デュアル内部ネットワーク用の ASA の設定

内容

概要

このドキュメントでは、ソフトウェア バージョン 9.x を実行する Cisco 適応型セキュリティ アプライアンス（ASA）を、2 つの内部ネットワークを使用するように設定する方法を説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメント内の情報は、ソフトウェア バージョン 9.x を実行している Cisco ASA に基づきます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ASA ファイアウォールの背後に 2 番目の内部ネットワークを追加する場合は、以下の点に留意してください。

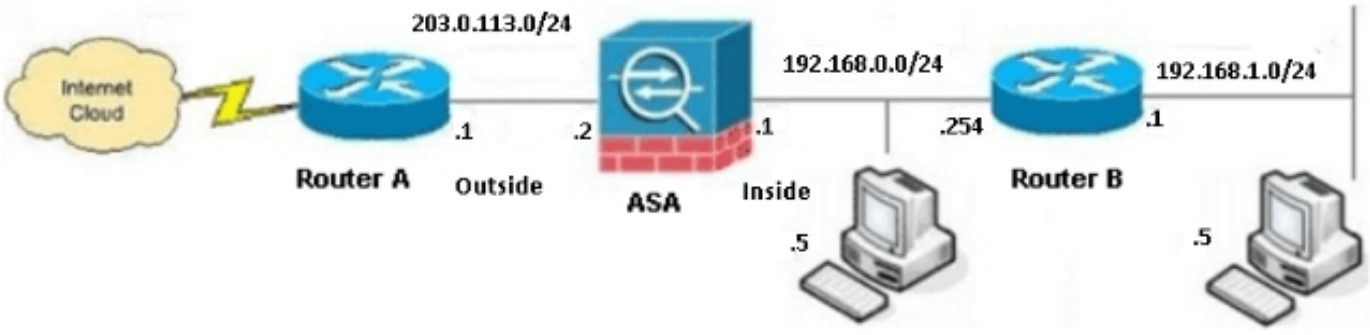
- ASA ではセカンダリ アドレッシングがサポートされていません。
- 現在のネットワークと新しく追加されるネットワーク間でルーティングを行うためには、ルータは ASA の背後で使用する必要があります。
- すべてのホストのデフォルト ゲートウェイが、内部ルータをポイントしている必要があります。
- ASA をポイントする内部ルータにデフォルト ルートを追加する必要があります。
- 内部ルータの Address Resolution Protocol（ARP）キャッシュをクリアする必要があります。

設定

この項で説明する情報を使用して、ASA を設定します。

ネットワーク図

以下に、このドキュメントの例で使用するトポロジを示します。



注：この設定で使用される IP アドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらは RFC 1918 アドレスであり、ラボ環境で使用されるものです。

ASA 9.x の設定

使用中のシスコ デバイスからの **write terminal コマンドの出力データがあれば、**[アウトプット インタープリタ ツール（登録ユーザ専用）を使用して、今後予想される障害と修正を表示できます。]

ソフトウェア バージョン 9.x が稼働している ASA の設定は以下のとおりです。

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
```

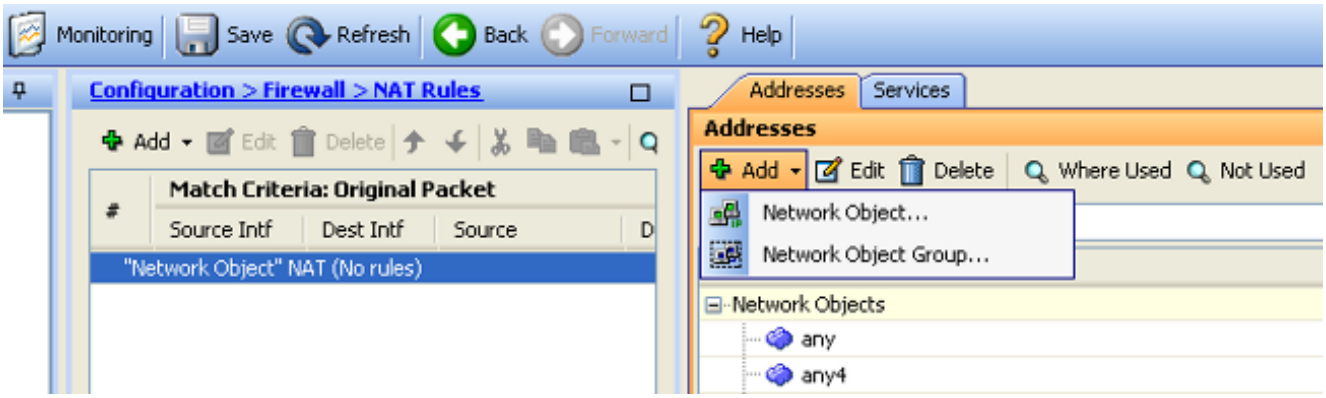
```
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

PAT を使用した inside ホストから outside ネットワークへのアクセスの許可

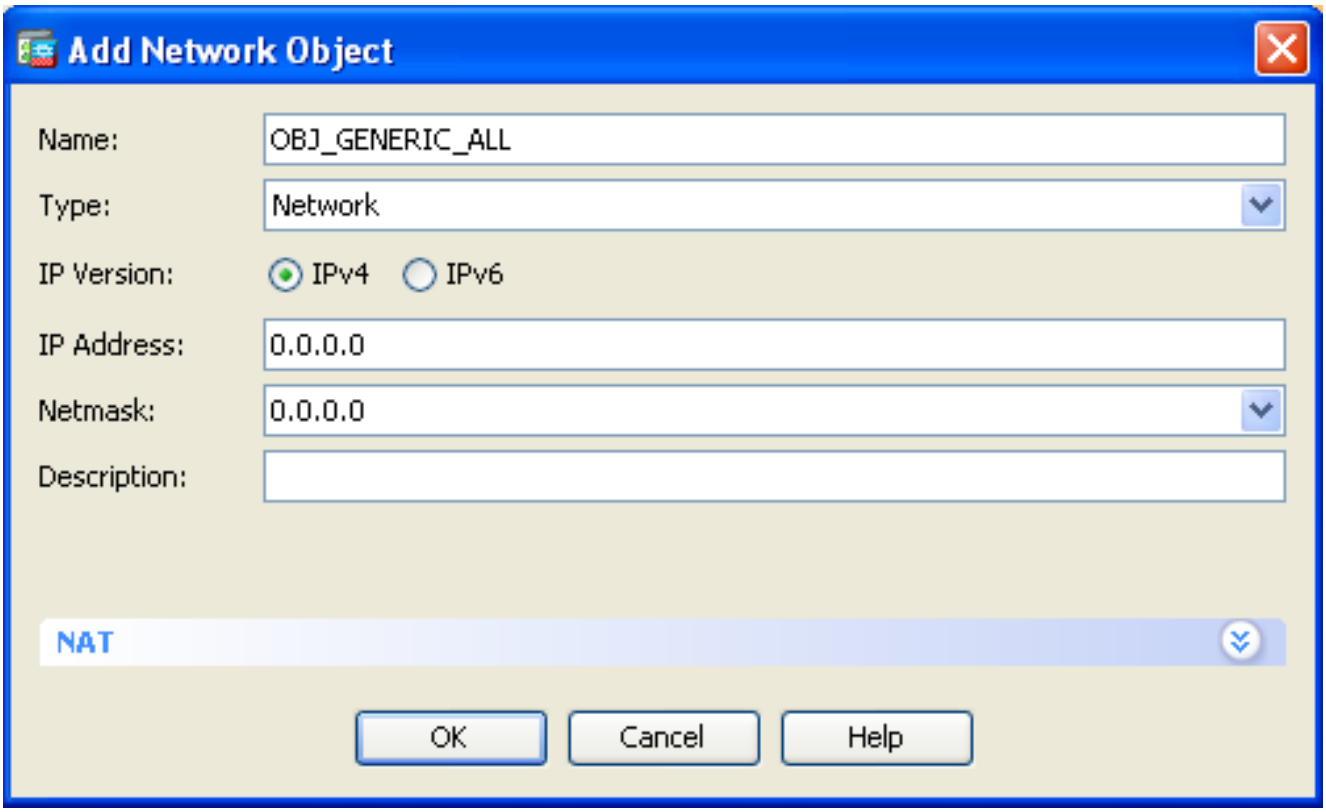
複数の内部ホストで、変換用に単一のパブリック アドレスを共有する場合は、ポート アドレス変換（PAT）を使用します。 最も単純な PAT 設定の 1 つは、すべての内部ホストを変換して外部インターフェイス IP のように見せることです。この PAT 設定は、ISP から使用できるルーティング可能な IP アドレスの数が少数に限られている場合、または 1 つしかない場合に使用される典型的な設定です。

PAT を使用して内部ホストから外部ネットワークへのアクセスを許可するには、次の手順を実行します。

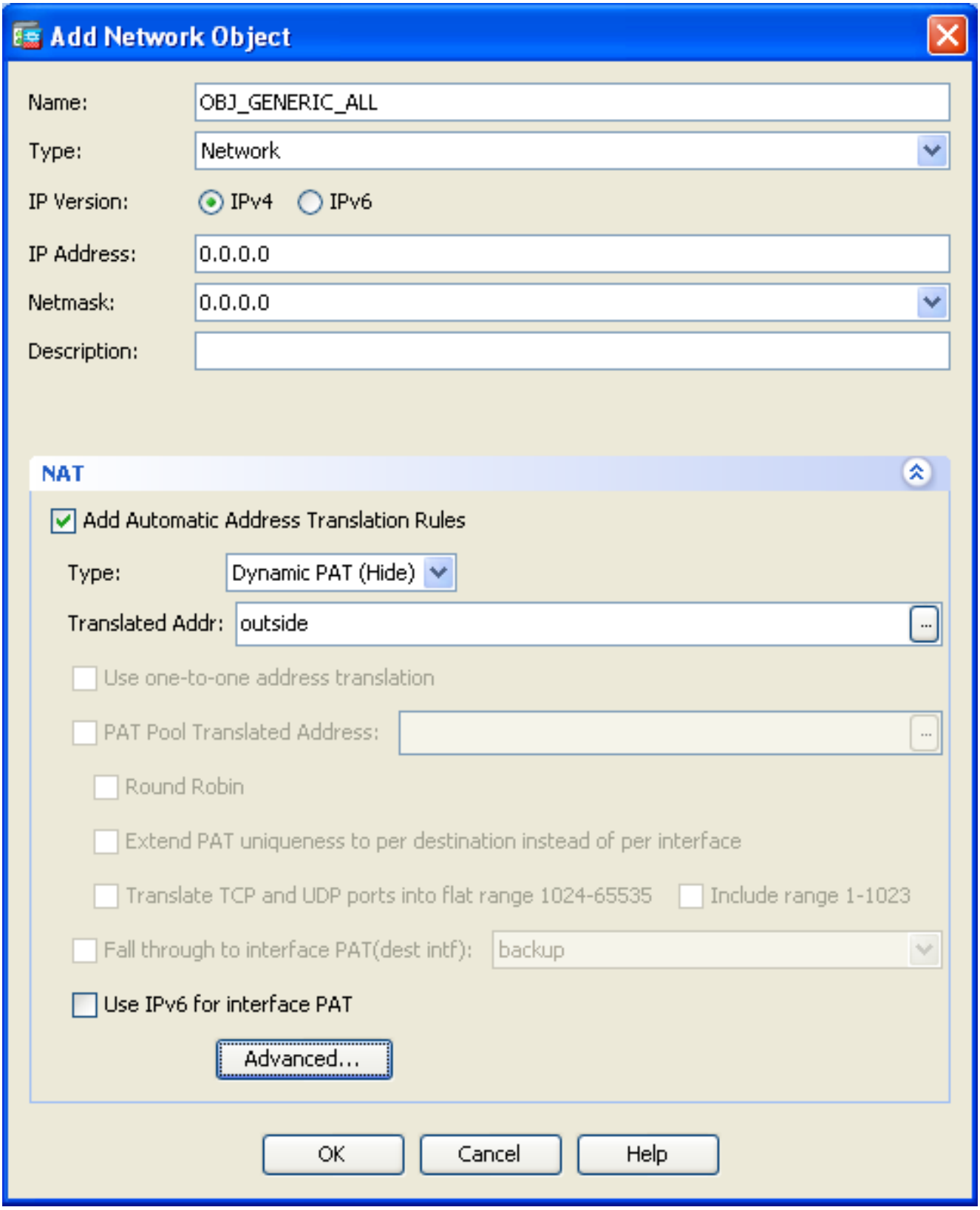
1. [Configuration] > [Firewall] > [NAT Rules] に移動し、[Add] をクリックして [Network Object] を選択し、ダイナミック NAT ルールを設定します。



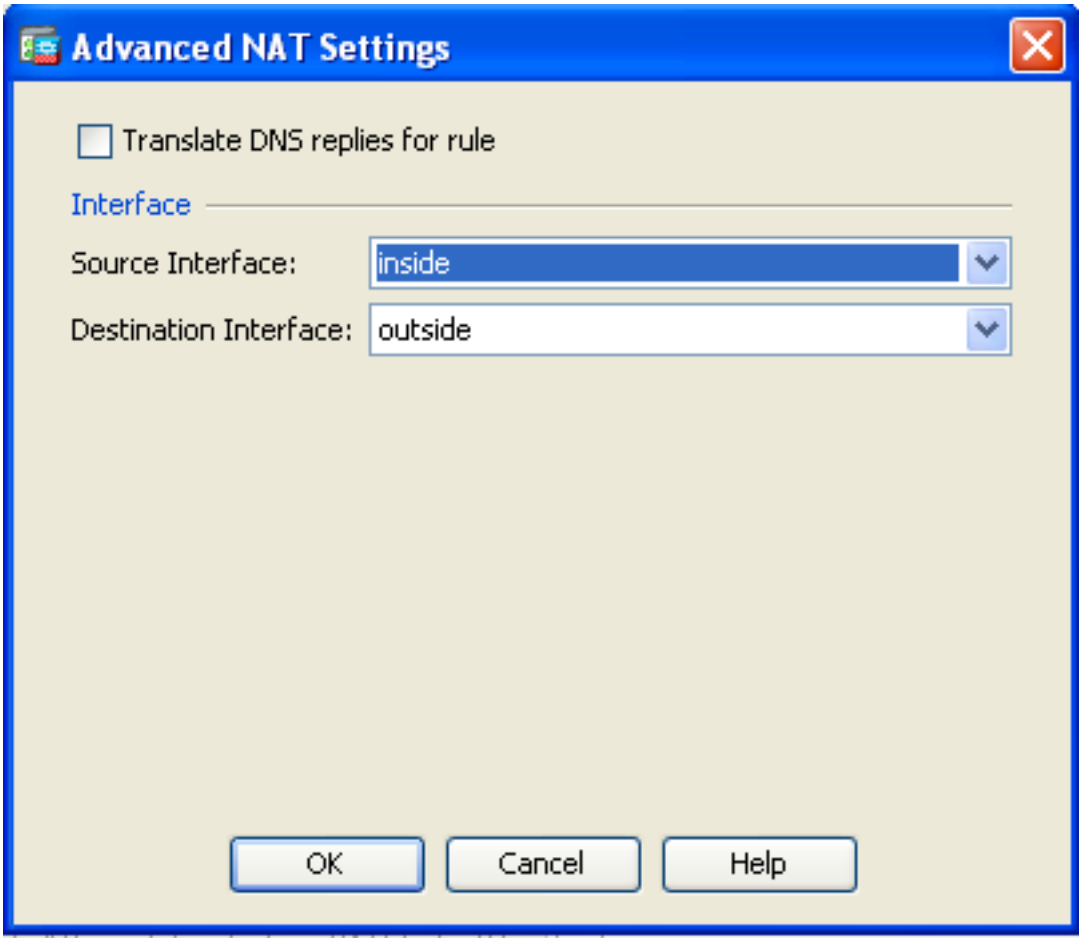
2. ダイナミック PAT を必要とするネットワーク/ホスト/範囲を設定します。以下の例では、すべての内部のサブネットが選択されています。このプロセスは、この方法で変換するすべてのサブネットについて繰り返す必要があります。



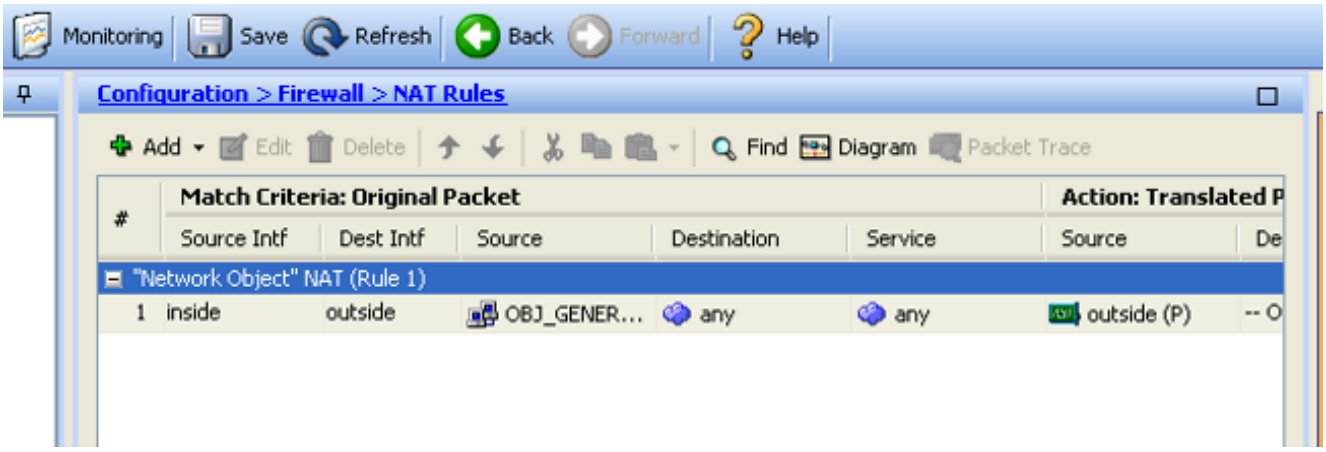
3. [NAT] をクリックし、[Add Automatic Address Translation Rule] **チェックボックスをオンにしてから、[Dynamic]** を入力し、外部インターフェイスを反映するように [Translated Addr] オプションを設定します。省略記号ボタンをクリックすると、外部インターフェイスなどの事前設定されたオブジェクトを選択することができます。



4. [Advanced] をクリックし、送信元および宛先インターフェイスを選択します。



5. [OK] をクリックし、次に [Apply] をクリックして変更を適用します。完了すると、Adaptive Security Device Manager（ASDM）に NAT ルールが示されます。



ルータ B の設定

ルータ B の設定は以下のとおりです。

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

確認

設定が正しく機能することを確認するには、Web ブラウザで HTTP を介して Web サイトにアクセスします。

この例では、IPアドレス*198.51.100.100*でホストされているサイトを使用しています。*接続が成功した場合*は、次のセクションに示す出力をASA CLIで確認できます。

Connection

接続を検証するには、**show connection address コマンドを入力します。**

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA はステートフル ファイアウォールであり、Web サーバからのリターン トラフィックはファイアウォール接続テーブル内にある接続の 1 つと一致するため、ファイアウォールの通過が許可されます。既存の接続と一致するトラフィックは、インターフェイス アクセス コントロール リスト（ACL）によってブロックされずにファイアウォールを通過することが許可されます。

上の出力では、内部インターフェイス上のクライアントが外部インターフェイスからの 198.51.100.100 ホストへの接続を確立しました。この接続では TCP プロトコルが使用されており、6 秒間アイドル状態です。接続のフラグは、この接続の現在の状態を示します。

> **注**：接続フラグの詳細については、『ASA の TCP 接続フラグ（接続の確立および切断）』シスコ ドキュメントを参照してください。

トラブルシュート

設定の問題をトラブルシューティングするには、この項で説明する情報を使用します。

Syslog

Syslog を表示するには **show log コマンドを入力します。**

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:192.168.1.5/58799 (203.0.113.2/58799)
```

ASA ファイアウォールは通常の動作中に Syslog を生成します。Syslog の詳細レベルはログ設定に基づきます。上記の出力例には 2 つの Syslog がレベル 6、つまり「*情報」レベルで示されています。*

この例では、2 つの Syslog が生成されています。最初の Syslog は、ファイアウォールが変換を作成したことを示すログ メッセージです。具体的には、ダイナミック TCP 変換（PAT）です。ここには、トラフィックが内部インターフェイスから外部インターフェイスに渡るときの、送信元 IP アドレスとポート、および変換後の IP アドレスとポートが示されています。

2 番目の Syslog はファイアウォールがクライアントとサーバ間のこの特定のトラフィック用に接続テーブルで接続を作成したことを示しています。この接続試行をブロックするようにファイアウォールが設定されている場合や、その他の要因（リソース制約または設定ミスの可能性）によってこの接続の作成が妨げられた場合は、ファイアウォールは接続が確立されたことを示すログを生成しません。代わりに、接続が拒否される理由や、接続の作成を妨げた要因に関する兆候を記録します。

パケット トレーサ

次のコマンドを入力して、パケット トレーサ機能を有効にします。

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

ASA のパケット トレーサ機能を使用すると、*シミュレートされたパケットを指定して、ファイアウォールでトラフィックを処理するときに行われるさまざまなステップ、チェック、機能をすべて確認できます。*このツールを使用すると、ファイアウォールを通過することが許可されるはずのトラフィックの例を識別するのに役立ち、その 5 タプルを使用してトラフィックをシミュレートできます。前記の例では、以下の条件を満たす接続試行をシミュレートするために、パケット トレーサを使用します。

- シミュレートされたパケットは内部インターフェイスに到達します。
- 使用されるプロトコルは TCP です。
- シミュレートされたクライアントの IP アドレスは 192.168.1.5 です。
- クライアントは送信元がポート 1234 であるトラフィックを送信します。
- トラフィックは、IP アドレス 198.51.100.100 のサーバ宛てに送信されます。
- トラフィックの宛先はポート 80 です。

コマンドには外部インターフェイスが指定されていないことに注意してください。これはパケット トレーサの設計によるものです。このツールは、このタイプの接続試行をファイアウォールでどのように処理するのかを示し、ルーティングの方法や、どのインターフェイスから送信するのかが含まれます。

> **ヒント**：パケット トレーサ機能の詳細については、『*Cisco ASA 5500 シリーズ CLI 8.4 および 8.6 を使用した構成ガイド*』の「パケット トレーサを使用したパケットのトレース」セクションを参照してください。

キャプチャ

キャプチャを適用するには、以下のコマンドを入力します。

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
```

```
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

ASA ファイアウォールでは、インターフェイスに着信または発信するトラフィックをキャプチャできます。このキャプチャ機能によって、トラフィックがファイアウォールに着信したかどうか、ファイアウォールを通過したかどうかを確実を証明できます。前の例は、内部インターフェイスの **capin と外部インターフェイスの capout という 2 つのキャプチャの設定を示しています。capture コマンドでは、match キーワードを使用して、キャプチャ対象のトラフィックを指定できます。**

*capinキャプチャの例では、tcp host 192.168.1.5 host 198.51.100.100に一致する内部インターフェイス（入力または出力）で見られるトラフィックを照合することが示されています。つまり、ホスト192.16から送信されるTCPトラフィックをホスト198.51.100.100に対して。1.5、またはその逆。*match キーワードを使用することで、ファイアウォールでトラフィックを双方向でキャプチャできます。外部インターフェイスに定義された **capture コマンドは、ファイアウォールがそのクライアントの IP アドレスに PAT を実行するため、内部クライアントの IP アドレスを参照しません。**したがって、そのクライアントの IP アドレスとは照合できません。代わりに、この例では、可能性のあるすべての IP アドレスがその基準と一致することを示すために any を使用します。

キャプチャを設定したら、次に接続の確立を再試行してから、**show capture *<capture_name>*** コマンドによるキャプチャの表示に進みます。この例では、キャプチャにある TCP の 3 ウェイ ハンドシェイクによって明らかなようにクライアントがサーバに接続できたことを確認できます。

関連情報

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500-X シリーズ次世代ファイアウォール
- Request For Comments（RFC）
- 『Cisco ASA シリーズ CLI 構成ガイド 9.0』の「スタティックおよびデフォルト ルートの構成」

- テクニカル サポートとドキュメント - Cisco Systems