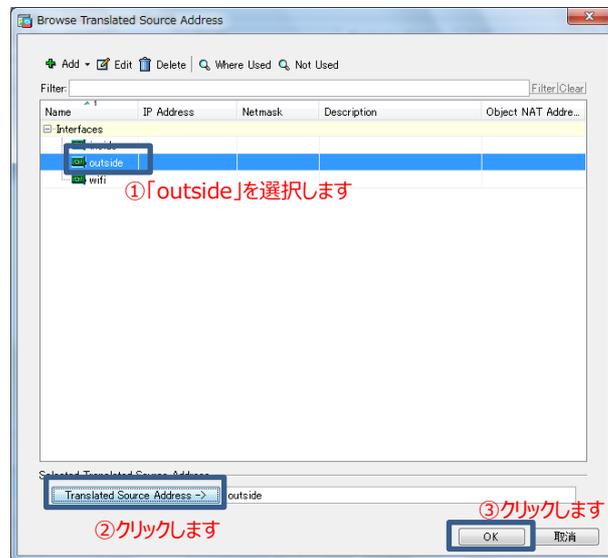


図 8 Translated Source Address の設定

- 4) NAT ルールの設定に戻り、「OK」をクリックして完了します。

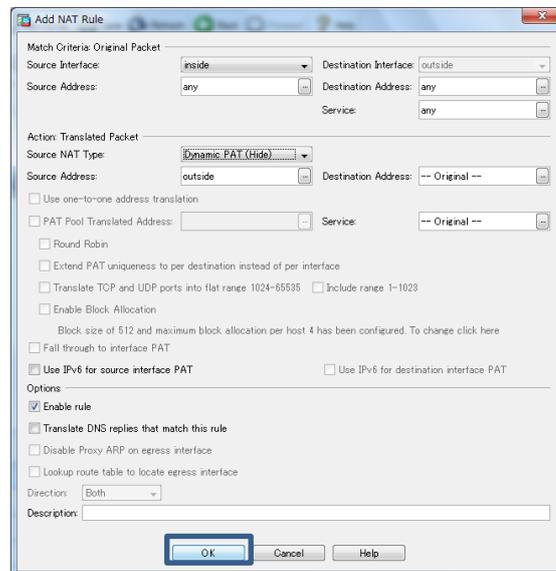


図 9 NAT ルールの追加



Cisco Start Firewall

Cisco ASA 5506-X

PAT (Port Address Translation) の設定



5) NAT ルールが作成されている事を確認し、「Apply」をクリックして ASA に設定を適用します。

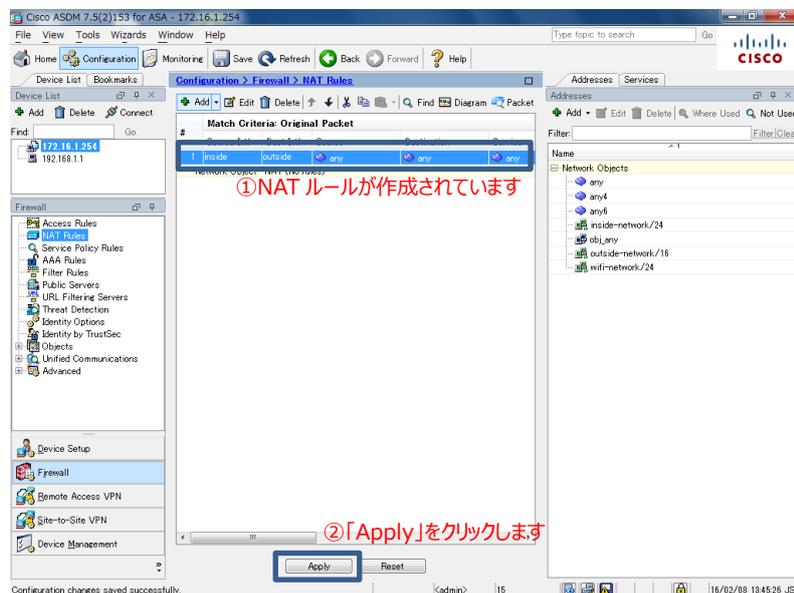


図 10 設定の適用

6) ASA に実行されるコマンドのプレビューが表示されるので、「Send」をクリックして実行します

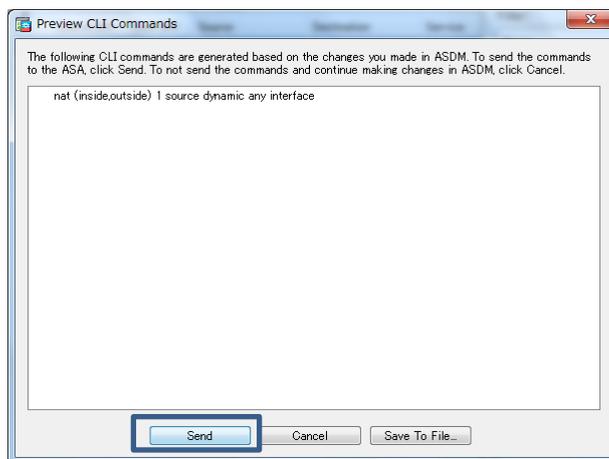


図 11 コマンドのプレビュー



3.3 PAT の設定 (対象のトラフィックを指定)

本節では PAT の対象トラフィックを Network Object により指定する場合の設定手順について説明します。ここでは別紙「Cisco ASA 5506-X Network Object Group と Service Group の設定」で作成した Network Object Group を使用します。

- 1) 「Configuration」>「Firewall」>「NAT Rules」を開き、「Add」をクリックして「Add NAT Rule Before “Network Object” NAT Rules」を開きます。

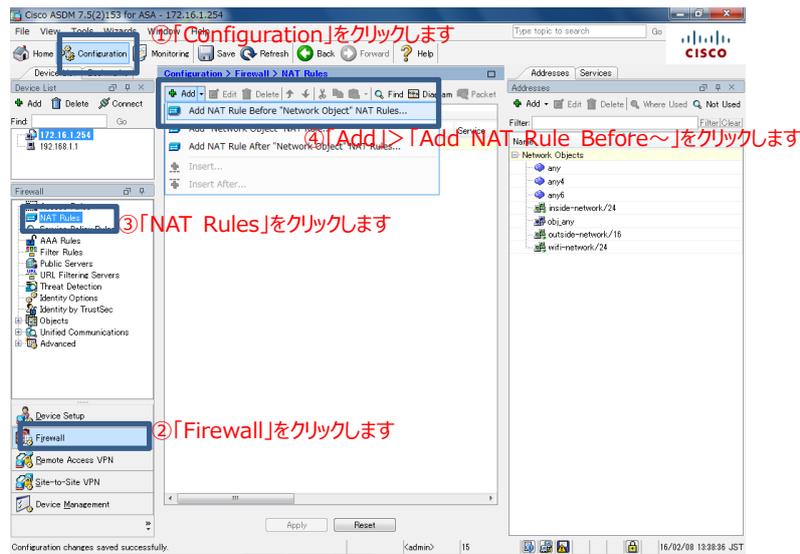


図 12 NAT ルールの設定に移動

- 2) 「Source Interface」を「inside」、「Destination Interface」を「outside」とし、「Source Address」の「…」をクリックします。

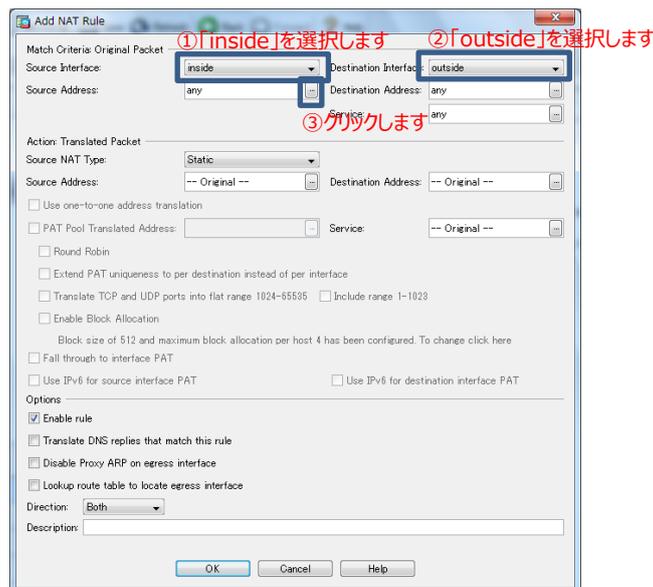


図 13 NAT ルールの設定



- 3) PAT の対象となる Source Address に Network Object を指定します。「Network Object Groups」で「Sales-Group-1」を選択し、「OK」をクリックします。

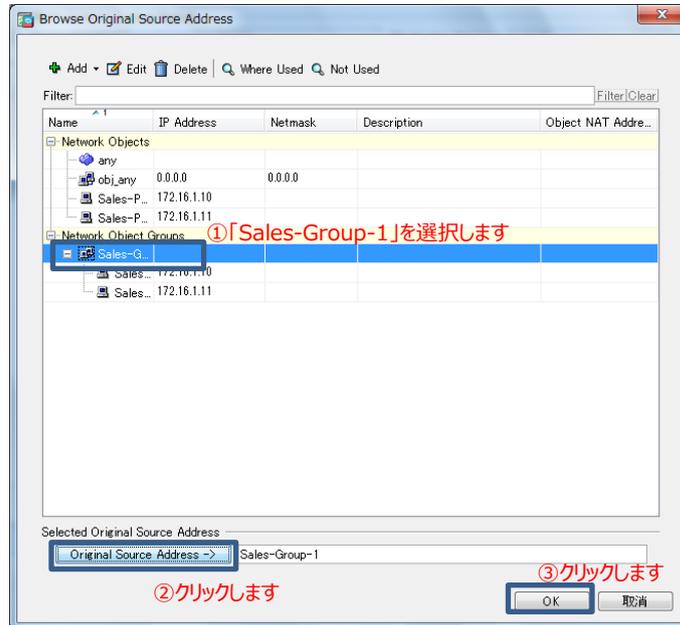


図 14 Source Address に Network Object Group を指定

- 1) 「Source NAT Type」は「Dynamic PAT (Hide) 」を選択し、「Source Address」の「…」をクリックします。

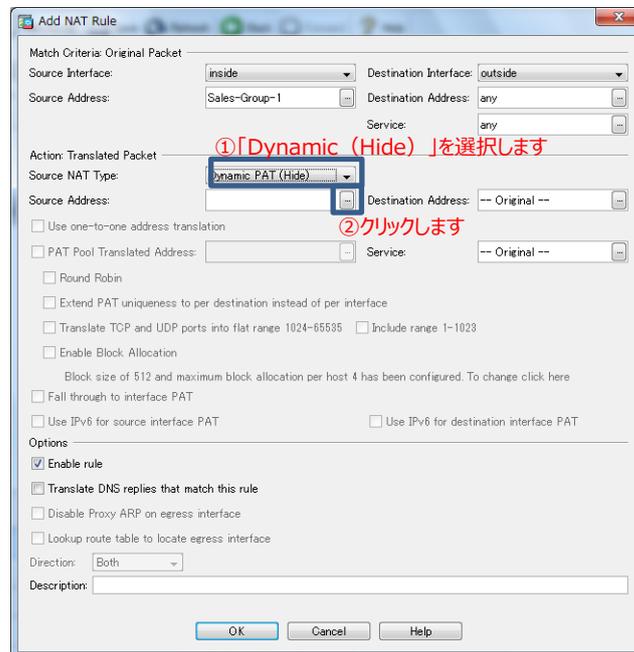


図 15 NAT ルール設定



- 2) 変換後の Source Address となるインタフェースを「outside」に指定し、「OK」をクリックします。

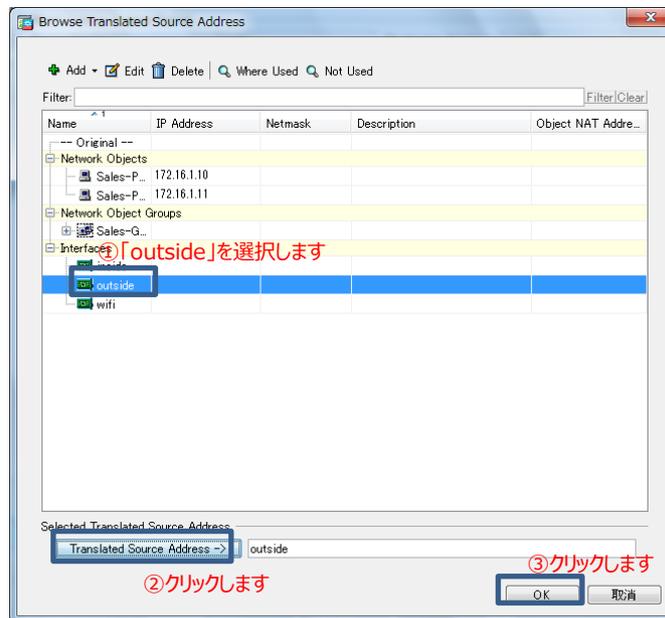


図 16 Translated Source Address の設定

- 3) 「OK」をクリックし、NAT ルールを追加します。

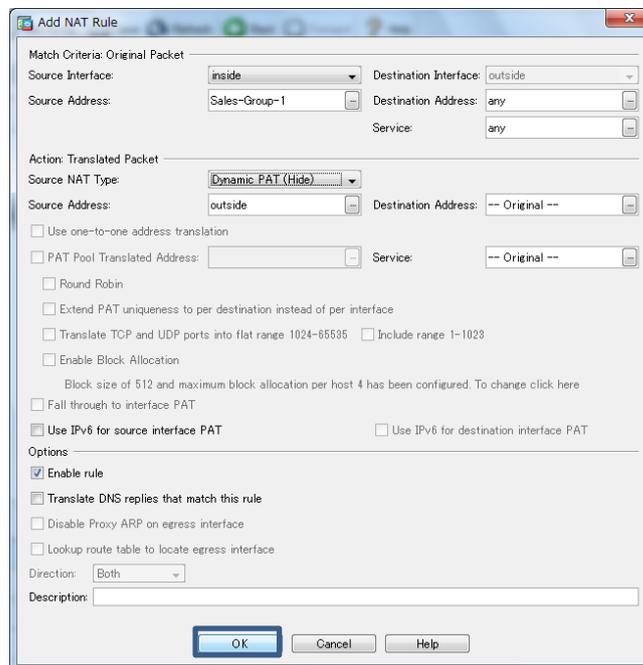


図 17 NAT ルールの追加



- 4) NAT ルールが作成されている事を確認し、「Apply」をクリックして ASA に設定を適用します。

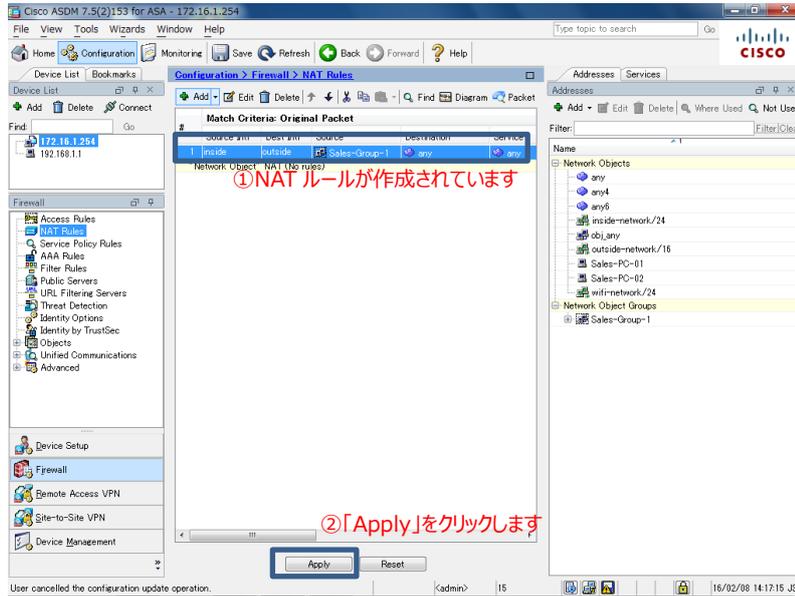


図 18 設定の適用

- 5) ASA に実行されるコマンドのプレビューが表示されるので、「Send」をクリックして実行します

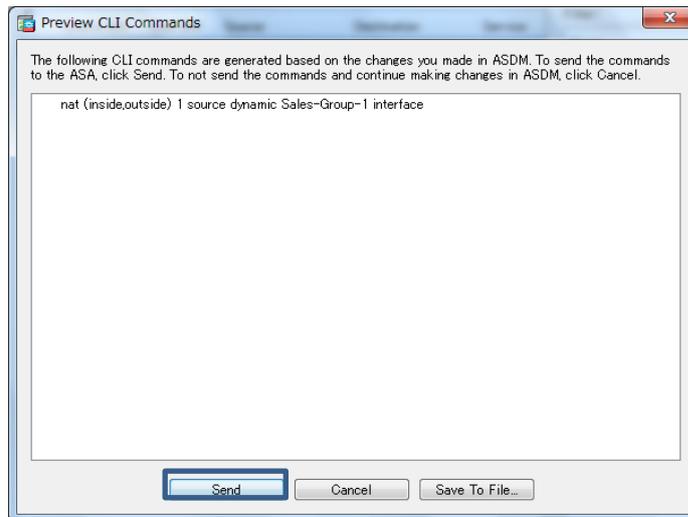


図 19 コマンドのプレビュー



3.4 PAT の確認

本節では、クライアント端末からインターネットへ PAT を介してアクセスできている状態で、ASA の PAT のログを確認する手順を説明します。

- 1) 「Tools」>「Command Line Interface」を開きます。

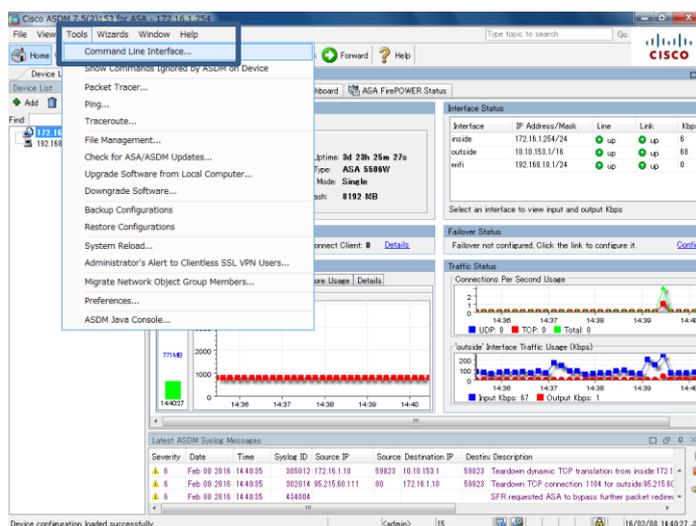


図 20 Command Line Interface を開く

- 2) 「show xlate」を選択して「send」をクリックし、コマンドを実行します。



図 21 show xlate の実行



Cisco Start Firewall

Cisco ASA 5506-X

PAT (Port Address Translation) の設定



- 3) 「Response」に PAT により inside 側の Source Address が outside 側の Source Address に変換されていることが確認できます。

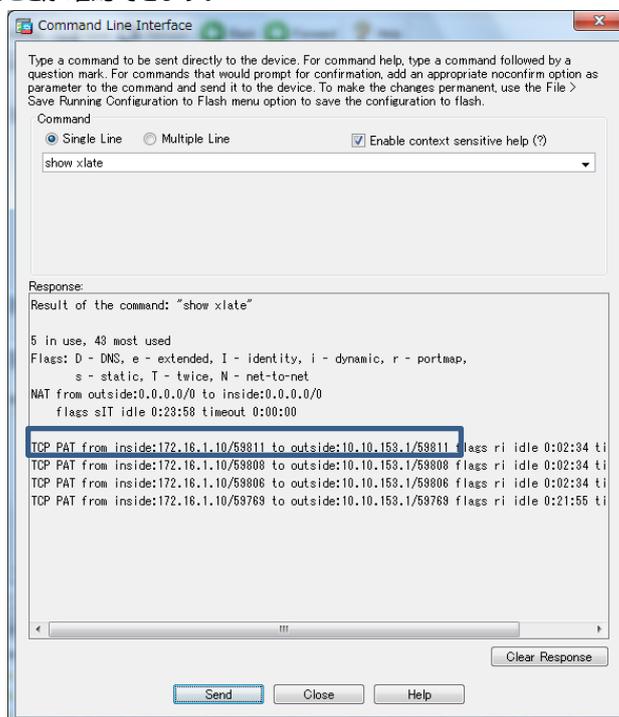


図 22 PAT によるアドレス変換の確認

お問い合わせ

Q 製品のご購入に関するお問い合わせ

<https://info-networld.smartseminar.jp/public/application/add/152>

Q ご購入後の製品導入に関するお問い合わせ

弊社担当営業にご連絡ください。

Q 製品の保守に関するお問い合わせ

保守開始案内に記載されている連絡先にご連絡ください。

本書に記載されているロゴ、会社名、製品名、サービス名は、一般に各社の登録商標または商標です。
本書では、®、™、©マークを省略しています。

www.networld.co.jp

株式会社ネットワーク

