基本的な ASA NAT コンフィギュレーション：ASA バージョン 8.3 以降の DMZ での Web サーバ

目次

概要

この資料は方法の簡単で、簡単な例を送信、また受信接続を可能にするために ASA ファイアウォールのネットワーク アドレス変換（NAT）およびアクセス コントロール リスト（ACL）を設定する提供したものです。 この文書は実行 ASA コードバージョン 9.1(1) より（ASA） 5510 ファイアウォールと適応型セキュリティ アプライアンス（ASA）ソフトウェア書かれていました、これは他のどの ASA ファイアウォール プラットフォームにも容易に適用できます。 物理インターフェイスの代りに VLAN を使用する ASA 5505 のようなプラットフォームを使用する場合、適切ようにインターフェイスの種類を変更する必要があります。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

この 文書に記載されている 情報は ASA コードバージョン 9.1(1) を実行する ASA 5510 ファイアウォールに基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

概要

目標

この設定例では、どんな NAT および ACL構成を検知であって下さいでき内部および DMZ ホストからの送信接続を許可しますか ASA ファイアウォールの DMZ の Webサーバにインバウンドアクセスに与えるため必要。 これは、次の 2 つの目的に集約できます。

1. 内部および DMZ のホストに、インターネットへの発信接続を許可する。
2. インターネットのホストが 192.168.1.100 の IP アドレスの DMZ の Webサーバにアクセスするようにして下さい。

これら二つの目的を達成するために完了する必要があるステップへ到達する前にこの文書は ASA コード（バージョン 8.3 および それ 以降）の新しいバージョンの方法 ACL および NAT 作業に簡潔に行きます。

アクセス コントロール リストの概要

アクセス コントロール リスト（短縮してアクセス リストまたは ACL）は、ASA ファイアウォールがトラフィックを許可するか拒否するかを決定する方法です。 デフォルトで、**下部の**から**より高度のセキュリティレベル**に通じるトラフィックは拒否されます。 これは、低いセキュリティ インターフェイスに ACL を適用することで上書きできます。 また ASA は、デフォルトで、より**高く**から**より低いセキュリティインターフェイス**にトラフィックを可能にします。 この動作も ACL で上書きできます。

ASA コード（8.2 およびそれ以前）の以前のバージョンでは、ASA はインターフェイスの ACL に対してパケットを最初に untranslating 着信接続かパケットを比較しました。 つまり ACL では、インターフェイスでキャプチャした状態のパケットを許可する必要がありました。 バージョン 8.3 および それ 以降コードでは、インターフェイス ACL をチェックする前に ASA untranslates ことパケット。 つまり、8.3 以降のコード、そしてこのドキュメントでは、ホストの変換された IP ではなく、ホストの実際の IP へのトラフィックが許可されます。

アクセス コントロール リストの詳細については、「アクセス ルールの設定」の項（『ニュアル 2： Cisco ASA シリーズ ファイアウォール CLI コンフィギュレーション ガイド、ACL に関する詳細については 9.1。

NAT の概要

バージョン 8.3 および それ 以降の ASA の NAT は**オート NAT（オブジェクト NAT）**および**手動 NAT（二度 NAT）**として知られている 2 つのタイプに分けられます。 1 つめの **Object NAT** は、ネットワーク オブジェクトの定義の中で設定されます。 この例については、この後このドキュメントで説明します。 この NAT 方式の 1 つのプライマリ長所は ASA が競合を避ける処理のために自動的にルールを発注することです。 この方法は NAT の最も簡単な形式ですが、この簡明さに

よってコンフィギュレーションの詳細度は制限されます。 たとえば NAT の第 2 型とできたので、**手動 NAT** パケットの宛先に基づいて変換デシジョンを作ることができません。 **手動 NAT は**細かさで非常に堅牢ですが、修正挙動を実現できるように行が正しい順序で設定されることを必要とします。 これはこの NAT 型を複雑にし、その結果この設定例で使用されません。

NAT の詳細については、「 NAT について」の項 (『 ニュアル 2： Cisco ASA シリーズ ファイアウォール CLI コンフィギュレーション ガイド 9.1』) を参照してください。

設定

はじめに

基本的な ASA 設定のセットアップでは、3 つのネットワーク セグメントに接続された 3 つのインターフェイスがあります。 ISP ネットワーク セグメントは Ethernet0/0 インターフェイスに接続され、セキュリティ レベル 0 の **outside** のラベルが付けられます。 内部ネットワークは Ethernet0/1 に接続され、セキュリティ レベル 100 の **inside** のラベルが付けられます。 Webサーバが常駐する DMZ セグメントは Ethernet0/2 に接続され、50 のセキュリティレベルとの **DMZ** として分類されます。

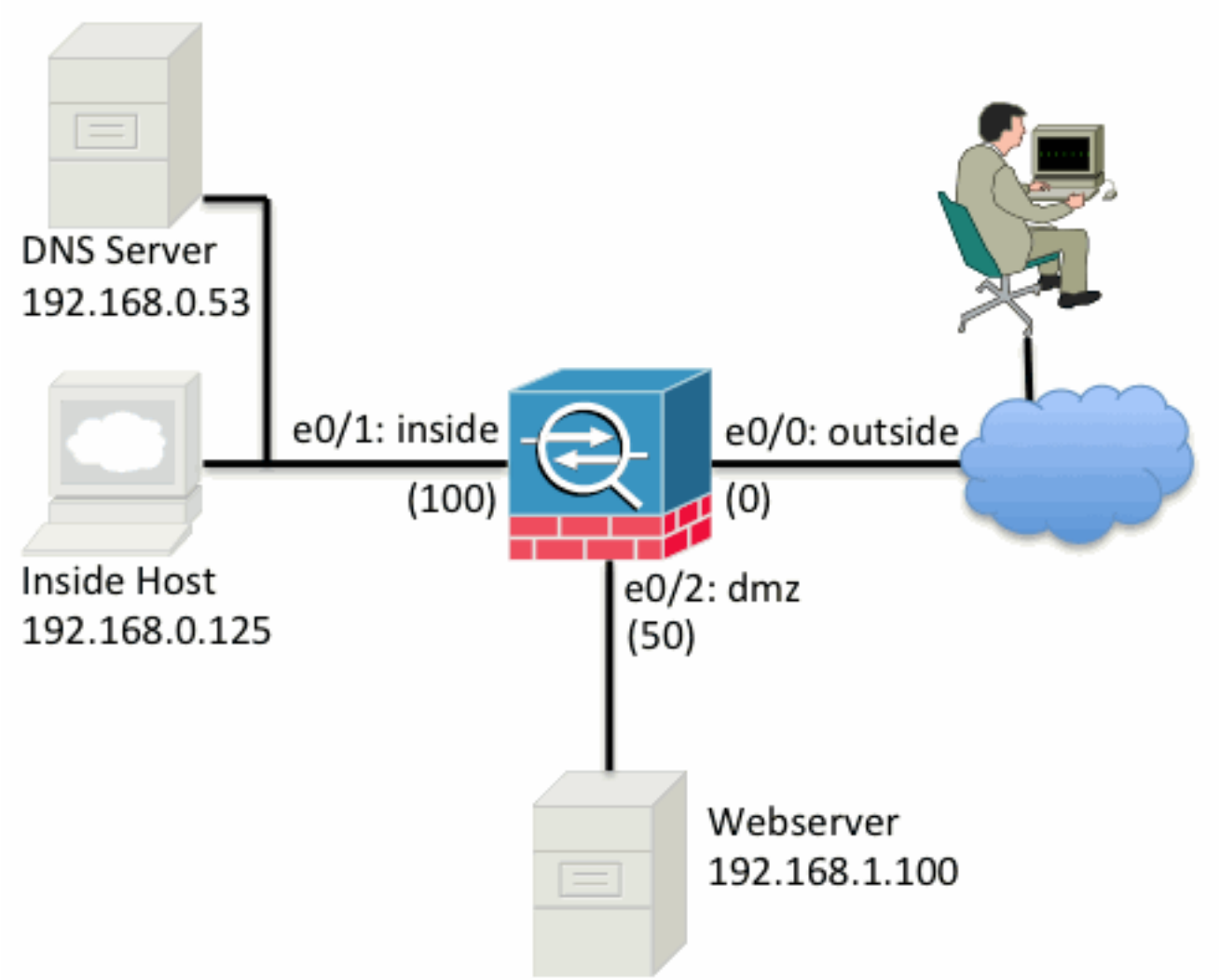
例のためのインターフェイスコンフィギュレーションおよび IP アドレスはここに参照されます:

```
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

ASA の **inside** インターフェイスは IP アドレスが 192.168.0.1 に設定されていることがわかります。これが内部ホストのデフォルト ゲートウェイです。 ASA の **outside** インターフェイスは ISP から入手した IP アドレスで設定されています。 ISP ゲートウェイのためにネクスト・ホップを設定するデフォルト・ルートがあります。 DHCP を使用する場合、これは自動的に提供されます。 **DMZ** インターフェイスは 192.168.1.1 の IP アドレスで設定され、それは DMZ ネットワーク セグメントのホストのためのデフォルト ゲートウェイです。

トポロジ

ケーブル接続と設定を次に図示します。



ステップ 1 -ホストがインターネットに出かけるように NAT を設定して下さい

この例では Object NAT、別名 AutoNAT を使用します。 最初に設定するのは、inside および dmz セグメント上のホストのインターネットへの接続を許可する NAT ルールです。 これらのホストが私用 IP アドレスを使用するので、インターネットでルーティング可能である何かにそれらを変換する必要があります。 この場合彼らが ASA の **outside インターフェイス** IP アドレスのように見えるように、アドレスを変換して下さい。 外部 IP が頻繁に変更すれば（DHCP が多分原因で）これはこれをセットする最も簡単な方法です。

この NAT を設定するには、inside サブネットを表すネットワーク オブジェクトと、dmz のサブネットを表すネットワーク オブジェクトを作成する必要があります。 これらのオブジェクトのそれぞれでは、個々のインターフェイスから **outside インターフェイス**にポート アドレス変換（PAT）これらのクライアントのでそれら通じる**ダイナミック NAT** ルールを設定して下さい。

このコンフィギュレーションは次のようになります。

```
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
nat (inside,outside) dynamic interface
!
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
nat (dmz,outside) dynamic interface
```

実行コンフィギュレーションを（**show run コマンド**の出力と）この時点で検知 すれば、オブジ

エクト 定義が出力の 2 部に分割されることがわかります。 最初の一部はそのオブジェクトに結ばれる第 2 セクションはことを NAT ルール示すがだけあるものがオブジェクト (ホスト/サブネット、IP アドレス、等) に示します。 前の出力の最初のエントリを奪取 すれば:

内部インターフェイスからの outside インターフェイスへの 192.168.0.0/24 サブネット横断を一致するホストが、動的に outside インターフェイスにそれらを変換したいと思う時。

ステップ 2 -インターネットから Webサーバにアクセスするために NAT を設定して下さい

内部および **DMZ** インターフェイスのホストがインターネットに出ることができるのでインターネットのユーザが TCPポート 80 の Webサーバにアクセスできるように設定を修正する必要があります。 この例では、設定はインターネットの個人が ISP が提供した別の IP アドレスに、*所有*する追加 IP アドレス接続できるようにあります。 この例では 198.51.100.101 を使用します。 この設定によって、インターネットのユーザは TCPポート 80 の 198.51.100.101 にアクセスして **DMZ** Webサーバに達できます。 このタスクの実行に**オブジェクト NAT を**使用すれば、ASA は Webサーバの TCPポート 80 を変換します (192.168.1.100) **外部**の TCPポート 80 の 198.51.100.101 のように見えるため。 同様に以前にされ、オブジェクトを定義し、そのオブジェクトのためのトランスレーション ルールを定義することがに。 また、このホストをに変換する IP を表すために第 2 オブジェクトを定義して下さい。

このコンフィギュレーションは次のようになります。

```
object network webserver-external-ip
host 198.51.100.101
!
object network webserver
host 192.168.1.100
nat (dmz,outside) static webserver-external-ip service tcp www www
```

この例の NAT ルールの内容をまとめると次のようになります。

DMZ セグメントの IP アドレス 192.168.1.100 と一致する接続によってが outside インターフェイス出かけ、ホストが TCPポート 80 (www) からソースをたどられる接続を確立する時、outside インターフェイスの TCPポート 80 (www) であるためにおよび 198.51.100.101 であるためにその IP アドレスを変換するようにそれを変換したいと思う。

これは多少奇妙に思えます。「TCP ポート 80 (www) を送信元とする」とありますが、Web トラフィックはポート 80 を*宛先にします*。 これらの NAT ルールがその性質に双方向であることを理解しておくことは重要です。 その結果、この文を言い直すために言葉遣いを移行できます。 変換した結果はより理解しやすくなります。

外部のホストが宛先TCP ポート 80 (www) の 198.51.100.101 への接続を確立する場合、192.168.1.100 であるために宛先 IP アドレスを変換し、宛先ポートは TCPポート 80 (www) で、それを DMZ 送信 します。

このように表現した方がより理解しやすくなります。 次に ACL を設定する必要があります。

ステップ 3 : ACL を設定する

NAT が設定され、今回のコンフィギュレーションの終了に近づきました。 ASA の ACL によって次のようなデフォルトのセキュリティ動作を上書きできることを思い出してください。

- **より低いセキュリティインターフェイス**から行くトラフィックは**より高セキュリティのインターフェイス**に行くとき**拒否されます**。
- **より高セキュリティのインターフェイス**から行くトラフィックは**より低いセキュリティインターフェイス**に行くとき**許可されます**。

従って設定への ACL の付加なしで、例のこのトラフィックははたらきます:

- **内部**のホスト（セキュリティレベルは **DMZ**（50）セキュリティレベルのホストに 100）接続できます。
- **内部**のホスト（セキュリティレベルは**外部**（0）セキュリティレベルのホストに 100）接続できます。
- **DMZ** のホスト（セキュリティレベルは**外部**（0）セキュリティレベルのホストに 50）接続できます。

ただし、このトラフィックは拒否されます:

- **外部**のホスト（セキュリティレベルは**内部**（100）セキュリティレベルのホストに 0）接続できません。
- **外部**のホスト（セキュリティレベルは **DMZ**（50）セキュリティレベルのホストに 0）接続できません。
- **DMZ** のホスト（セキュリティレベルは**内部**（100）セキュリティレベルのホストに 50）接続できません。

外部からの **DMZ** ネットワークへのトラフィックが現在のコンフィギュレーションを用いる ASA によって拒否されるので、インターネットのユーザはステップ 2.の NAT 設定にもかかわらず Webサーバに達することができません。 このトラフィックを明示的に許可する必要があります。 8.3 以降のコードでは、**変換された IP** ではなくホストの**実際の IP** を ACL で使用する必要があります。 つまり、コンフィギュレーションでは、宛先が 198.51.100.101 のポート 80 のトラフィック**ではなく**、宛先が 192.168.1.100 のトラフィックを許可する必要があります。 For simplicity の為はこの ACL のために、ステップ 2 で定義されたオブジェクト同様に使用されます。 ACL を作成したら、それを外側のインターフェイスの着信に適用する必要があります。

これらのコンフィギュレーション コマンドは次のようになります。

```
access-list outside_acl extended permit tcp any object webserver eq www
!
access-group outside_acl in interface outside
```

この access-list 行は次を意味します。

any（where）からのオブジェクト Webサーバによって表されるホストへの割り当てトラフィック（192.168.1.100）ポート 80 で。

ここで **any** キーワードを使用することが重要です。 クライアントのソース IP アドレスがそれとして達する Webサイトに知られないので、意味を「あらゆる IP アドレス」規定 して下さい。

dmz セグメントから **inside ネットワーク** セグメントのホスト宛のトラフィックについてはどうすればよいでしょうか。 たとえば、**内部ネットワーク**のサーバ接続する **DMZ** 必要のホスト。 ASA が **dmz** から **inside** サーバ宛の特定のトラフィックのみを許可し、それ以外は **inside** セグメント宛のトラフィックをすべてブロックするにはどうすればよいでしょうか。

この例では、inside ネットワークに IP アドレス 192.168.0.53 の DNS サーバがあり、DNS 解決のために **dmz** 上のホストがこのサーバにアクセスする必要があると仮定します。 必要とされる ACL を作成し、**DMZ** インターフェイスに適用します従って ASA はそのインターフェイスに入る

トラフィックのために、上記されるその既定のセキュリティ動作を無効にすることができます。

これらのコンフィギュレーション コマンドは次のようになります。

```
object network dns-server
host 192.168.0.53
!
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
access-group dmz_acl in interface dmz
```

ACL はで UDP ポート 53 の DNSサーバにそのトラフィックを単に許可しますより複雑。 最初の 'permit' 行だけにした場合、**dmz** からインターネット上のホストへのすべてのトラフィックはブロックされます。 ACL に ACL の終わりに暗示「deny ip any any」があります。 この結果、**dmz** のホストはインターネットにアクセスすることができなくなります。 **DMZ** からの**外部**へのトラフィックがデフォルトで許可されるのに **DMZ** インターフェイスへの ACL のアプリケーションと、**DMZ** インターフェイスのためのそれらの既定のセキュリティ動作は事実上もはやないし、割り当てインターフェイス ACL のトラフィック明示的になります。

ステップ 4 -パケット トレーサー機能との設定をテストして下さい

設定が完了するので、確かめるためにそれをテストする必要がありますはたらくことを。 最も簡単な方法は実際のホストを使用することです (自分が所有するネットワークの場合)。 ただし、CLI からこれをテストすることのためにおよびそれ以上いくつかの ASA のツールを探索して、直面する問題をテストし、可能性としてはデバッグするためにパケット トレーサーを使用して下さい。

パケット トレーサーは一連のパラメータに基づいてパケットの模倣によってはたらき、そのパケットをネットワークを離れて取られた場合実際パケットが方法と同じようなインターフェイス データパスにインジェクトします。 このパケットは実行されるプロセスおよびチェックの無数によってファイアウォールを通り、パケットがトレーサー結果に注意すると同時に続かれます。 インターネット上のホストに送信しようとしている内部ホストのシミュレーションを行います。 次のコマンドはファイアウォールに次の内容を指示します。

*ポート **80** の **203.0.113.1** の IP アドレスに向かう送信元ポート **12345** の IP アドレス **192.168.0.125** から**内部インターフェイス**入って来 **TCP**パケットを**模倣**して下さい。*

```
ciscoasa# packet-tracer input inside tcp 192.168.0.125 12345 203.0.113.1 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config: Additional Information:
```

```
in 0.0.0.0 0.0.0.0 outside Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network inside-subnet
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1, packet dispatched to next module

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

最終結果は、すべての NAT および ACL にチェックインし、設定を送信された出力 インターフェイス渡した whichmeans、トラフィックが**許可される**こと**外部で**です。 パケットはフェーズ 3 で変換されており、ヒットしたルールがこのフェーズの詳細に表示されていることに注目してください。 ホスト 192.168.0.125 はコンフィギュレーションに従って動的に 198.51.100.100 に変換されています。

この場合、インターネットから Webサーバへの接続のためにそれを実行して下さい。 、インターネットのホスト アクセスします **outside インターフェイス**の 198.51.100.101 に接続によって

Webサーバに覚えていて下さい。 このコマンドは次のように翻訳できます。

ポート 80 の 198.51.100.101 の IP アドレスに向かう送信元ポート 12345 の IP アドレス 192.0.2.123 から outside インターフェイス入って来 TCPパケットを模倣して下さい。

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
```

```
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

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

再度、結果はパケットが許可されることです。 ACL は、設定外観うまくチェックし、インターネットのユーザは（**外部で**）外部 IP のその Webサーバにアクセスできるはずです。

確認

確認 手順はステップ 4 に含まれています-パケット トレーサー機能との設定のテスト。

トラブルシューティング

現在のところ、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。

結論

基本的な NAT を行う ASA のコンフィギュレーションはそれほど大変な作業ではありません。 この資料の例は特定のシナリオに設定例で使用される IP アドレスおよびポートを変更する場合適応させることができます。 コンフィギュレーションをまとめると、この例の最終的な ASA の設定は、ASA 5510 に対しては次のようになります。

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
```

```
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

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

以前に示されている接続されてインターフェイスが ASA 5505、たとえば、（Ethernet0/1 および Ethernet0/2 に接続される **DMZ** に接続される**の中の** Ethernet0/0 に、接続される**外部**）：

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
```

```
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

Result:
input-interface: outside
```

```
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```