Cisco Start Firewall

Cisco ASA 5506-X アクセスリストと静的 NAT による公開サーバの設定

2016 年 2 月 12 日
第 1.0 版

株式会社ネットワールド
Networld

改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016 年 2 月 12 日	ネットワールド	● 新規

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ルド(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ございません。
- 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ございません。

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
<italic>（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。

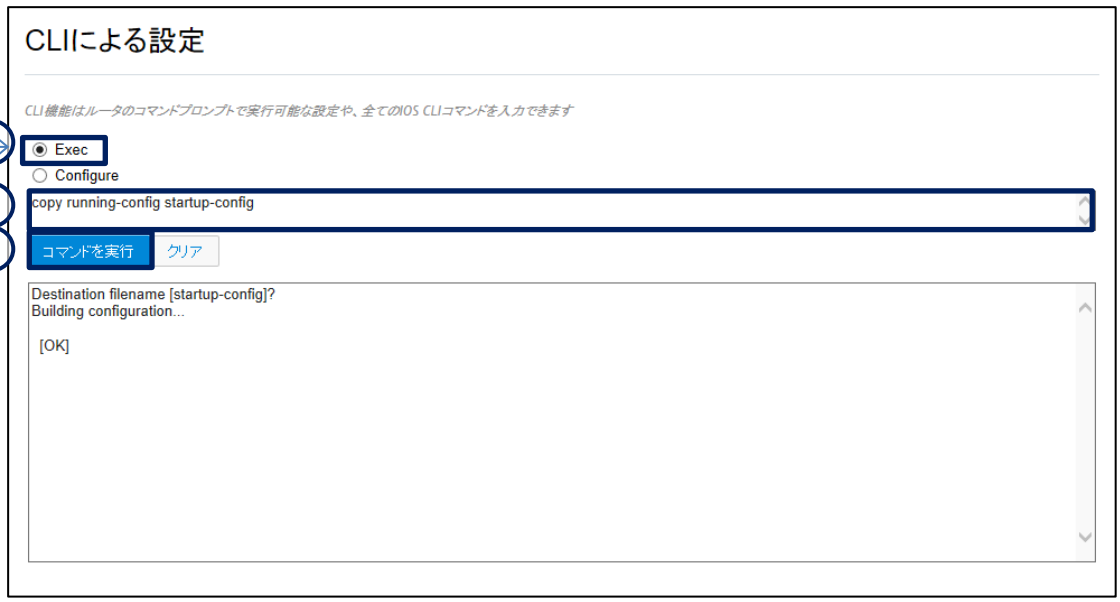
② テキストボックスに以下のコマンドを入力します。

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]



目次

1. はじめに

本書はCisco ASA 5506-Xにおけるアクセスリストと静的NATによる公開サーバの設定手順について説明しています。

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)
☑	☑

1.2 アクセスリストと静的 NAT について

アクセスリストは特定のホストやサービスに対してアクセスの許可もしくは不許可を定義する機能です。デフォルトではインターネット側（outside）から内部へはアクセスできませんが、アクセスリストを使用する事で、LAN 側の WEB サーバにインターネットからアクセスすることができます。また、LAN 側からインターネットへのアクセスを制御する際にも利用することができます。

静的 NAT は、あるインタフェースから他のインタフェースを通るトラフィックに対して、IP アドレスを静的に変換する機能です。LAN にある WEB サーバのプライベート IP アドレスをインターネットに公開する IP アドレスに変換することで、インターネット側から WEB サーバにアクセスが行えるようになります。

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。

別紙「Cisco ASA 5506-X クイックスタートガイド」の内容に基づいて初期設定が完了した状態となっています。GE1/1(outside)には DHCP によりグローバル IP アドレスが払い出され、インターネットからアクセスできる状態を前提としています。

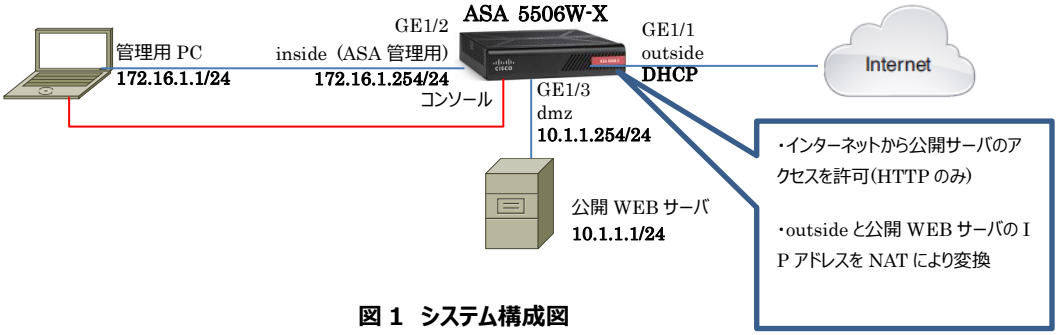


図 1 システム構成図

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	インタフェース設定
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) GE1/3 nameif:dmz IP アドレス:10.1.1.254/24 Security level:50(デフォルト)
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	・インターネット側へデフォルトルートを DHCP により取得
アクセスリスト	・outside から dmz のホスト 10.1.1.1 への HTTP アクセスを許可
NAT	・any→outside への PAT (デフォルト) ・outside と dmz のホスト 10.1.1.1 との静的 NAT

3. アクセスリストと静的 NAT の設定

3.1 DMZ インタフェースの設定

1) 管理 PC から ASDM により ASA にアクセスし、「Configuration」>「Device Setup」>「Interface Settings」>「Interfaces」を開き、「Gigabit Ethernet1/3」を選択して「Edit」を開きます。

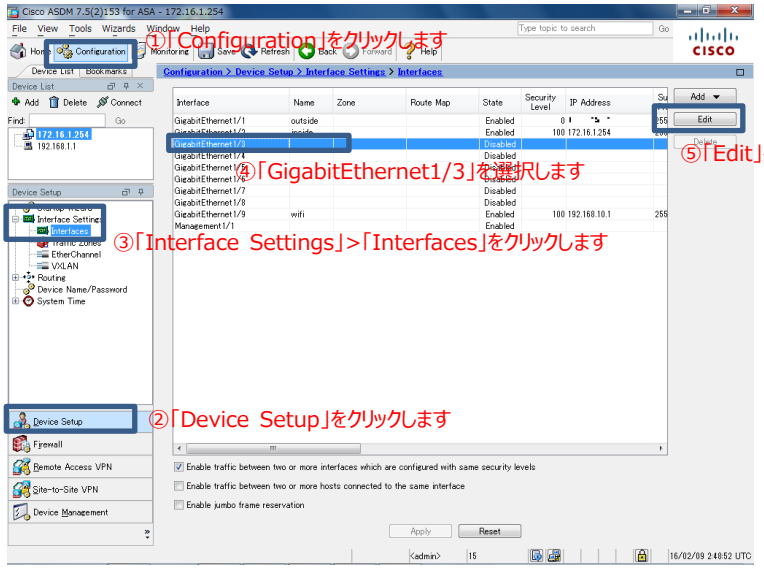


図 2 インタフェースの設定を開く

2) DMZ 用のインタフェースの設定を入力し、「OK」をクリックします。

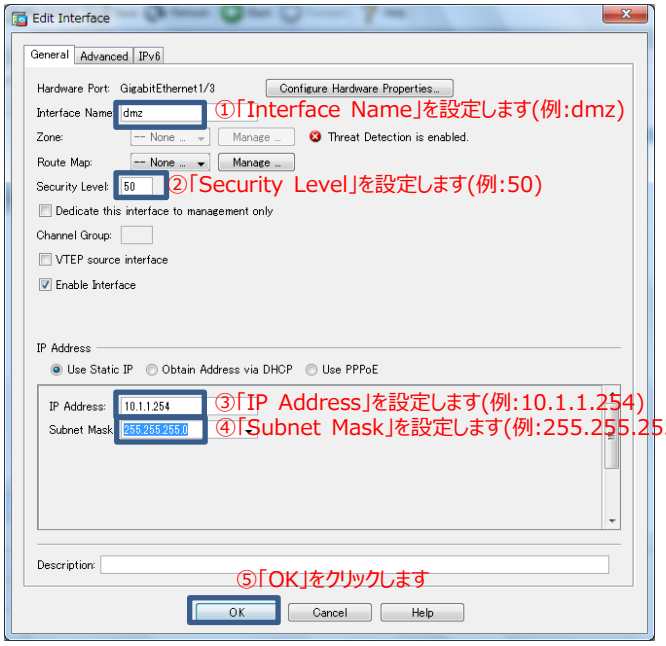


図 3 DMZ 用インタフェースの設定

3) Security Level の変更に対する警告文が表示されますが、「OK」をクリックして先に進みます。

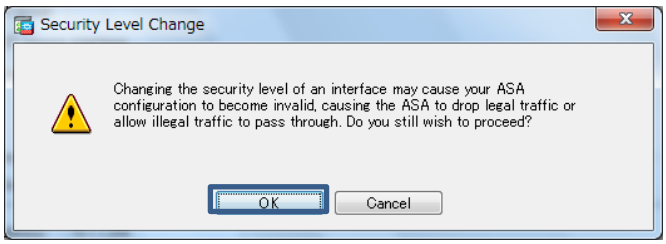


図 4 Security Level 変更の警告文

4) 「Apply」をクリックして ASA に設定を反映します。

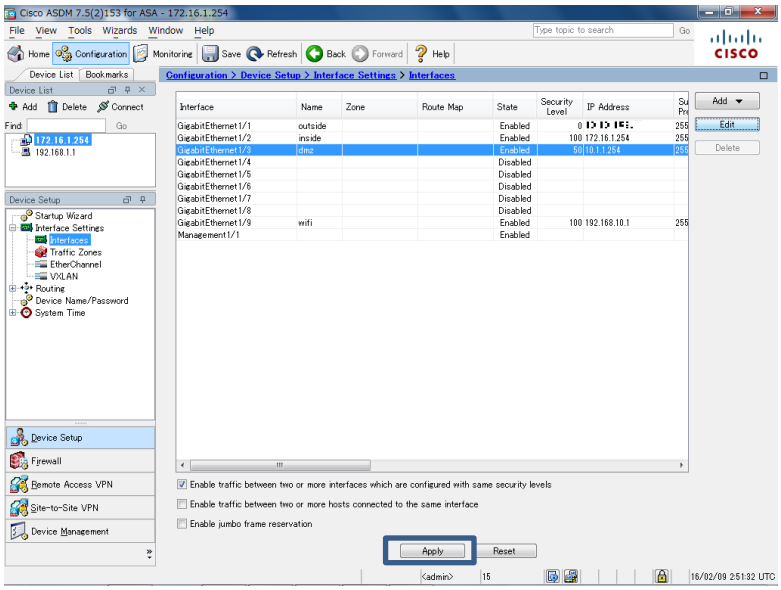


図 5 設定の反映

5) ASA に投入されるコマンドのプレビューが表示されますので、「Send」をクリックして実行します。

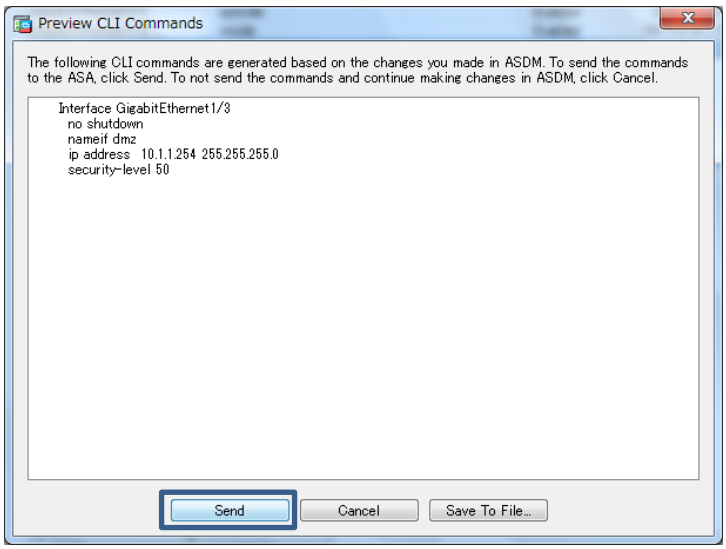


図 6 コマンドのプレビュー

3.2 アクセスリストの設定

本節では、インターネットから DMZ の WEB サーバへのアクセスを許可するためのアクセスリストの設定手順について説明します。

6) 「Configuration」>「Firewall」>「Access Rules」を開き、「Add」>「Add Access Rule」を開きます。

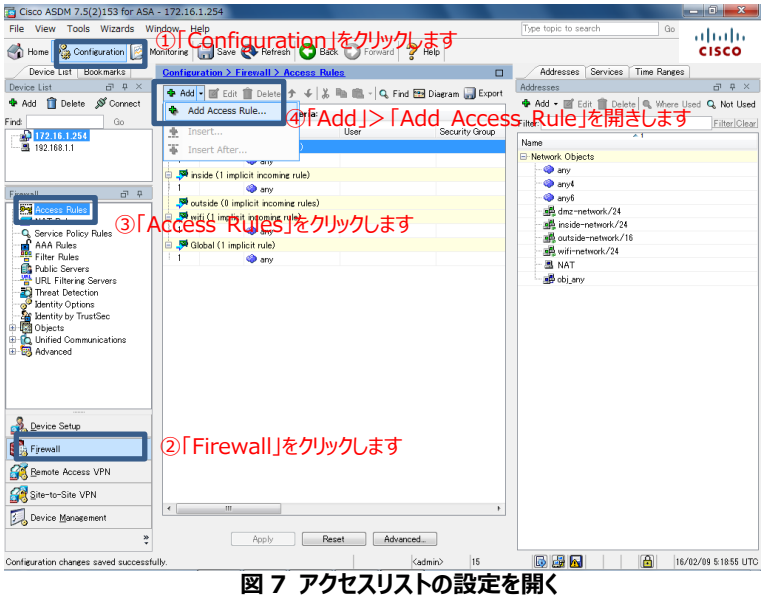


図 7 アクセスリストの設定を開く

7) アクセスリストの条件を入力し、「OK」をクリックします。

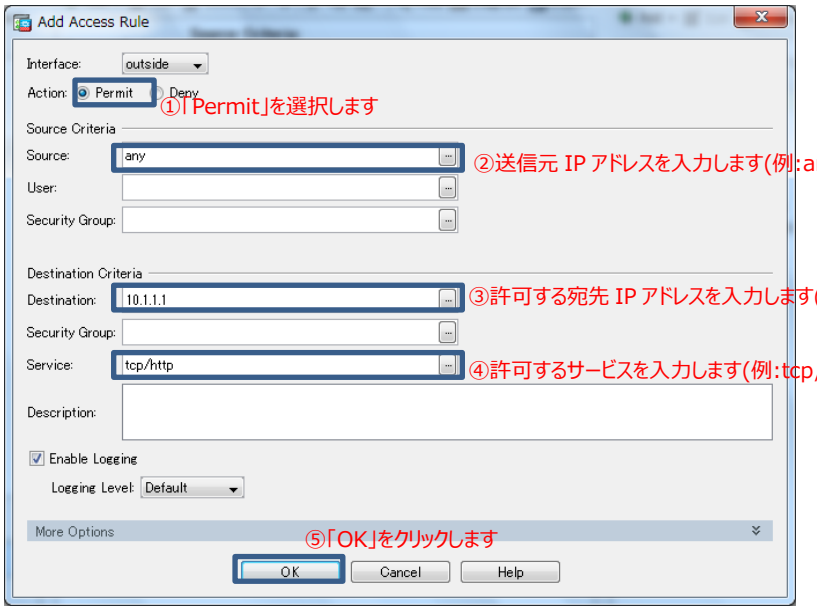


図 8 アクセスリストの設定

8) アクセスリストが作成されている事を確認し、「Apply」をクリックして ASA に設定を反映します。

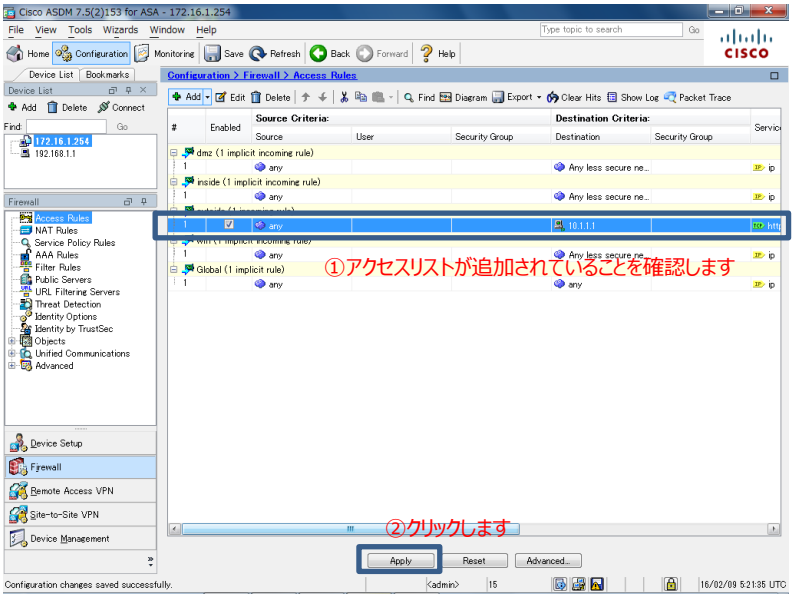


図 9 設定の反映

9) ASA に投入されるコマンドのプレビューが表示されますので、「Send」をクリックして実行します。

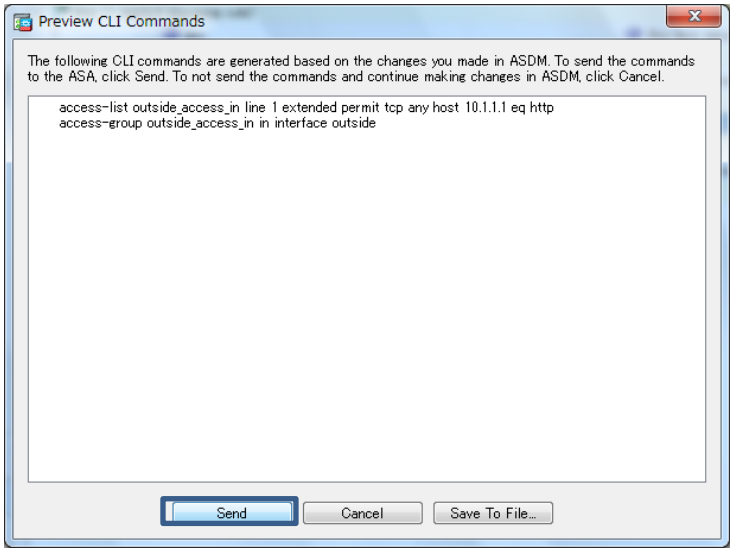


図 10 コマンドのプレビュー

3.3 静的 NAT の設定

1) 「Configuration」>「Firewall>「NAT Rules」を開き、「Add」>「Add “Network Object” NAT Rule」を開きます。

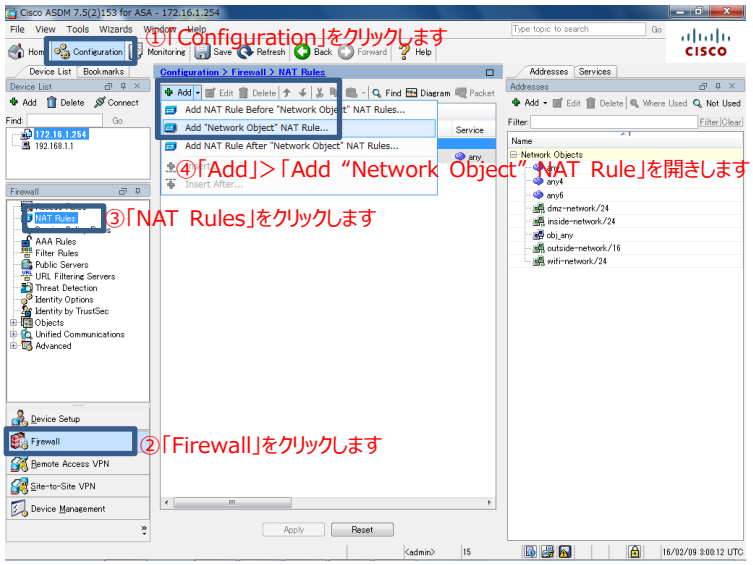


図 11 NAT ルールの設定を開く

2) NAT の設定を入力後、「Advanced」をクリックします。

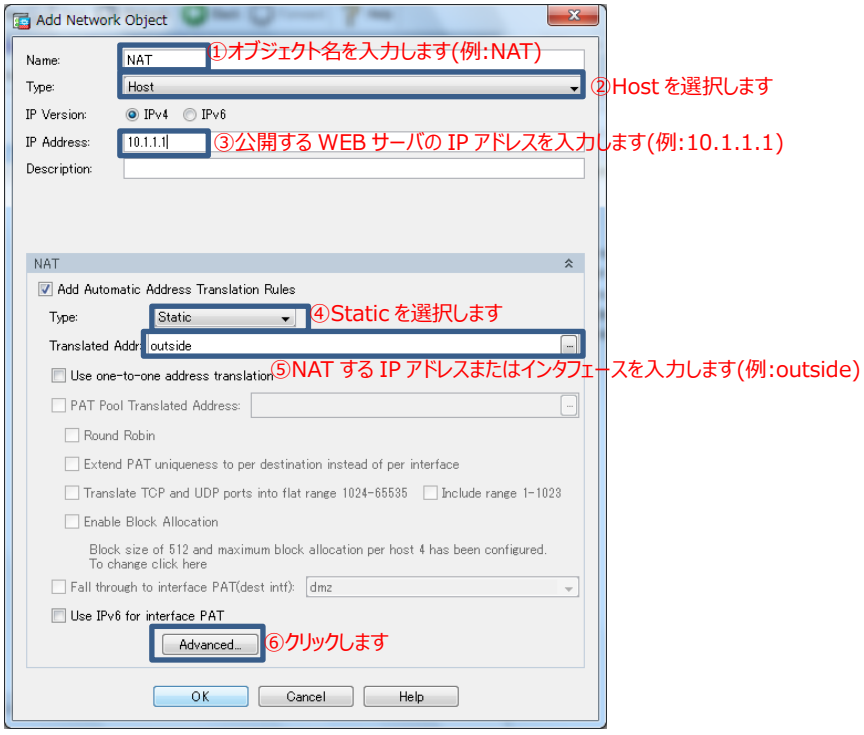


図 12 NAT ルールの設定

3) 公開するポートを設定し、「OK」をクリックします。

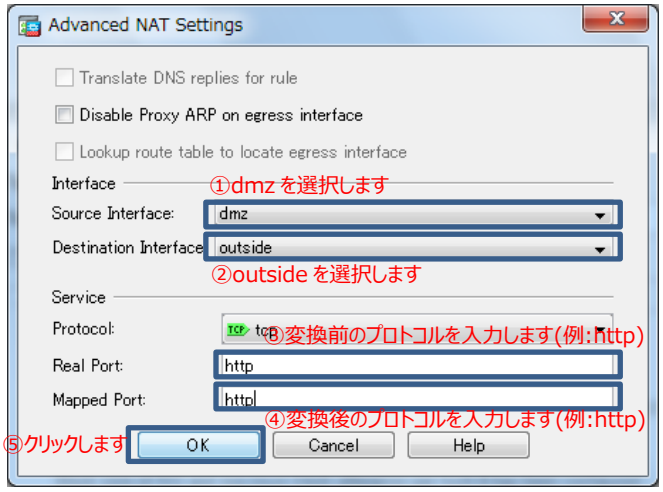


図 13 NAT ルールの設定(advanced)

4) 「OK」をクリックして NAT ルールの設定を完了します。

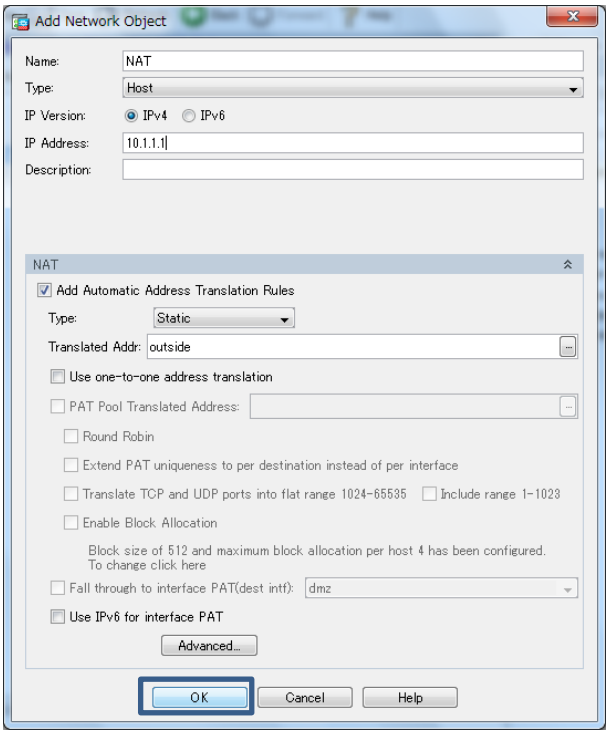


図 14 NAT ルール設定の完了

5) NAT ルールが追加されている事を確認し、「Apply」をクリックして ASA に設定を反映します。

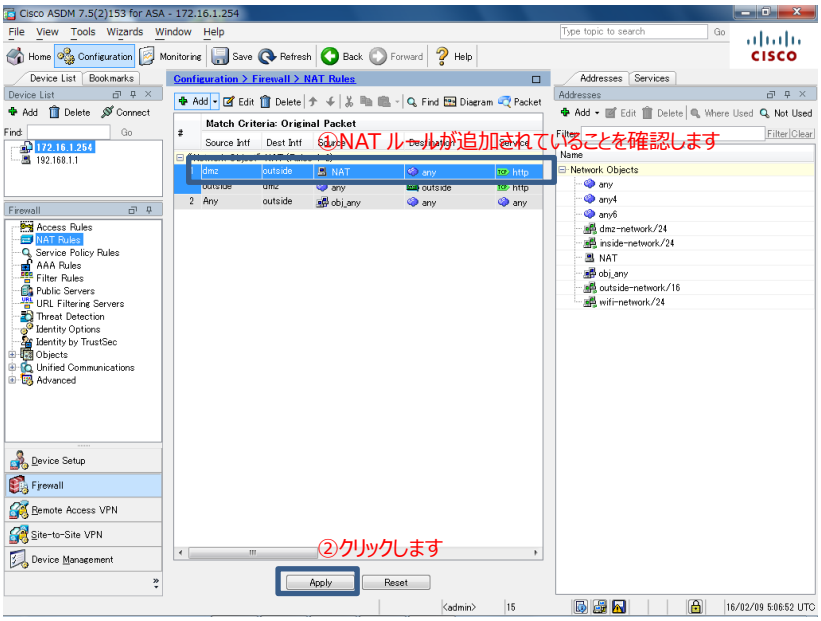


図 15 設定の反映

6) ASA に投入されるコマンドのプレビューが表示されますので、「Send」をクリックして実行します。

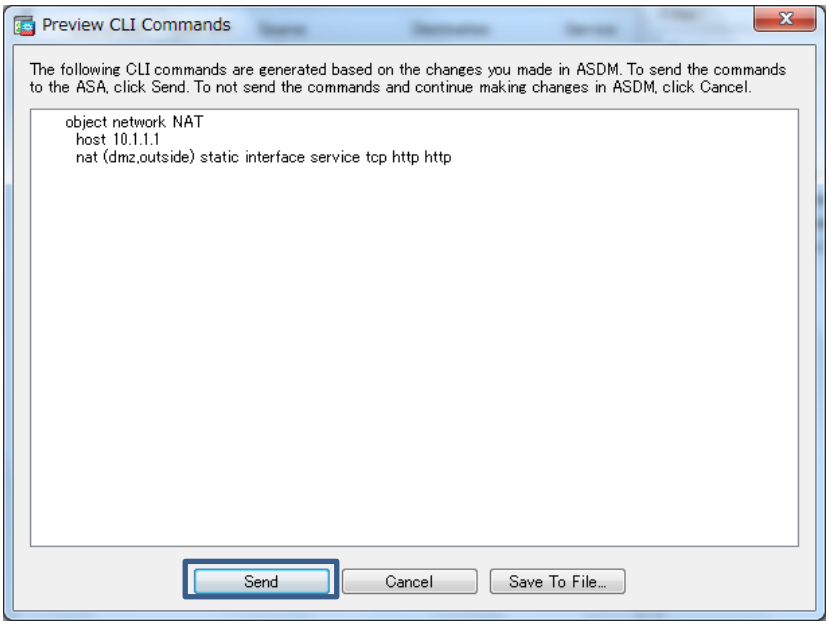


図 16 コマンドのプレビュー

7) ここまでで、DMZ の WEB サーバを、アクセスリストと静的 NAT によりインターネットに公開する設定が完了となります。インターネットより ASA の GE1/1(outside)の IP アドレスに HTTP アクセスし、WEB サーバにアクセスできるか確認して下さい。

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。

株式会社ネットワールド

Networld