



## 静的 NAT 変換の構成

- [ネットワーク アドレス変換の概要 \(1 ページ\)](#)
- [スタティック NAT に関する情報 \(1 ページ\)](#)
- [NAT の内部アドレスおよび外部アドレス \(3 ページ\)](#)
- [スタティック NAT の注意事項および制約事項 \(4 ページ\)](#)
- [スタティック NAT の設定 \(5 ページ\)](#)

## ネットワーク アドレス変換の概要

ネットワークアドレス変換 (NAT) は、登録されていない IP アドレスを使用してインターネットへ接続するプライベート IP インターネットワークをイネーブルにします。NAT はデバイス (通常、2 つのネットワークを接続するもの) で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの (グローバルに一意のアドレスではなく) プライベート IP アドレスを正規の IP アドレスに変換します。NAT は、ネットワーク全体に対して 1 つの IP アドレスだけを外部にアドバタイズするように設定できます。この機能により、1 つの IP アドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT が設定されたデバイスには、内部ネットワークと外部ネットワークのそれぞれに接続するインターフェイスが少なくとも 1 つずつあります。標準的な環境では、NAT はスタブドメインとバックボーンの間の出ルータに設定されます。パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元アドレスをグローバルに一意のアドレスに変換します。パケットがドメインに入ってくる際は、NAT はグローバルに一意な宛先アドレスをローカルアドレスに変換します。出口点が複数存在する場合、個々の NAT は同じ変換テーブルを持っている必要があります。

NAT は RFC 1631 に記述されています。

## スタティック NAT に関する情報

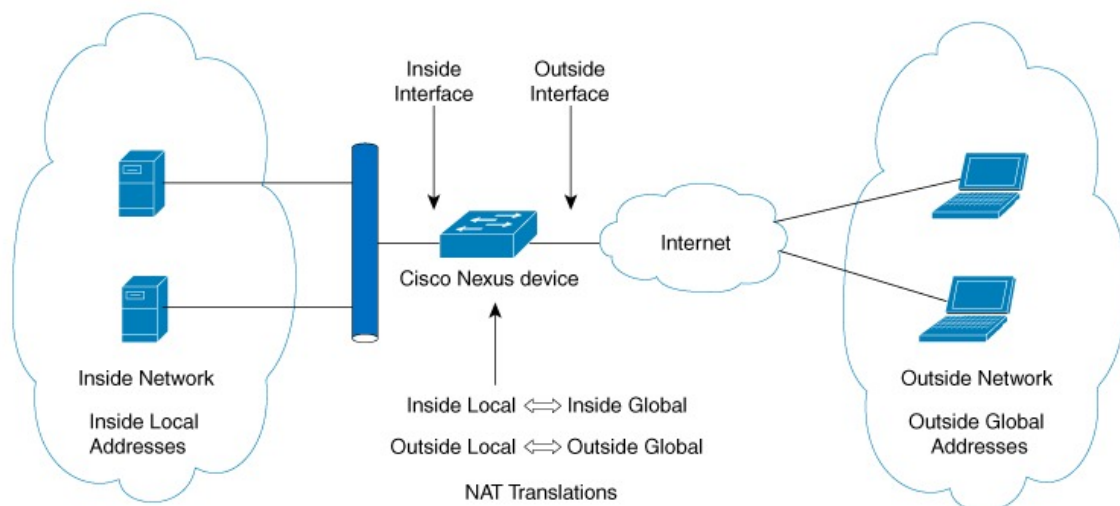
スタティック ネットワーク アドレス変換 (NAT) を使用すると、ユーザは内部ローカルアドレスから外部グローバルアドレスへの 1 対 1 変換を設定することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両

方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 構成で NAT 変換を追加または削除できることを意味します。

スタティック NAT では、プライベートアドレスからパブリックアドレスへの固定変換が作成されます。スタティック NAT では 1 対 1 ベースでアドレスが割り当てられるため、プライベートアドレスと同じ数のパブリックアドレスが必要です。スタティック NAT では、パブリックアドレスは連続する各接続で同じであり、永続的な変換規則が存在するため、宛先ネットワークのホストは変換済みのホストへのトラフィックを開始できます（そのトラフィックを許可するアクセスリストがある場合）。

次の図に、一般的なスタティック NAT のシナリオを示します。変換は常にアクティブであるため、変換対象ホストとリモートホストの両方で接続を生成でき、マップアドレスは **static** コマンドによって静的に割り当てられます。

図 1:スタティック NAT



次に、スタティック NAT を理解するのに役立つ主な用語を示します。

- NAT の内部インターフェイス：プライベートネットワークに面するレイヤ3インターフェイス。
- NAT の外部インターフェイス：パブリック ネットワークに面するレイヤ3インターフェイス。
- ローカルアドレス：ネットワークの内部（プライベート）部分に表示される任意のアドレス。
- グローバルアドレス：ネットワークの外部（パブリック）部分に表示される任意のアドレス。
- 正規の IP アドレス：Network Information Center (NIC) やサービス プロバイダーにより割り当てられたアドレス。

- 内部ローカルアドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは正規の IP アドレスである必要はありません。
- 外部ローカルアドレス：内部ネットワークから見た外部ホストの IP アドレス。これは、内部ネットワークのルーティング可能なアドレス空間から割り当てられるため、正規のアドレスである必要はありません。
- 内部グローバルアドレス：1つ以上の内部ローカル IP アドレスを外部に対して表すために使用できる正規の IP アドレス。
- 外部グローバルアドレス：ホスト所有者が外部ネットワーク上のホストに割り当てる IP アドレス。このアドレスは、ルート可能なアドレスまたはネットワーク空間から割り当てられた正規のアドレスです。

## NAT の内部アドレスおよび外部アドレス

NAT 内部とは、変換を必要とする組織が所有するネットワークを指します。NAT が設定されている場合、このネットワーク内のホストは、別の空間（グローバルアドレス空間として知られている）にあるものとしてネットワークの外側に現れる1つ空間（ローカルアドレス空間として知られている）内のアドレスを持つことになります。

同様に、NAT 外部とは、スタブ ネットワークが接続するネットワークを指します。通常、組織の管理下にはありません。外部ネットワーク内のホストを変換の対象にすることもできるため、これらのホストもローカルアドレスとグローバルアドレスを持つことができます。

NAT では、次の定義が使用されます。

- ローカルアドレス：ネットワークの内側部分に表示されるローカルな IP アドレスです。
- グローバルアドレス：ネットワークの外側部分に表示されるグローバルな IP アドレスです。
- 内部ローカルアドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは、多くの場合、インターネット ネットワーク 情報センター（InterNIC）やサービス プロバイダーにより割り当てられた正規の IP アドレスではありません。
- 内部グローバルアドレス：外部に向けて、1つ以上の内部ローカル IP アドレスを表現した正規の IP アドレス（InterNIC またはサービス プロバイダーにより割り当てられたもの）。
- 外部ローカルアドレス：内部ネットワークから見た外部ホストの IP アドレス。必ずしも正規のアドレスではありません。内部でルート可能なアドレス空間から割り当てられたものです。
- 外部グローバルアドレス：外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられたものです。

## スタティック NAT の注意事項および制約事項

スタティック NAT 設定時の注意事項および制約事項は、次のとおりです。

- キーワードが付いている **show** コマンド **internal** はサポートされていません。
- 変換された IP が、外部インターフェイス サブネットの一部である場合、NAT の外部インターフェイスで **ip proxy-arp** コマンドを使用します。 **add-route** キーワードを使用する場合は、 **ip proxy-arp** を有効にする必要があります。
- Cisco Nexus デバイスは、次のインターフェイスタイプで NAT をサポートします。
  - ルーテッド ポート
- NAT はデフォルトの仮想ルーティングおよびフォワーディング (VRF) テーブルのみでサポートされます。
- NAT は、IPv4 ユニキャストだけでサポートされています。
- Cisco Nexus デバイスは次をサポートしていません。
  - ソフトウェアの変換。すべての変換はハードウェアで行われます。
  - NAT ルーティング
  - アプリケーション層の変換。レイヤ 4 およびその他の組み込み IP は変換されません (FTP、ICMP の障害、IPSec、HTTPS など)。
  - インターフェイス上で同時に設定された NAT および VLAN アクセス コントロール リスト (VACL)。
  - フラグメント化された IP パケットの PAT 変換。
  - ソフトウェア転送パケットの NAT 変換。たとえば、IP オプションを持つパケットは NAT 変換されません。
- IP アドレスがスタティック NAT 変換または PAT 変換に使用される場合、他の目的には使用できません。たとえば、インターフェイスに割り当ててはできません。
- スタティック NAT の場合は、外部グローバル IP アドレスが外部インターフェイス IP アドレスと異なる必要があります。
- (100 を超える) 多数の変換を設定する場合、変換を設定してから NAT インターフェイスを設定する方が迅速に設定できます。
- ECMP NAT は Cisco Nexus® 3550-T スイッチではサポートされません。

# スタティック NAT の設定

## スタティック NAT のイネーブル化

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>feature nat</b>	デバイス上でスタティック NAT 機能をイネーブルにします。
ステップ 3	switch(config)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## インターフェイスでのスタティック NAT の設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>interface type slot/port</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# <b>ip nat {inside   outside}</b>	内部または外部としてインターフェイスを指定します。  (注) マーク付きインターフェイスに到着したパケットだけが変換できます。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次に、スタティック NAT を使用して内部のインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# ip nat inside
```

## 内部送信元アドレスのスタティック NAT のイネーブル化

内部送信元変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。NAT は、内部ローカル IP アドレスを内部グローバル IP アドレスに変換します。リターントラフィックでは、宛先の内部グローバル IP アドレスが内部ローカル IP アドレスに変換されて戻されます。



- (注) が、内部送信元 IP アドレス (Src:ip1) を外部送信元 IP アドレス (newSrc:ip2) に変換するように設定されている場合、は内部宛先 IP アドレス (newDst: ip1) への外部宛先 IP アドレス (Dst: ip2) の変換をCisco Nexus デバイス暗黙的に追加します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>ip nat inside source static local-ip-address global-ip-address [group group-id ]</b>	内部グローバルアドレスを内部ローカルアドレスに、またはその逆に (内部ローカルトラフィックを内部ローカル (local) トラフィックに) 変換するようにスタティック NAT を設定します。 <b>group</b> を指定することにより、スタティック Twice NAT でこの変換が属するグループが指定されます。
ステップ 3	(任意) switch(config)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次に、内部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.1 5.5.5.5
switch(config)# copy running-config startup-config
```

## 外部送信元アドレスのスタティック NAT のイネーブル化

外部送信元変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。NAT は、外部グローバル IP アドレスを外部ローカル IP アドレスに変換します。リターントラフィックでは、宛先の外部ローカル IP アドレスが外部グローバル IP アドレスに変換されて戻されます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>ip nat outside source static</b> <i>outsideGlobalIP outsideLocalIP</i> <b>[dynamic]</b> <b>[add-route]</b>	外部グローバル アドレスを外部ローカル アドレスに、またはその逆に（外部ローカルトラフィックを外部グローバルトラフィックに）変換するようにスタティック NAT を設定します。ポートなしで内部変換が設定されると、暗黙的な追加ルートが実行されます。外部変換の設定中、最初の追加ルート機能はオプションです。
ステップ 3	(任意) switch(config)# <b>copy</b> <b>running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次に、外部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static 2.2.2.2 6.6.6.6
switch(config)# copy running-config startup-config
```

## 内部送信元アドレスのスタティック PAT の設定

ポートアドレス変換 (PAT) を使用して、特定の内部ホストにサービスをマッピングできます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>ip nat inside source static</b> { <i>inside-local-address</i> <i>inside-global-address</i>   { <b>tcp</b>   <b>udp</b> } <i>inside-local-address</i> { <i>local-tcp-port</i>   <i>local-udp-port</i> } <i>inside-global-address</i> { <i>global-tcp-port</i>   <i>global-udp-port</i> }}	スタティック NAT を内部ローカル ポート、内部グローバル ポートにマッピングします。
ステップ 3	(任意) switch(config)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

### 例

次に、UDP サービスを特定の内部送信元アドレスおよび UDP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static udp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

## 外部送信元アドレスのスタティック PAT の設定

ポートアドレス変換 (PAT) を使用して、サービスを特定の外部ホストにマッピングできます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>ip nat outside source static</b> { <i>outside-global-address</i> <i>outside-local-address</i>   { <b>tcp</b>   <b>udp</b> } <i>outside-global-address</i> { <i>global-tcp-port</i>	スタティック NAT を、外部グローバル ポート、外部ローカル ポートにマッピングします。



	コマンドまたはアクション	目的
	<code>global-udp-port} outside-local-address {global-tcp-port   global-udp-port}} {add-route}</code>	
ステップ 3	(任意) <code>switch(config)# copy running-config startup-config</code>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

### 例

次に、TCP サービスを特定の外部送信元アドレスおよび TCP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static tcp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

## no-alias 設定の有効化と無効化

NAT デバイスは内部グローバル (IG) アドレスと外部ローカル (OL) アドレスを所有し、これらのアドレス宛での ARP 要求に応答します。IG/OL アドレス サブネットがローカルインターフェイス サブネットと一致すると、NAT は IP エイリアスと ARP エントリをインストールします。この場合、デバイスは local-proxy-arp を使用して ARP 要求に応答します。

`no-alias` 機能は、アドレス範囲が外部インターフェイスの同じサブネットにある場合、特定の NAT プールアドレス範囲からのすべての変換された IP の ARP 要求に応答します。

NAT が設定されたインターフェイスで `no-alias` が有効になっている場合、外部インターフェイスはサブネット内の ARP 要求に応答しません。`no-alias` を無効にすると、外部インターフェイスと同じサブネット内の IP に対する ARP 要求が処理されます。



(注) この機能をサポートしていない古いリリースにダウングレードすると、`no-alias` オプションの設定が削除されることがあります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>switch(config)# feature nat</code>	デバイス上でスタティック NAT 機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# <b>show run nat</b>	NAT の設定を表示します。
ステップ 4	switch(config)# <b>show ip nat-alias</b>	エイリアスが作成されたかどうかの情報を表示します。  (注) デフォルトでは、エイリアスが作成されます。エイリアスを無効にするには、 <i>no-alias</i> キーワードをコマンドに追加する必要があります。
ステップ 5	switch(config)# <b>clear ip nat-alias ip address/all</b>	エイリアス リストからエントリを削除します。特定のエントリを削除するには、削除する IP アドレスを指定する必要があります。すべてのエントリを削除するには、すべてのキーワードを使用します。

## 例

次に、すべてのインターフェイスの情報を表示する例を示します。

```
switch# configure terminal
switch(config)# show ip int b
IP Interface Status for VRF "default"(1)
Interface          IP Address      Interface Status
Lo0                 100.1.1.1      protocol-up/link-up/admin-up
Eth1/1             7.7.7.1        protocol-up/link-up/admin-up
Eth1/3             8.8.8.1        protocol-up/link-up/admin-up
```

次に、実行コンフィギュレーションの例を示します。

```
switch# configure terminal
switch(config)# show running-config nat
!Command: show running-config nat
!Running configuration last done at: Thu Aug 23 11:57:01 2018
!Time: Thu Aug 23 11:58:13 2018

version 9.2(2) Bios:version 07.64
feature nat
interface Ethernet1/1
 ip nat inside
interface Ethernet1/3
 ip nat outside
switch(config)#
```

この例は、エイリアスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool p1 7.7.7.2 7.7.7.20 prefix-length 24
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3
switch(config)# show ip nat-alias
Alias Information for Context: default
```

```

Address      Interface
7.7.7.2      Ethernet1/1
8.8.8.2      Ethernet1/3
switch(config)#

```

次に、`show ip nat-alias` の出力例を示します。デフォルトでは、エイリアスが作成されます。

```

switch# configure terminal
switch(config)# show ip nat-alias
Alias Information for Context: default
Address      Interface
7.7.7.2      Ethernet1/1
8.8.8.2      Ethernet1/3
switch(config)#

```

この例は、エイリアスを無効にする方法を示します。

```

switch# configure terminal
switch(config)# ip nat pool p1 7.7.7.2 7.7.7.20 prefix-length 24 no-alias
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3 no-alias
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3 no-alias
switch(config)# show ip nat-alias
Alias Information for Context: default
Address      Interface
7.7.7.2      Ethernet1/1
8.8.8.2      Ethernet1/3
switch(config)#

```

```

** None of the entry got appended as alias is disabled for above CLIs.
switch(config)#

```

この例は、エイリアスをクリアする方法を示します。エイリアスリストからエントリを削除するには、`clear ip nat-alias` を使用します。IP アドレスを指定して 1 つのエントリを削除することも、すべてのエイリアス エントリを削除することもできます。

```

switch# configure terminal
switch(config)# clear ip nat-alias address 7.7.7.2
switch(config)# show ip nat-alias
Alias Information for Context: default
Address      Interface
8.8.8.2      Ethernet1/3
switch(config)#
switch(config)# clear ip nat-alias all
switch(config)# show ip nat-alias
switch(config)#

```

## スタティック NAT および PAT の設定例

次に、スタティック NAT の設定例を示します。

```

ip nat inside source static 103.1.1.1 11.3.1.1
ip nat inside source static 139.1.1.1 11.39.1.1
ip nat inside source static 141.1.1.1 11.41.1.1
ip nat inside source static 149.1.1.1 95.1.1.1
ip nat inside source static 149.2.1.1 96.1.1.1
ip nat outside source static 95.3.1.1 95.4.1.1
ip nat outside source static 96.3.1.1 96.4.1.1
ip nat outside source static 102.1.2.1 51.1.2.1

```

```
ip nat outside source static 104.1.1.1 51.3.1.1
ip nat outside source static 140.1.1.1 51.40.1.1
```

次に、スタティック PAT の設定例を示します。

```
ip nat inside source static tcp 10.11.1.1 1 210.11.1.1 101
ip nat inside source static tcp 10.11.1.1 2 210.11.1.1 201
ip nat inside source static tcp 10.11.1.1 3 210.11.1.1 301
ip nat inside source static tcp 10.11.1.1 4 210.11.1.1 401
ip nat inside source static tcp 10.11.1.1 5 210.11.1.1 501
ip nat inside source static tcp 10.11.1.1 6 210.11.1.1 601
ip nat inside source static tcp 10.11.1.1 7 210.11.1.1 701
ip nat inside source static tcp 10.11.1.1 8 210.11.1.1 801
ip nat inside source static tcp 10.11.1.1 9 210.11.1.1 901
ip nat inside source static tcp 10.11.1.1 10 210.11.1.1 1001
ip nat inside source static tcp 10.11.1.1 11 210.11.1.1 1101
ip nat inside source static tcp 10.11.1.1 12 210.11.1.1 1201
```

## スタティック NAT の設定の確認

スタティック NAT の設定を表示するには、次の作業を行います。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>show ip nat translations</b>	内部グローバル、内部ローカル、外部ローカル、および外部グローバルの各 IP アドレスを示します。

### 例

次に、スタティック NAT の設定を表示する例を示します。

```
switch# sh ip nat translations
Pro Inside global      Inside local      Outside local     Outside global
--- ---
--- ---                ---              51.3.1.1          104.1.1.1
--- ---                ---              95.4.1.1          95.3.1.1
--- ---                ---              96.4.1.1          96.3.1.1
--- ---                ---              51.40.1.1         140.1.1.1
--- ---                ---              51.42.1.1         142.1.2.1
--- ---                ---              51.1.2.1          102.1.2.1
--- 11.1.1.1           101.1.1.1        ---
--- 11.3.1.1           103.1.1.1        ---
--- 11.39.1.1          139.1.1.1        ---
--- 11.41.1.1          141.1.1.1        ---
--- 95.1.1.1           149.1.1.1        ---
--- 96.1.1.1           149.2.1.1        ---
--- 130.1.1.1:590      30.1.1.100:5000  ---
--- 130.2.1.1:590      30.2.1.100:5000  ---
--- 130.3.1.1:590      30.3.1.100:5000  ---
--- 130.4.1.1:590      30.4.1.100:5000  ---
--- 130.1.1.1:591      30.1.1.101:5000  ---
```

```
switch# sh ip nat translations verbose
Pro Inside global      Inside local      Outside local      Outside global
any ---                ---                22.1.1.3           22.1.1.2
  Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.130         11.1.1.3         ---                ---
  Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:0
any 11.1.1.133         11.1.1.33       ---                ---
  Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.133         11.1.1.33       22.1.1.3           22.1.1.2
  Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:0
tcp 10.1.1.100:64490   10.1.1.2:0       20.1.1.2:0         20.1.1.2:0
  Flags:0x82 time-left(secs):43192 id:31 state:0x3 grp_id:0 vrf: default
N3550T-1#
```



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。