Cisco Secure ASA Firewall で使用する NAT および PAT ステートメントの設定例

内容

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス（ASA）ファイアウォールでの Network Address Translation（NAT; ネットワーク アドレス変換）および Port Address Translation（PAT; ポート アドレス変換）の基本設定例を紹介しています。また、簡単なネットワーク ダイアグラムも紹介しています。詳細については、使用している ASA ソフトウェア バージョンに対応する ASA のマニュアルを参照してください。

この文書では、個別のユーザに合わせたシスコ デバイスの分析を行います。

詳細については、『ASA 上の NAT の設定』で、ASA 5500/5500-X シリーズ適応型セキュリティ アプライアンスに関する情報を参照してください。

前提条件

要件

Cisco Secure ASA Firewall についての知識があることが推奨されます。

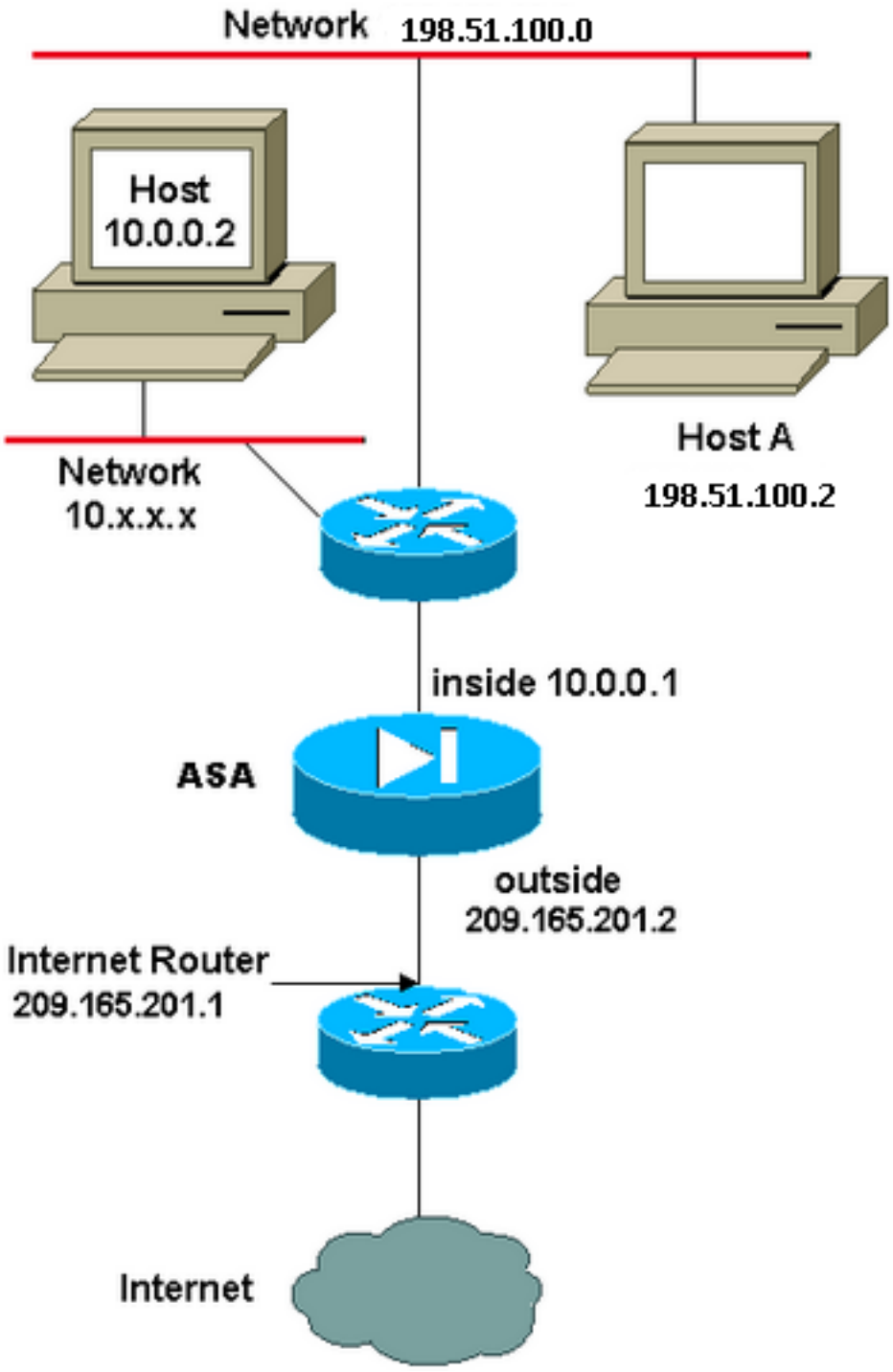
使用するコンポーネント

このドキュメントの情報は、Cisco ASA ファイアウォール ソフトウェア バージョン 8.4.2 以降に基づくものです。

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。

設定：手動および自動 NAT での複数の NAT ステートメント

ネットワーク図



この例では、ISPは209.165.201.1 ~ 209.165.201.30の範囲のIPアドレスブロック209.165.201.0/27をネットワークマネージャに提供します。ネットワークマネージャは、インターネットルータの内部インターフェイスに209.165.201.1、ASAの外部インターフェイスに209.165.201.2を割り当てることにします。

このネットワークには Class C アドレス 198.51.100.0/24 がすでに割り当てられ、これらのアドレスを使用してインターネットにアクセスするワークステーションが存在しています。これらのワークステーションには有効なアドレスが割り当てられているので、アドレス変換は不要です。ただし、新しいワークステーションには 10.0.0.0/8 ネットワーク内のアドレスが割り当てられるため、変換が必要です（RFC 1918 によると 10.x.x.x はルーティング不可能なアドレス レンジです）。

このネットワーク設計に対応するには、次のように、ASA 設定で 2 つの NAT 設定と 1 つのグローバル プールを使用する必要があります。

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

このコンフィギュレーションでは、198.51.100.0/24 ネットワークからのアウトバウンド トラフィックで送信元アドレスが変換されるものはありません。この設定では、10.0.0.0/8 ネットワーク内の送信元アドレスが、209.165.201.3 ~ 209.165.201.30 の範囲のアドレスに変換されます。

> **注**：NAT ポリシーを使用するインターフェイスがあり、他のインターフェイスに対するグローバル プールがない場合は、nat 0 を使用して NAT 例外を設定する必要があります。

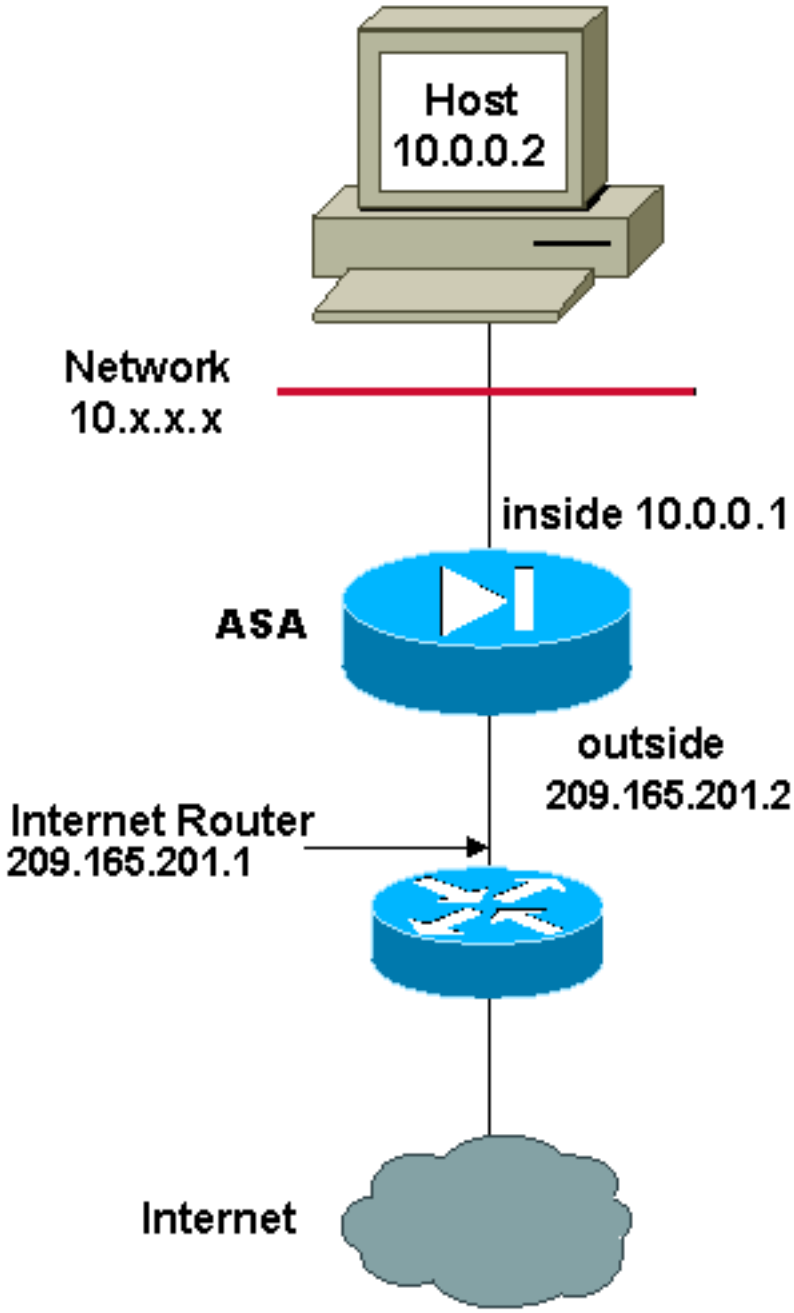
ASA バージョン 8.3 以降

次に設定を示します。

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

設定：複数のグローバル プール

ネットワーク図



この例では、インターネットに登録されている 2 つの IP アドレス範囲がネットワーク管理者に提供されています。ネットワーク管理者は、10.0.0.0/8 の範囲にあるすべての内部アドレスを登録アドレスに変換する必要があります。ネットワーク管理者が使用する必要があるIPアドレスの範囲は、209.165.201.1 ~ 209.165.201.30および209.165.200.225 ~ 209.165.200.254です。ネットワーク管理者は、次の操作を実行できます。

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
global (outside) 1 209.165.200.225-209.165.200.254 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

> **注**：NAT ステートメントでは、ワイルドカード アドレッシング方式が使用されています。この文は、ASA に対して、インターネットへの送出時にすべての内部発信元アドレスを変換するよう指示しています。必要な場合は、このコマンドのアドレスをさらに絞り込むことができます。

ASA バージョン 8.3 以降

次に設定を示します。

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0
```

Using the Manual Nat statements:

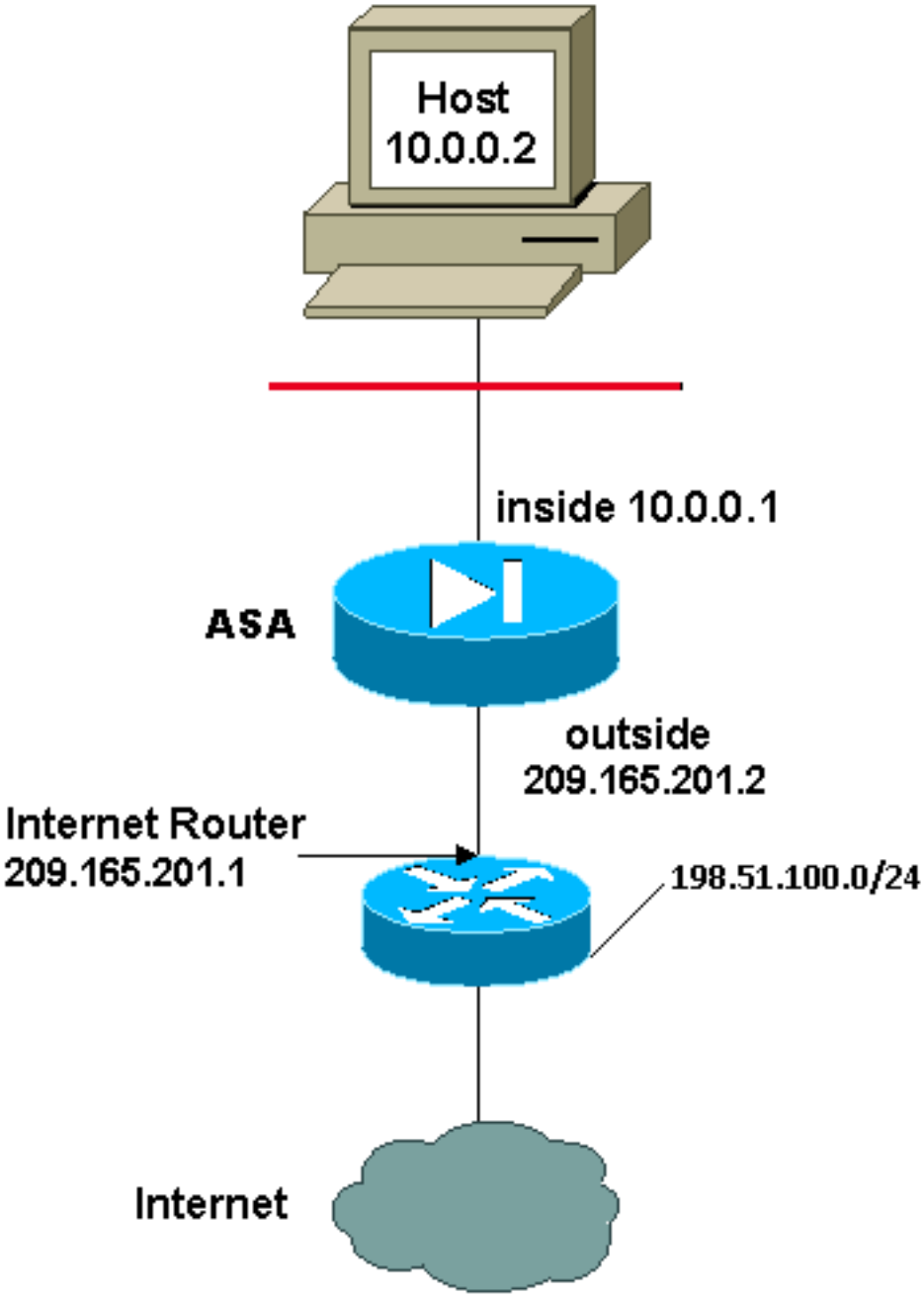
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

Using the Auto Nat statements:

```
object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

設定：NAT および PAT ステートメントの混合

ネットワーク図



この例では、ISP からネットワーク管理者に対し、会社用に 209.165.201.1 ~ 209.165.201.30 の範囲のアドレスが提供されています。ネットワーク管理者は、インターネット ルータの Inside インターフェイスに 209.165.201.1 を、ASA の Outside インターフェイスに 209.165.201.2 をそれぞれ割り当てることに決めました。したがって、NAT プールには残りの 209.165.201.3 ~ 209.165.201.30 を使用できます。ただし、この会社では同時に 28 人以上のユーザが ASA から外部にアクセスする可能性があります。したがって、ネットワーク管理者は複数のユーザが 1 つのアドレスを同時に共有できるように、209.165.201.30 を PAT アドレスとして使用することに決定しました。

これらのコマンドは、ASA を通過する最初の 27 名の内部ユーザについて、その送信元アドレスを 209.165.201.3 ~ 209.165.201.29 に変換するように ASA に指示しています。これらのアドレスが使い果たされると、ASA では、NAT プール内のアドレスの 1 つが解放されるまで、後続の送信元アドレスすべてを 209.165.201.30 に変換することになります。

注：NAT ステートメントでは、ワイルドカード アドレッシング方式が使用されています。この文は、ASA に対して、インターネットへの送出時にすべての内部発信元アドレスを変

換するよう指示しています。必要な場合は、このコマンドのアドレスをさらに絞り込むことができます。

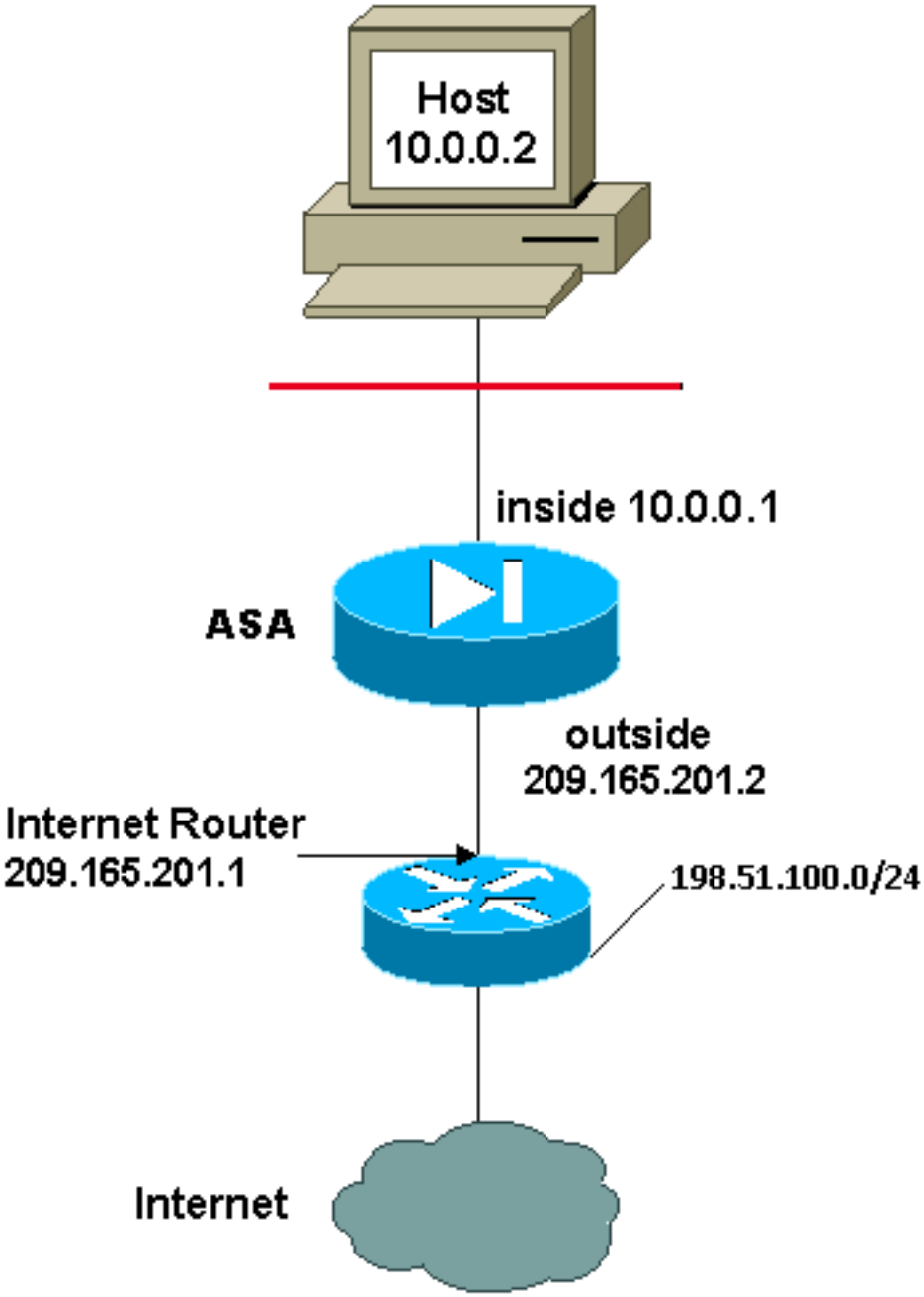
ASA バージョン 8.3 以降

次に設定を示します。

```
Using the Manual Nat statements:
object network any-1
subnet 0.0.0.0 0.0.0.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
subnet 209.165.201.30 255.255.255.224

nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

設定：手動ステートメントでの複数の NAT ステートメント

ネットワーク図



この例では、ISPからネットワーク管理者に209.165.201.1 ~ 209.165.201.30の範囲のアドレスが再度提供されます。ネットワーク管理者は、インターネットルータの内部インターフェイスに209.165.201.1、ASAの外部インターフェイスに209.165.201.2を割り当てることにします。

ただし、このシナリオでは、インターネット ルータの他に別のプライベート LAN セグメントが存在しています。ネットワーク管理者は、通常、これら 2 つのネットワーク上のホスト同士が通信する際にグローバル プールのアドレスを無駄に使用しないようにすることを選好します。それでも、内部ユーザ（10.0.0.0/8）がインターネットにアクセスする際には、必ず送信元アドレスを変換する必要があります。

この設定では、送信元アドレスが10.0.0.0/8、宛先アドレスが198.51.100.0/24のアドレスは変換されません。10.0.0.0/8ネットワーク内から開始され、198.51.100.0/24以外の任意の宛先へのトラフィックの送信元アドレスは、209.165.201.3 ~ 209.165.201.30のアドレスに変換されます。

シスコ デバイスからの **write terminal コマンドの出力がある場合、**Output Interpreter Tool（登録ユーザ専用）を使用できます。

ASA バージョン 8.3 以降

次に設定を示します。

Using the Manual Nat statements:

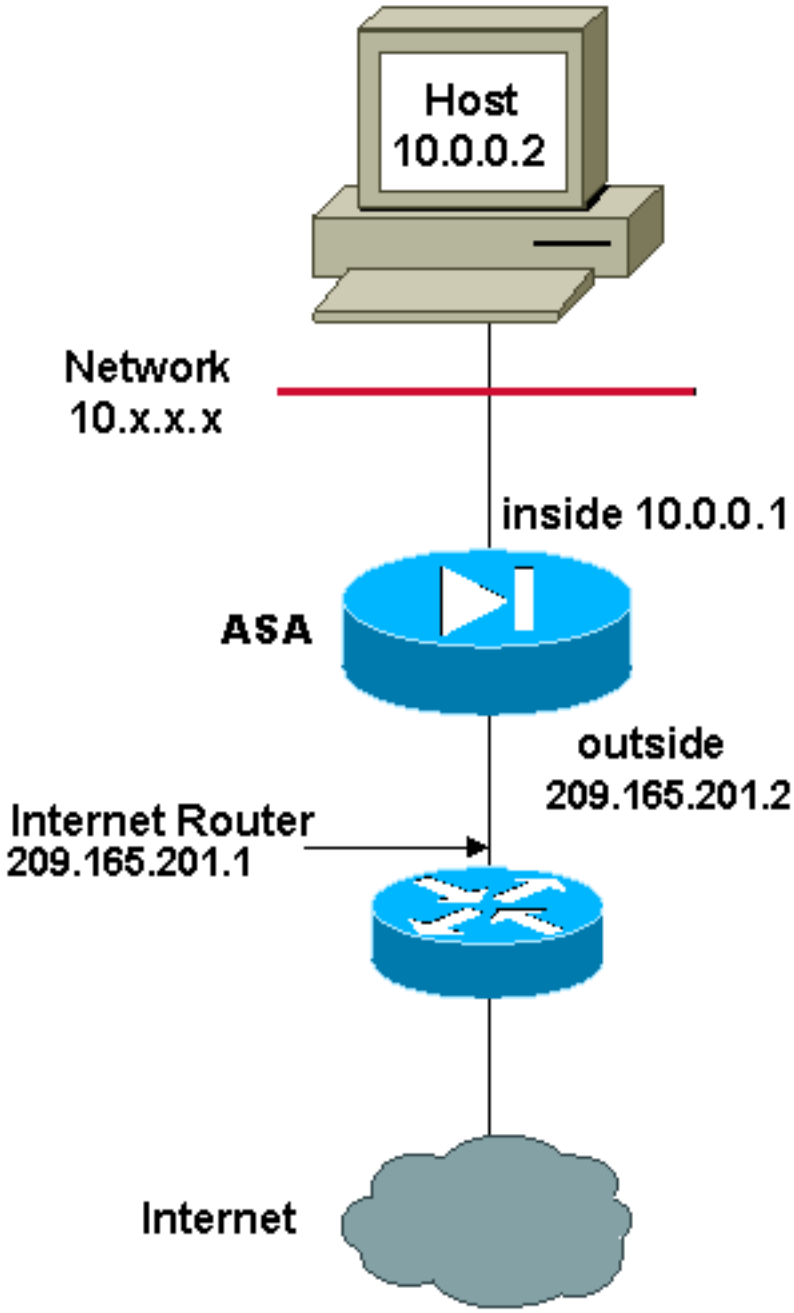
```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

設定：ポリシー NAT の使用

ネットワーク図



0 以外の NAT ID の **nat コマンドでアクセス リストを使用すると、ポリシー NAT が有効になります。**

ポリシー NAT を使用すると、アクセス リストでの送信元および宛先アドレス（またはポート）の指定により、アドレス変換に対するローカル トラフィックを識別できます。通常の NAT で使用されるのは、送信元のアドレス/ポートだけです。ポリシー NAT では、送信元と宛先の両方のアドレス/ポートが使用されます。

> **注：**NAT 免除（nat 0 access-list）を除き、すべてのタイプの NAT でポリシー NAT がサポートされています。NAT 例外では、ローカル アドレスの識別にアクセス コントロール リスト（ACL）が使用されますが、ポートは考慮されないという点がポリシー NAT と異なります。

ポリシー NAT では、発信元/ポートと宛先/ポートの組み合わせが設定ごとに一意である限り、同じローカル アドレスを識別する複数の NAT 設定やスタティック設定を作成できます。これにより、それぞれの送信元ポートと宛先ポートのペアに対して異なるグローバル アドレスを対応させることができます。

この例では、ポート 80（Web）とポート 23（Telnet）が宛先 IP アドレス 172.30.1.11 にアクセスできるようにする必要がありますが、送信元アドレスとして 2 つの異なる IP アドレスを使用する必要があります。209.165.201.3 を Web 用の送信元アドレスとして使用し、209.165.201.4 を Telnet 用に使用します。また、10.0.0.0/8 の範囲のすべての内部アドレスを変換する必要があります。ネットワーク管理者は、次の方法でこれを実現できます。

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0
172.30.1.11 255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 209.165.201.3 255.255.255.224
global (outside) 2 209.165.201.4 255.255.255.224
```

ASA バージョン 8.3 以降

次に設定を示します。

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-172.30.1.11
host 172.30.1.11

object network obj-209.165.201.3
host 209.165.201.3

object network obj-209.165.201.4
host 209.165.201.4

object service obj-23
service tcp destination eq telnet

object service obj-80
service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

> **注**：ASA バージョン 8.4 上の NAT および PAT の設定の詳細は、『NAT に関する情報』を参照してください。
>
> ASA バージョン 8.4 上のアクセス リスト設定の詳細は、『アクセス リストに関する情報』を参照してください。

確認

Webブラウザで HTTP経由でWebサイトにアクセスしてみてください。この例では、

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、次のセクションの出力をASA CLIで確認できます。

Connection

```
ASA(config)# show connection address 10.0.0.2
16 in use, 19 most used
TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137,
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の***接続の 1 つと一致するため、ファイアウォールの通過を許可されます。***事前に存在する接続の 1 つと一致するトラフィックは、インターフェイス ACL によってブロックされないでファイアウォールの通過を許可されます。

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。接続のフラグの詳細については、『ASA の TCP 接続フラグ』を参照してください。

Syslog

```
ASA(config)# show log | in 10.0.0.2

Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.0.0.2/57431 to outside:209.165.201.3/57431

Jun 28 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:10.0.0.2/57431 (209.165.201.3/57431)
```

ASA ファイアウォールは正常動作中に 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。この出力はレベル 6、つまり「情報」レベルでの 2 種類の syslog を示します。

この例では、2 つの Syslog が生成されています。1 番目は、ファイアウォールが変換を作成したこと、具体的にはダイナミックな TCP の変換（PAT）を行ったことを示すログ メッセージです。 これは、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 アドレスとポートを示します。

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た場合や、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る場合は、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。通常は、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。

NAT 変換（Xlate）

```
ASA(config)# show xlate local 10.0.0.2
3 1in use, 810 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
```

```
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
0:12:22 timeout 0:00:30
```

この設定の一部として、内部ホストの IP アドレスをインターネットでルーティングできるアドレスに変換するために PAT が設定されます。これらの変換が作成されていることを確認するには、xlate（変換）テーブルをチェックします。コマンド **show xlate, local** キーワードおよび内部ホストの IP アドレスと組み合わせると、そのホストの変換テーブルにあるすべてのエントリを表示します。上記の出力は、内部インターフェイスと外部インターフェイスの間でこのホストに対して現在作成された変換があることを示しています。内部ホストの IP とポートは設定を通じて 10.165.200.226 アドレスに変換されます。

示されているフラグ **ri** は、変換がダイナミックであり、ポートマップであることを示しています。異なる NAT 設定の詳細は、『NAT に関する情報』を参照してください。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。