ITD の設定

この章では、Cisco NX-OS デバイスで Intelligent Traffic Director（ITD）を設定する方法について説明します。

ITD について

Intelligent Traffic Director（ITD）は、ハードウェアベースのインテリジェントなテラビット規模のソリューションです。レイヤ 3 およびレイヤ 4 のトラフィック分散、ロード バランシング、およびリダイレクション用のスケーラブルなアーキテクチャを構築できます。

ITD の利点

- ライン レートがマルチテラビット規模のソリューション
- エンド デバイスに対する透過性とステートレス プロトコルの利点
- 低減された複雑性と Web Cache Communication Protocol（WCCP）やポリシーベース ルーティングなどの代替機能に対するアーキテクチャの拡張性
- 簡素化されたプロビジョニングおよび容易な展開

- レガシー サービス アプライアンスと新しいサービス アプライアンスの共存が可能
- 高価な外部ロード バランサが不要

ITD の特徴

- スイッチ上のすべてのポートをロード バランシングとトラフィック リダイレクションに使用
- 同時リダイレクションおよびロード バランシング
- 中断のないノードの追加または削除
- 双方向フローの一貫性（たとえば A から B へのトラフィックと B から A へのトラフィックは同じサービス ノードに送信されます）
- IP スティッキ性の復元力（復元力の高い ECMP など）
- IP SLA ベースのプローブを使用したサーバおよびアプライアンスのヘルス モニタリング
- サーバまたはアプライアンスの自動障害処理
- VRF および vPC のサポート
- 重み付けベースのロード バランシング
- 同じスイッチ上の複数の ITD サービス間でのレート共有

使用例

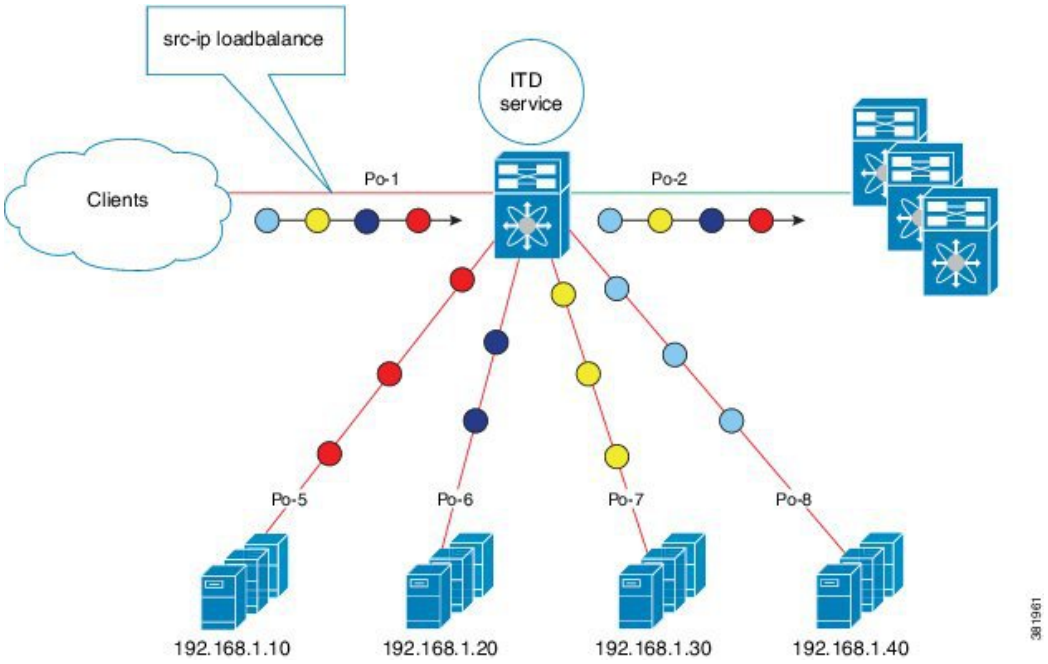
- ファイアウォール プールへのロード バランス
- Wide Area Application Services（WAAS）または Web アクセラレータ エンジン（WAE）ソリューションのトラフィック リダイレクション メカニズム
- DSR モードでのサーバ ロード バランシング
- スタンドアロン デバイスへのロード バランシングによる NG 侵入防御システム（IPS）および Web アプリケーション ファイアウォール（WAF）の拡張
- VDS-TC（ビデオキャッシュ）ソリューションの拡大
- 再ハッシュの回避を目的とした ECMP またはポートチャネルの置き換え
- レイヤ 7 ロード バランサを介したレイヤ 5 へのロード バランス

展開モード

ワンアーム展開モード

サーバをワンアーム展開モードでスイッチに接続できます。このトポロジでは、サーバはクライアントトラフィックまたはサーバトラフィックの直接パスに存在しないため、既存のトポロジやネットワークを変更することなく、サーバをネットワークに接続できます。

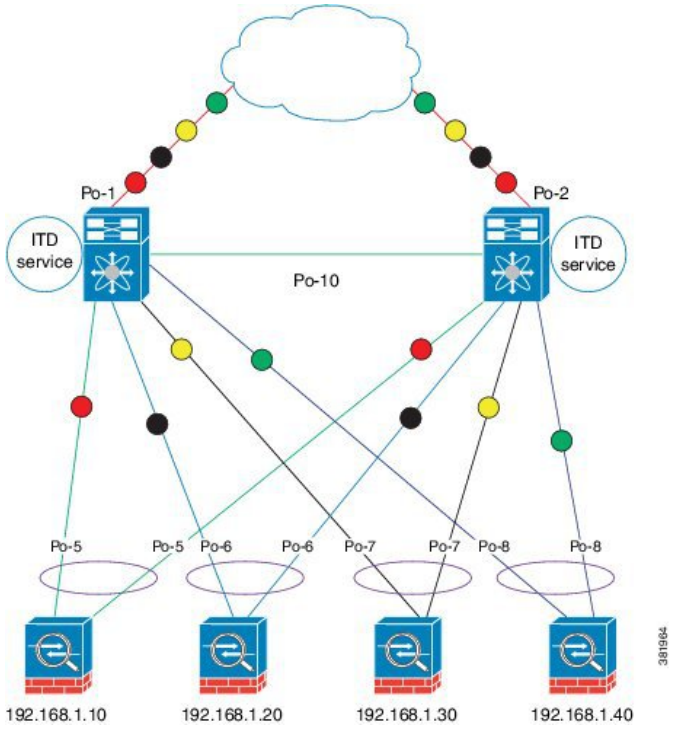
図 *1*：ワンアーム展開モード



vPC でのワンアーム展開モード

ITD は仮想ポート チャネル（vPC）に接続されたアプライアンス プールをサポートします。ITD サービスは各スイッチで実行されます。ITD は、フローがノードを通過する一貫したトラフィックを得られるように各スイッチをプログラムします。

図 *2*：*vPC* でのワンアーム展開モード



サンドイッチ展開モード

サンドイッチ展開モードでは、2 台のスイッチを使用してトラフィックをステートフルに処理します。

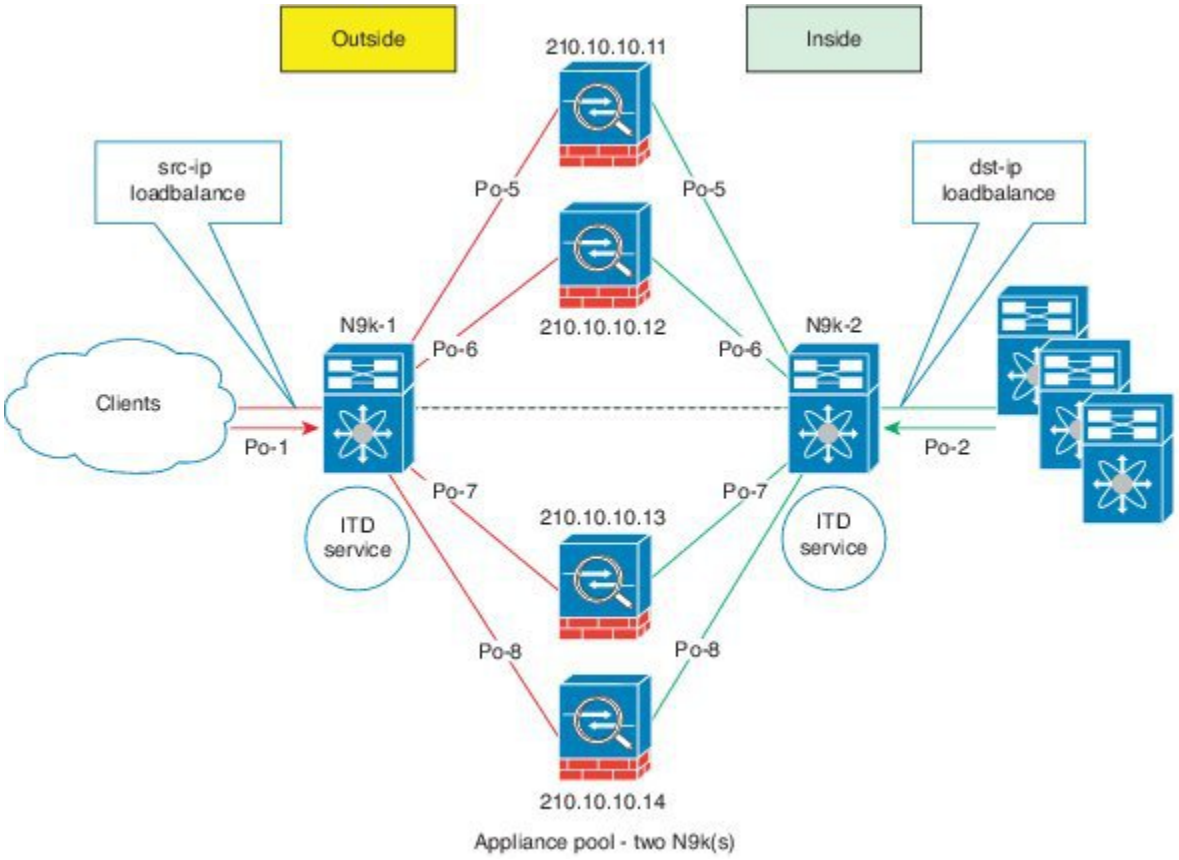
このモードの主な要件は、フローのフォワード トラフィックとリバース トラフィックの両方が同じアプライアンスを通過しなければならないことです。サンドイッチ展開の例としては、クライアントとサーバ間のトラフィックが同じアプライアンスを通過する必要があるファイアウォールおよびロード バランサの展開があります。

主な機能は次のとおりです。

- ネットワーク セグメントごとの ITD サービス（外部ネットワーク用に 1 つの ITD サービスおよび内部ネットワーク用にもう 1 つの ITD サービス）。
- 送信元 IP アドレスのロードバランシング スキーム（ITD サービスは外部に接続する入力方向のインターフェイス上で動作します）。

- 宛先 IP アドレスのロードバランシング スキーム（ITD サービスはサーバに接続する入力方向のインターフェイス上で動作します）。

図 *3*：サンドイッチ展開モード

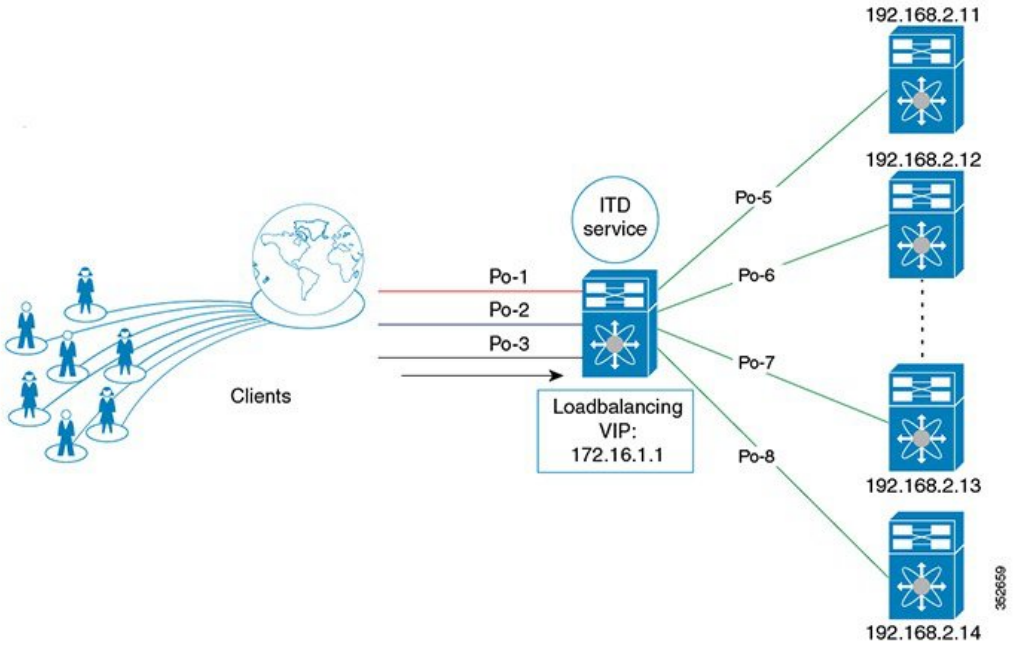


サーバ ロード バランシング展開モード

ITD サービスは、スイッチ上の仮想 IP（VIP）をホストするように設定できます。VIP を宛先とするインターネット トラフィックの負荷は、アクティブ ノードに分散されます。ITD サービスはステートフル ロード バランサではありません。

（注） ITD サービスを各スイッチで同様に手動で設定する必要があります。

図 *4* : *VIP* を使用した *ITD* 負荷分散



デバイス グループ

ITD はデバイス グループをサポートしています。デバイス グループを設定する際に、次を指定できます。

- デバイス グループのノード
- デバイス グループのプローブ

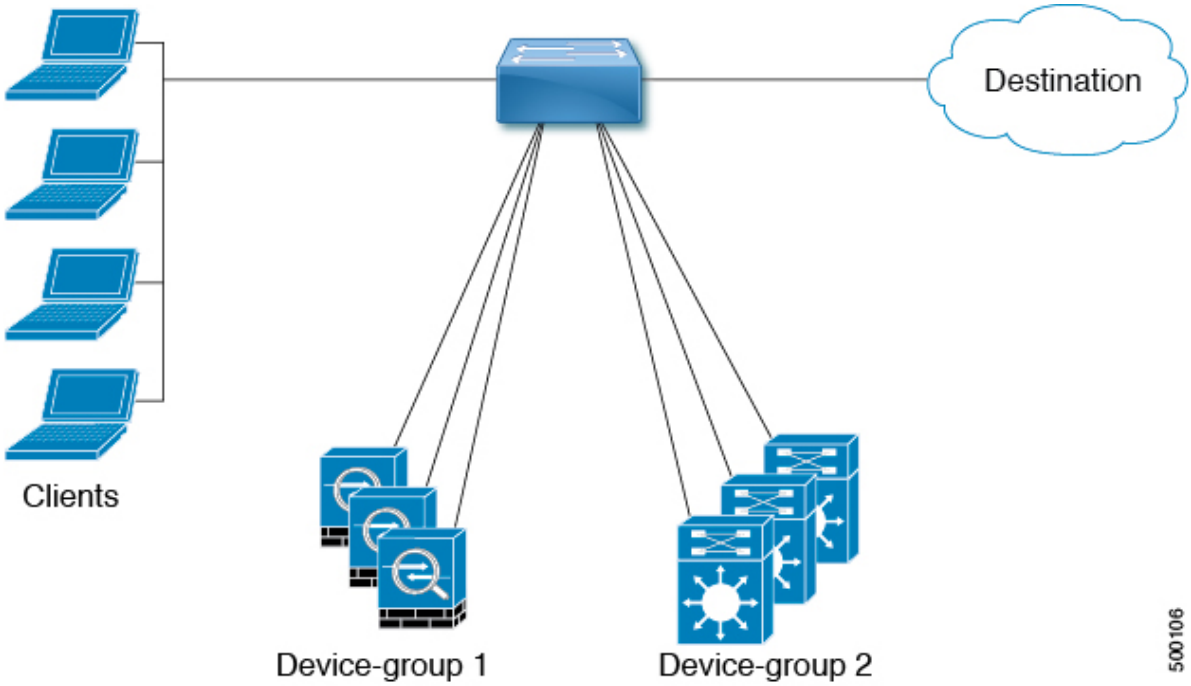
デバイス グループ レベルまたはノード レベルでプローブを設定できます。ノードレベルのプローブでは、各ノードに独自のプローブを設定でき、ノードごとの詳細なカスタマイズが可能です。ノードレベルのプローブは、障害の状況について各ノードを別々の方法でモニタする必要があるシナリオ（IPv6 デバイス グループでノードごとに特定の IPv4 プローブが必要な場合など）に役立ちます。

ITD サービスの複数のデバイス グループ

Cisco NX-OS Release 7.0(3)I3(1) 以降、ITD サービスで複数のデバイス グループがサポートされています（以下の図を参照）。ITD サービスは、さまざまなデバイス グループを指定する複数のシーケンスを含むルート マップを 1 つ生成します。

各デバイス グループは、必要なサービスは異なるが同じ入力インターフェイスに到達するさまざまなタイプのトラフィックを表します。インターフェイス上のトラフィックは、仮想 IP アドレスに基づいて適切なデバイス グループにリダイレクトされます。同じインターフェイス上の ITD サービスごとに複数のデバイス グループがサポートされるので、ITD を拡張することができます。

図 *5*：*ITD* サービスの複数のデバイス グループ



サポートされるデバイス グループの数については、ご使用のリリースの『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

VRF のサポート

ITD サービスは、デフォルト VRF でもデフォルト以外の VRF でも設定できます。

ITD サービスでトラフィックをリダイレクトするには、入力インターフェイスおよびデバイス グループ ノードのすべてが同じ VRF に属している必要があります。設定済み VRF で、関連するデバイス グループのすべての入力インターフェイスおよびノード メンバーが到達可能であることを確認する必要があります。

ルータ ACL

スイッチは ITD によるルータ アクセス コントロール リスト（RACL）をサポートします。

ITD と RACL を同じ入力インターフェイスに設定できます。TCAM にダウンロードされる設定結果の RACL は、ITD によって生成された ACL とユーザ設定 RACL を合わせた成果物です。RACL で設定された permit ステートメントと deny ステートメントは、ITD によって作成された ACL 許可およびリダイレクト エントリと結合されます。この機能により、選択したトラフィックのフィルタリングおよび負荷分散を行うことができます。

（注） ITD の入力インターフェイスで RACL を設定すると、ITD 統計情報は機能しません。

許可および除外 ACL

許可 ACL 機能では、ITD サービスにアクセス コントロール リスト（ACL）を割り当てることができます。ACL 内の permit メソッドを指定した各アクセス コントロール エントリ（ACE）について、この機能は不要なトラフィックをフィルタリングし、IP アクセス リストとルートマップを生成して許可トラフィックをロード バランシングします。

ITD に ITD ロード バランサから除外させるトラフィックを指定する除外 ACL を設定できます。除外 ACL によって選択されたトラフィックは RIB ルーティングされ、ITD をバイパスします。除外 ACL では、送信元と宛先の両方のフィールドに基づいてフィルタリングできます。除外 ACL は仮想 IP アドレスより優先されます。

仮想 IP アドレス フィルタリング

仮想 IP アドレスを使用して ITD のトラフィックをフィルタリングできます。トラフィック フィルタリング用の仮想 IP アドレスとサブネット マスクの組み合わせは、宛先フィールドでのみサポートされます。

ポート番号ベースのフィルタリング

ポート番号を使用して ITD のトラフィックをフィルタリングできます。レイヤ 4 ポート（例：ポート 80）に基づくトラフィックのフィルタリングでは、次の方法がサポートされます。

- 宛先ポートの照合

  宛先ポートが 80 の送信元または宛先 IP アドレスが一致します（例：仮想 IP アドレスを **0.0.0.0 0.0.0.0 tcp 80** として設定します）。

- 送信元ポートの照合

80 以外のポートは ITD をバイパスし、ポート 80 はリダイレクトされます（例：除外 ACL を **permit tcp any neq 80 any** として設定します）。

- 複数のポート番号の照合

  ITD に複数の仮想 IP アドレス ライン（各ポートに 1 つずつ）を設定できます。

複数の入力インターフェイス

複数の入力インターフェイスに対してトラフィック リダイレクト ポリシーを適用するように ITD サービスを設定できます。この機能では、単一の ITD サービスを使用して、さまざまなインターフェイスに到着するトラフィックを一連のノードにリダイレクトできます。

システム ヘルス モニタリング

ITD は次のヘルスモニタリング機能をサポートしています。

- サンドイッチ モードの ITD チャネルおよび ITD ピア サービスをモニタする。
- 設定済みプローブを使用して、ノードの正常性をモニタする。
- 入力インターフェイスの状態をモニタする。

ヘルス モニタリングでは次の重大なエラーを検出して修正します。

- ITD サービスが shut/no shut モードであるか、削除されている。
- スイッチのリブート。
- スーパーバイザ スイッチオーバー。
- インサービス ソフトウェア アップグレード（ISSU）。
- ITD サービス ノード障害。
- 入力インターフェイスがダウンしている。

ノードのモニタリング

ITD ヘルス モニタリング モジュールは、障害の検出および障害シナリオの処理を目的に、定期的にノードをモニタします。ヘルス モニタリング用に各ノードを定期的にプローブで検査するため、ICMP、TCP、UDP、および DNS プローブがサポートされます。

ノードに接続されたインターフェイスの正常性

Cisco NX-OS Release 7.0(3)I3(1) から、ITD は IP サービス レベル契約（IP SLA）機能を活用して、定期的に各ノードをプローブで検査します。以前のリリースでは、ITD はインターネット制御メッセージプロトコル（ICMP）を使用して定期的に各ノードをプローブで検査します。プローブはデ

フォルトで 10 秒の頻度で送信され、最小で 1 秒まで設定可能です。プローブはすべてのノードに同時に送信されます。プール グループ設定の一部としてプローブを設定できます。

プローブは、3 回再試行した後に障害が発生したと宣言されます。その場合、ノードの状態は「Failed」になり、ステータスは「PROBE_FAILED」になります。

ピア同期

ピア同期機能は、サンドイッチ モードの 2 つの ITD ピア サービス間でノードのヘルス ステータスを同期します。これは、いずれかの ITD ピア サービスのリンクがダウンした場合にトラフィックの損失を防ぐために役立ちます。

各 ITD サービスはピア サービスを定期的にプローブで検査して、障害を検出します。ping は ITD ピア サービスに毎秒送信されます。応答がない場合は 3 回再試行されます。頻度と再試行回数は設定できません。

Failaction 再割り当て

ITD の Failaction により、障害が発生したノード上のトラフィックを、最初に使用可能なアクティブ ノードに再割り当てできます。

ノードがダウンすると、そのノードに関連付けられたトラフィックまたはバケットは、設定されている一連のノードで最初に検出されたアクティブ ノードに再割り当てされます。新しく再割り当てされたノードでも障害が発生すると、トラフィックまたはバケットは次に使用可能なアクティブ ノードに再割り当てされます。障害が発生したノードがアクティブ状態に戻ると、トラフィックはこの新しいノードに戻され、ノードは接続の提供を再開します。

すべてのノードがダウンした場合、パケットは自動的にルーティングされます。

（注） Failaction 機能をイネーブルにする前に、ITD デバイス グループにプローブを設定する必要があります。

Failaction 再割り当てを使用しない場合

Failaction によるノードの再割り当てを設定しない場合は、次の 2 つのシナリオが考えられます。

- シナリオ 1：プローブを設定する
- シナリオ 2：プローブを設定しない

プローブを設定して Failaction 再割り当てを使用しない場合

ITD プローブでは、ノードの障害やサービス到達可能性の消失を検出できます。ノードに障害が発生した場合、Failaction が設定されていないと、トラフィックはルーティングされ、再割り当ては行われません。ノードが回復すると、その回復したノードがトラフィックの処理を開始します。

プローブを設定せずに Failaction 再割り当てを使用しない場合

プローブが設定されていないと、ITDはノードの障害を検出できません。ノードがダウンしても、ITD はアクティブ ノードへのトラフィックの再割り当てまたはリダイレクトを行いません。

ITD のライセンス要件

製品	ライセンス要件
Cisco NX-OS	ITD にはネットワーク サービス ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ITD の前提条件

ITD には、次の前提条件があります。

- **feature pbr** コマンドを使用して、ポリシーベース ルーティング（PBR）をイネーブルにする必要があります。

ITD の注意事項と制約事項

ITD 設定時の注意事項と制約事項は次のとおりです。

- コンフィギュレーション ロールバックは、ITD サービスがターゲットとソースの両方の設定で shut モードになっている場合にのみサポートされます。
- ITD は IPv4 でのみサポートされます。IPv6 ではサポートされていません。
- ITD は次のスイッチでサポートされています。
  - Cisco Nexus 9332PQ、9372PX、9372TX、9396PX、9396TX、93120TX、および 93128TX スイッチ
  - Cisco Nexus X9432PQ、X9464PX、X9464TX、X9536PQ、X9564PX、X9564TX、および X9636PQ ライン カードを備えた Cisco Nexus 9500 シリーズ スイッチ

- ITD は Cisco Nexus 9300 シリーズ スイッチのアップリンク ポートではサポートされていません。
- 7.0(3)I3(1) より前の Cisco NX-OS リリースを使用して ITD サービスを設定する場合は、**access-list** オプションを設定しないでください。このオプションはサポートされていません。ただし、**exclude access-list** オプションはサポートされているため使用できます。
- 除外 ACL 機能には、次の注意事項と制約事項が適用されます。
  - 除外 ACL は、許可アクセス コントロール エントリ（ACE）のみをサポートします。拒否 ACE はサポートされていません。
  - 除外 ACL 内の許可 ACE に一致するトラフィックは ITD をバイパスします。
- 許可 ACL 機能には、次の注意事項と制約事項が適用されます。
  - ユーザ定義の ACL は 1 つのみサポートされます。
  - **permit** メソッドを指定した ACE のみが ACL でサポートされます。他のメソッド（**deny** や **remark** など）を指定した ACE は無視されます。
  - 1 つの ACL で最大 256 の許可 ACE がサポートされます。
  - Failaction と重み付けロード バランシングはどちらもノード間でサポートされます。
  - ITD では許可 ACL 機能または仮想 IP アドレス（VIP）機能のいずれかのみがサポートされ、両方はサポートされません。
  - 送信元および宛先 IP ベースのロード バランシングでは、ACE の送信元または宛先 IP アドレスで /28 を超えるサブネット マスクを使用することはできません。
  - 許可 ACL 機能にマスク位置を設定することはできません。
- デバイス グループのノードを中断なしで追加または削除できる ITD セッションは、次ではサポートされません。
  - スタンバイまたはバックアップ ノード
  - 重み
  - ネットワーク アドレス変換（NAT）
  - 許可および除外 ACL 機能
  - ノードレベルのプローブ

ITD のデフォルト設定

次の表に、ITD パラメータのデフォルト設定を示します。

表 *1*：デフォルトの *ITD* パラメータ

パラメータ	デフォルト
Probe frequency	10 秒
Probe retry down count	1
Probe retry up count	1
Probe timeout	5 秒

ITD の設定

サーバはスイッチにルーテッド インターフェイスまたはポート チャネルを介して接続することも、スイッチ仮想インターフェイス（SVI）を設定したスイッチポートを介して接続することもできます。

ITD のイネーブル化

ITD コマンドにアクセスするには、ITD 機能をイネーブルにしておく必要があります。

はじめる前に

ネットワーク サービス ライセンスがインストールされていることを確認します。

ポリシーベース ルーティング（PBR）がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **feature itd**
3. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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。

	コマンドまたはアクション	目的
ステップ 2	[**no**] **feature itd** 例： `switch(config)# feature itd`	ITD機能をイネーブルにします。ITDは、デフォルトではディセーブルに設定されています。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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ます。

デバイス グループの設定

ITD デバイス グループを作成してから、グループのノードを指定してプローブで検査することができます。Cisco NX-OS Release 7.0(3)I3(1) 以降では、複数のデバイス グループを設定できます。

はじめる前に

ITD 機能がイネーブルになっていることを確認します。

デバイスで Cisco NX-OS Release 7.0(3)I3(1) 以降を実行している場合は、**feature sla sender** および **feature sla responder** コマンドが設定されていることを確認してください。

手順の概要

1. **configure terminal**
2. [**no**] **itd device-group***name*
3. [**no**] **node ip***ipv4-address*
4. [**no**] **weight***weight*
5. **exit**
6. ノードごとにステップ 3 ～ 5 を繰り返します。
7. [**no**] **probe**{**icmp** | **tcp port***port-number* | **udp port***port-number* | **dns** {*hostname* | *target-address*}} [**frequency***seconds*] [[**retry-down-count** | **retry-up-count**] *number*] [**timeout***seconds*]
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **itd device-group***name*
	
	例：
	`switch(config)# itd device-group dg1`
	`switch(config-device-group)#`
		ITD デバイス グループを作成し、デバイス グループ コンフィギュレーション モードを開始します。最大 32 文字の英数字を入力できます。

ステップ 3	[**no**] **node ip***ipv4-address*
	
	例：
	`switch(config-device-group)# node ip 20.20.20.3`
	`switch(config-dg-node)#`
		ITD のノードを指定します。

ステップ 4	[**no**] **weight***weight* 例： `switch(config-dg-node)# weight 6`	ITD のノードの重みを指定します。有効な範囲は 1 ～ 256 です。

ステップ 5	**exit**
	
	例：
	`switch(config-dg-node)# exit`
	`switch(config-device-group)#`
		デバイス グループ ノード コンフィギュレーション モードを終了します。

ステップ 6	ノードごとにステップ 3 ～ 5 を繰り返します。	
ステップ 7	[**no**] **probe** {**icmp** | **tcp port***port-number* | **udp port***port-number* | **dns** {*hostname* | *target-address*}} [**frequency***seconds*] [[**retry-down-count** | **retry-up-count**] *number*] [**timeout***seconds*] 例： `switch(config-device-group)# probe icmp frequency 100`	ITD のグループ サービス プローブを設定します。Cisco NX-OS Release 7.0(3)I3(1) 以降で、ITD サービスのプローブとして指定できるプロトコルは ICMP、TCP、UDP、または DNS です。以前のリリースでは、ITD サービスのプローブとして ICMP が使用されます。 オプションは次のとおりです。 • **frequency**：プローブの頻度を秒単位で指定します。値の範囲は 1 ～ 604800 です。 • **retry-down-count**：ノードがダウンしたときにプローブによって行われる再試行の回数を指定します。指定できる範囲は 1 ～ 5 です。

	コマンドまたはアクション	目的
		• **retry-up-count**：ノードがアクティブ状態に戻ったときにプローブによって行われる再試行の回数を指定します。指定できる範囲は 1 ～ 5 です。 • **timeout**：タイムアウト時間を秒単位で指定します。値の範囲は 1 ～ 604800 です。
ステップ 8	**copy running-config startup-config** 例： `switch(config-device-group)# copy running-config startup-config`	（任意） 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ます。

ITD サービスの設定

はじめる前に

ITD 機能がイネーブルになっていることを確認します。

ITD サービスに追加するデバイス グループが設定されていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **itd***service-name*
3. [**no**] **device-group***device-group-name*
4. [**no**] **ingress interface***interface*
5. [**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range***x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range***x y*}} | **buckets***bucket-number* | **mask-position***position*}
6. **virtual ip***ipv4-address ipv4-network-mask* [**tcp** | **udp** {*port-number* | **any**}] [**advertise** {**enable** | **disable**}]
7. [**no**] **failaction node reassign**
8. [**no**] **vrf***vrf-name*
9. [**no**] **exclude access-list***acl-name*
10. （任意） [**no**] **peer local service***peer-service-name*
11. **no shutdown**
12. （任意） **show itd** [*itd-name*]
13. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **itd***service-name*
	
	例：
	`switch(config)# itd service1`
	`switch(config-itd)#`
		ITD サービスを設定し、ITD コンフィギュレーション モードを開始します。最大 32 文字の英数字を入力できます。

ステップ 3	[**no**] **device-group***device-group-name* 例： `switch(config-itd)# device-group dg1`	ITD サービスに既存のデバイス グループを追加します。*device-group-name* は、デバイス グループの名前を指定します。最大 32 文字の英数字を入力できます。 （注） Cisco NX-OS Release 7.0(3)I3(1) 以降では、ITD サービスに複数のデバイス グループを追加できます。
ステップ 4	[**no**] **ingress interface***interface* 例： `switch(config-itd)# ingress interface ethernet 4/1-10`	ITD サービスに 1 つ以上のインターフェイスを追加します。 複数のインターフェイスは、カンマを（「,」）を使用して区切ります。インターフェイスの範囲は、ハイフン（「-」）を使用して指定します。
ステップ 5	[**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range***x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range***x y*}} | **buckets***bucket-number* | **mask-position***position*} 例： `switch(config-itd)# load-balance method src ip buckets 16`	ITD サービスのロードバランシング オプションを設定します。 オプションは次のとおりです。 • **method**：送信元または宛先 IP アドレスベースの負荷またはトラフィック分散を指定します。 • **buckets**：作成するバケットの数を指定します。1 つ以上のバケットが、1 つのノードにマッピングされます。バケットは 2 のべき乗数で設定する必要があります。範囲は 2 ～ 256 です。 （注） 設定するバケットの数がノードの数より多い場合、バケットはすべてのノードにラウンドロビン方式で適用されます。 • **mask-position**：ロードバランスのマスク位置番号を指定します。範囲は 0 ～ 31 です。
ステップ 6	**virtual ip***ipv4-address ipv4-network-mask* [**tcp** | **udp** {*port-number* | **any**}] [**advertise** {**enable** | **disable**}]	ITD サービスの仮想 IPv4 アドレスを設定します。 **tcp** および **udp** オプションは、仮想 IP アドレスが指定のプロトコルによるフローを受け入れることを指定します。ポート範囲は 0 ～ 65535 です。

	コマンドまたはアクション	目的
	例： `switch(config-itd)# virtual ip 4.4.4.4 255.255.0.0 tcp any advertise enable`	**advertise** {**enable** | **disable**} オプションは、仮想 IP ルートをネイバー デバイスにアドバタイズするかどうかを指定します。
ステップ 7	[**no**] **failaction node reassign** 例： `switch(config-itd)# failaction node reassign`	ノード障害後のトラフィック再割り当てを有効にします。障害が発生したノードへのトラフィックは、最初に使用可能なアクティブ ノードに再割り当てされます。
ステップ 8	[**no**] **vrf***vrf-name* 例： `switch(config-itd)# vrf RED`	ITD サービスの VRF を指定します。
ステップ 9	[**no**] **exclude access-list***acl-name* 例： `switch(config-itd)# exclude access-list acl1`	ITD に ITD ロードバランサから除外させるトラフィックを指定します。
ステップ 10	[**no**] **peer local service***peer-service-name* 例： `switch(config-itd)# peer local service service-A`	（任意） 同じ（ローカル）VDC 上にあるサンドイッチ モードの 2 つの ITD ピア サービスのいずれかを指定します。2 番目の ITD ピア サービスを指定するには、別の ITD サービスを作成して、このコマンドを使用する必要があります。両方のサービスでこのコマンドを実行すると、ノードのヘルス ステータスが 2 つのサービス間で同期されます。 （注） 2 つのデバイス グループのノードが同じ順序である必要があります。具体的には、両方のデバイス グループの最初のエントリが同じサンドイッチ モードのエントリであれば、順序が維持されます。
ステップ 11	**no shutdown** 例： `switch(config-itd)# no shutdown`	ITD サービスをイネーブルにします。
ステップ 12	**show itd** [*itd-name*] 例： `switch(config-itd)# show itd`	（任意） 指定した ITD インスタンスのステータスおよび設定を表示します。
ステップ 13	**copy running-config startup-config** 例： `switch(config-itd)# copy running-config startup-config`	（任意） 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ます。

ITD サービスへの ACL の割り当て

許可アクセス コントロール リスト（ACL）機能を使用して ITD サービスに ACL を割り当てることができます。ACL 内の **permit** メソッドを指定した各アクセス コントロール エントリ（ACE）について、この機能は不要なトラフィックをフィルタリングし、IP アクセス リストとルート マップを生成して許可トラフィックをロード バランシングします。送信元または宛先のいずれかの IP アドレスを使用したロード バランシングがサポートされます。

はじめる前に

ITD 機能がイネーブルになっていることを確認します。

ITD サービスに追加するデバイス グループが設定されていることを確認します。

ITD サービスに割り当てる ACL が設定されていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **itd***itd-name*
3. [**no**] **device-group***device-group-name*
4. [**no**] **ingress interface***interface*
5. [**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range***x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range***x y*}} | **buckets***bucket-number*}
6. **access-list***acl-name*
7. **no shutdown**
8. **show ip access-lists** | **b***itd-name*
9. **show route-map***itd-name***_itd_pool**
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **itd***itd-name*
	
	例：
	`switch(config)# itd service1`
	`switch(config-itd)#`
		ITD サービスを設定し、ITD コンフィギュレーション モードを開始します。最大 32 文字の英数字を入力できます。

	コマンドまたはアクション	目的
ステップ 3	[**no**] **device-group***device-group-name* 例： `switch(config-itd)# device-group dg1`	ITD サービスに既存のデバイス グループを追加します。*device-group-name* は、デバイス グループの名前を指定します。最大 32 文字の英数字を入力できます。
ステップ 4	[**no**] **ingress interface***interface* 例： `switch(config-itd)# ingress interface ethernet 4/1-10`	ITD サービスに 1 つ以上のインターフェイスを追加します。 複数のインターフェイスは、カンマを（「,」）を使用して区切ります。インターフェイスの範囲は、ハイフン（「-」）を使用して指定します。
ステップ 5	[**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range***x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range***x y*}} | **buckets***bucket-number*} 例： `switch(config-itd)# load-balance method src ip buckets 16`	ITD サービスのロード バランシング オプションを設定します。 オプションは次のとおりです。 • **method**：送信元または宛先 IP アドレスベースの負荷またはトラフィック分散を指定します。 • **buckets**：作成するバケットの数を指定します。1 つ以上のバケットが、1 つのノードにマッピングされます。バケットは 2 のべき乗数で設定する必要があります。範囲は 2 ～ 256 です。 （注） 設定するバケットの数がノードの数より多い場合、バケットはすべてのノードにラウンド ロビン方式で適用されます。
ステップ 6	**access-list***acl-name* 例： `switch(config-itd)# access-list acl1`	ITD サービスに ACL を割り当てます。
ステップ 7	**no shutdown** 例： `switch(config-itd)# no shutdown`	ITD サービスをイネーブルにします。
ステップ 8	**show ip access-lists** | **b***itd-name* 例： `switch(config-itd)# show ip access-lists | b service1`	ITD サービスへの ACL の割り当て後に各バケットに対して生成される IP アクセス リストを表示します。
ステップ 9	**show route-map***itd-name***_itd_pool** 例： `switch(config-itd)# show route-map service1_itd_pool`	ITD サービスへの ACL の割り当て後に生成されるルート マップを表示します。

	コマンドまたはアクション	目的
ステップ 10	**copy running-config startup-config** 例： `switch(config-itd)# copy running-config startup-config`	（任意） 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ます。

中断のないノードの追加または削除

ITD サービスをシャットダウンせずにデバイス グループのノードを追加または削除できる ITD セッションを設定できます。これにより、ITD サービスのシャットダウン時に発生する可能性があるトラフィックの中断が回避されます。

はじめる前に

ITD 機能がイネーブルになっていることを確認します。

デバイス グループおよび ITD サービスが設定されていることを確認します。

手順の概要

1. **configure terminal**
2. **itd session device-group***device-group-name*
3. [**no**] **node ip***ip-address*
4. {**commit** | **abort**}
5. （任意） **show itd session device-group** [*name*]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**itd session device-group***device-group-name*
	
	例：
	`switch(config)# itd session device-group dg1`
	`switch(config-session-device-group)#`
		指定されたデバイス グループの ITD セッションを作成します。

	コマンドまたはアクション	目的
ステップ 3	[**no**] **node ip***ip-address* 例： `switch(config-session-device-group)# node ip 2.2.2.1`	指定されたノードをITDデバイス グループに追加します。このコマンドの **no** 形式を使用すると、指定したノードがITD デバイス グループから削除されます。 追加または削除するノードごとにこのステップを繰り返します。

ステップ 4	{**commit** | **abort**}
	
	例：
	`switch(config-session-device-group)# commit`
	`switch(config)#`
		commit コマンドは、一連の新しいノードまたは変更されたノードで ITD デバイス グループを更新して、バケットを再割り当てし、ITDセッションの設定をクリーンアップします。
		abort コマンドでは ITD セッションの設定が無視されて、ITD デバイス グループは更新されません。

ステップ 5	**show itd session device-group** [*name*] 例： `switch(config)# show itd session device-group dg1`	（任意） 設定されているすべてのITDセッションまたは指定したデバイス グループの ITD セッションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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ます。

ITD 設定の確認

ITD 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip access-lists | **b***itd-name*	ITD サービスに ACL を割り当てるときに各バケットに対して生成される IP アクセス リストを表示します。

コマンド	目的
show itd [*itd-name*] [**brief** | **vrf** [*vrf-name*]]	指定したITDインスタンスのステータスおよび設定を表示します。 • 特定の ITD インスタンスのステータスおよび設定を表示するには、*itd-name* 引数を使用します。 • ステータスおよび設定の要約情報を表示するには、**brief** キーワードを使用します。 • 指定した ITD インスタンスの VRF を表示するには、**vrf** キーワードを使用します。
show itd {**all** | *itd-name*} [**dst***ip-address* | **src***ip-address*] **statistics** [**brief**]	すべてまたは指定したITDインスタンスの統計情報を表示します。 • 特定の ITD インスタンスの統計情報を表示するには、*itd-name* 引数を使用します。 • 要約情報を表示するには、**brief** キーワードを使用します。 （注） このコマンドを使用して ITD の統計情報を表示するには、あらかじめ **itd statistics***itd-name* コマンドを使用してITDの統計情報をイネーブルにしておく必要があります。
show itd session device-group [*name*]	設定されているすべてのITDセッションまたは指定したデバイス グループの ITD セッションを表示します。
show route-map*itd-name***_itd_pool**	ITD サービスに ACL を割り当てるときに生成されるルート マップを表示します。
show running-config services	設定された ITD デバイス グループおよびサービスを表示します。

以下に、ITD 設定を確認する例を示します。

```
switch# show itd

Name           Probe LB Scheme  Status   Buckets
-------------- ----- ---------- -------- -------
WEB            ICMP  src-ip     ACTIVE   2

Device Group                                        VRF-Name
--------------------------------------------------- -------------
WEB-SERVERS
```

```
Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
WEB_itd_pool                   Po-1         UP       -

Virtual IP     Netmask/Prefix            Protocol   Port
-------------------------------------- ---------- -----
10.10.10.100 / 255.255.255.255           IP           0

  Node  IP                 Config-State Weight Status     Track_id
  ------------------------ ------------ ------ ---------- ---------
  1     10.10.10.11        Active       1      OK           -

        Bucket List
        ----------------------------------------------------------------------
        WEB_itd_vip_1_bucket_1


  Node  IP                 Config-State Weight Status     Track_id
  ------------------------ ------------ ------ ---------- ---------
  2     10.10.10.12        Active       1      OK           -

        Bucket List
        ----------------------------------------------------------------------
        WEB_itd_vip_1_bucket_2
```

```
switch# show itd brief

Name           Probe LB Scheme  Interface  Status   Buckets
-------------- ----- ---------- ---------- -------- --------
WEB            ICMP  src-ip     Eth3/3     ACTIVE   2

Device Group                                    VRF-Name
----------------------------------------------- -------------
WEB-SERVERS


Virtual IP      Netmask/Prefix      Protocol     Port
----------------------------------- ------------ ----------
10.10.10.100 / 255.255.255.255      IP           0

  Node  IP                 Config-State Weight Status     Track_id
  ------------------------ ------------ ------ ---------- ---------
  1     10.10.10.11        Active       1      OK           -
  2     10.10.10.12        Active       1      OK           -
```

```
switch# show itd statistics

Service        Device Group             VIP/mask               #Packets
-------------------------------------------------------------------------------
test            dev              9.9.9.10 / 255.255.255.0       114611  (100.00%)

Traffic Bucket        Assigned to      Mode       Original Node   #Packets
-------------------------------------------------------------------------------
test_itd_vip_0_acl_0  10.10.10.9       Redirect    10.10.10.9      57106  (49.83%)

Traffic Bucket        Assigned to      Mode       Original Node   #Packets
-------------------------------------------------------------------------------
test_itd_vip_0_acl_1  12.12.12.9       Redirect    12.12.12.9      57505  (50.17%)
```

```
switch# show running-config services

version 7.0(3)I1(2)
feature itd

itd device-group WEB-SERVERS
node ip 10.10.10.11
node ip 10.10.10.12
probe icmp
```

```
itd WEB
device-group WEB-SERVERS
virtual ip 10.10.10.100 255.255.255.255
ingress interface ethernet 3/3
no shut
```

ITD の設定例

以下に、ITD デバイス グループを設定する例を示します。

```
switch(config)# feature itd
switch(config)# itd device-group dg
switch(config-device-group)# node ip 210.10.10.11
switch(config-dg-node)# weight 6
switch(config-dg-node)# exit
switch(config-device-group)# node ip 210.10.10.12
switch(config-dg-node)# weight 6
switch(config-dg-node)# exit
switch(config-device-group)# node ip 210.10.10.13
switch(config-dg-node)# weight 2
switch(config-dg-node)# exit
switch(config-device-group)# node ip 210.10.10.14
switch(config-dg-node)# weight 2
switch(config-dg-node)# exit
switch(config-device-group)# probe icmp
```

次に、ノードレベルのプローブを設定する例を示します（デバイス グループレベルのプローブではありません）。ノードレベルのプローブでは、各ノードに独自のプローブを設定でき、ノードごとの詳細なカスタマイズが可能です。

```
switch(config)# feature itd
switch(config)# itd device-group Servers
switch(config-device-group)# node ip 192.168.1.10
switch(config-dg-node)# probe icmp frequency 10 retry-down-count 5
switch(config-device-group)# node ip 192.168.1.20
switch(config-dg-node)# probe icmp frequency 5 retry-down-count 5
switch(config-device-group)# node ip 192.168.1.30
switch(config-dg-node)# probe icmp frequency 20 retry-down-count 3
```

以下に、仮想 IPv4 アドレスを設定する例を示します。

```
switch(config)# feature itd
switch(config)# itd test
switch(config-itd)# device-group dg
switch(config-itd)# ingress interface ethernet 2/1
switch(config-itd)# virtual ip 210.10.10.100 255.255.255.255 advertise enable tcp any
```

次に、トラフィックを比例的に分散する重み付けロード バランシングを設定する例を示します。この例では、ノード 1 および 2 はノード 3 および 4 の 3 倍ものトラフィックを受け取ります。

```
switch(config)# feature itd
switch(config)# itd device-group dg
switch(config-device-group)# probe icmp
switch(config-device-group)# node ip 210.10.10.11
switch(config-dg-node)# weight 3
switch(config-device-group)# node ip 210.10.10.12
switch(config-dg-node)# weight 3
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
```

次に、ITD に ITD ロード バランサから除外させるトラフィックを指定する除外 ACL を設定する例を示します。たとえば、ファイアウォール検査を必要としない開発者 VLAN やテストベッド VLAN は ITD をバイパスできます。

```
switch(config)# feature itd
switch(config)# itd Service_Test
switch(config-itd)# device-group test-group
switch(config-itd)# ingress interface vlan10
switch(config-itd)# exclude access-list ITDExclude
switch(config-itd)# no shutdown

switch(config)# ip access-list ITDExclude
switch(config-acl)# 10 permit ip 5.5.5.0 255.255.255.0 any
switch(config-acl)# 20 permit ip 192.168.100.0 255.255.255.0 192.168.200.0
```

次に、acl1 を作成して ITD サービスに割り当てる例を示します。**show** コマンドは、生成された IP アクセス リストとルート マップを表示します。

```
switch(config)# ip access-list acl1
switch(config-acl)# 2460 permit tcp 100.1.1.0/24 any
switch(config-acl)# exit

switch(config)# itd test
switch(config-itd)# device-group dg1
switch(config-itd)# ingress interface Eth3/1
switch(config-itd)# load-balance method src ip
switch(config-itd)# access-list acl1

switch(config-itd)# show ip access-lists | b test
IP access list test_itd_ace_1_bucket_1
        10 permit tcp 100.1.1.0/26 any
IP access list test_itd_ace_1_bucket_2
        10 permit tcp 100.1.1.64/26 any
IP access list test_itd_ace_1_bucket_3
        10 permit tcp 100.1.1.128/26 any
IP access list test_itd_ace_1_bucket_4
        10 permit tcp 100.1.1.192/26 any

switch(config-itd)# show route-map test_itd_pool
route-map test_itd_pool, permit, sequence 10
Description: auto generated route-map for ITD service test
  Match clauses:
    ip address (access-lists): test_itd_ace_1_bucket_1
  Set clauses:
    ip next-hop verify-availability 1.1.1.1 track 2 [ UP ]
route-map test_itd_pool, permit, sequence 11
Description: auto generated route-map for ITD service test
  Match clauses:
    ip address (access-lists): test_itd_ace_1_bucket_2
  Set clauses:
    ip next-hop verify-availability 1.1.1.2 track 3 [ UP ]
route-map test_itd_pool, permit, sequence 12
Description: auto generated route-map for ITD service test
  Match clauses:
    ip address (access-lists): test_itd_ace_1_bucket_3
  Set clauses:
    ip next-hop verify-availability 10.10.10.9 track 4 [ up ]
route-map test_itd_pool, permit, sequence 13
Description: auto generated route-map for ITD service test
  Match clauses:
    ip address (access-lists): test_itd_ace_1_bucket_4
  Set clauses:
    ip next-hop verify-availability 10.10.10.10 track 5 [ up ]

switch(config-itd)# show itd test
Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
```

```
test           src-ip     ACTIVE   4

Exclude ACL
--------------------------------


Device Group                                          Probe  Port
------------------------------------------------- ----- ------
dg1                                                ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ --------
test_itd_pool                  Eth3/1       UP       1

ACL Name/SeqNo                   IP/Netmask/Prefix            Protocol Port
-------------------------------- ---------------------------- -------- ----
acl1/2460                          100.1.1.0/24                 TCP      0

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ----------------- ------- --- ----- ----- -------------- --- ---  -------
  1     1.1.1.1       Active   1  ICMP                      OK   2   10002
Bucket List
--------------------------------------------------------------------------------
test_itd_ace_1_bucket_1

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ----------------- ------- --- ----- ----- -------------- --- --- -------
  2     1.1.1.2       Active   1  ICMP                      OK   3   10003

Bucket List
--------------------------------------------------------------------------------
test_itd_ace_1_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ----------------- ------- --- ----- ----- -------------- --- --- -------
  3     10.10.10.9    Active   1  ICMP                      OK   4   10004

Bucket List
--------------------------------------------------------------------------------
test_itd_ace_1_bucket_3

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ----------------- ------- --- ----- ----- -------------- --- --- -------
  4     10.10.10.10   Active   1  ICMP                      OK   5   10005

Bucket List
--------------------------------------------------------------------------------
test_itd_ace_1_bucket_4
```

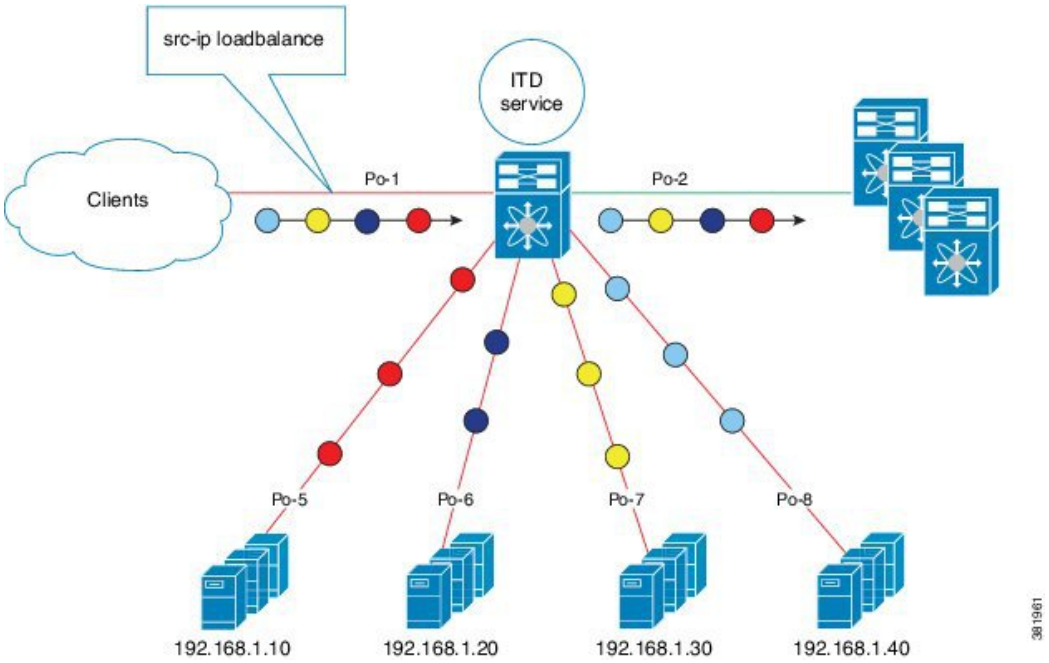
次に、デバイス グループ dg のノードを中断なしで追加および削除する ITD セッションを作成する例を示します。

```
switch(config)# itd session device-group dg
switch(config-session-device-group)# node ip 10.10.10.10
switch(config-session-device-group)# node ip 10.10.10.20
switch(config-session-device-group)# node ip 10.10.10.30
switch(config-session-device-group)# node ip 10.10.10.40
switch(config-session-device-group)# no node ip 20.20.20.20
switch(config-session-device-group)# commit
switch(config)#
```

設定例：ワンアーム展開モード

以下の設定では次の図に示すトポロジを使用します。

図 *6*：ワンアーム展開モード



手順 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

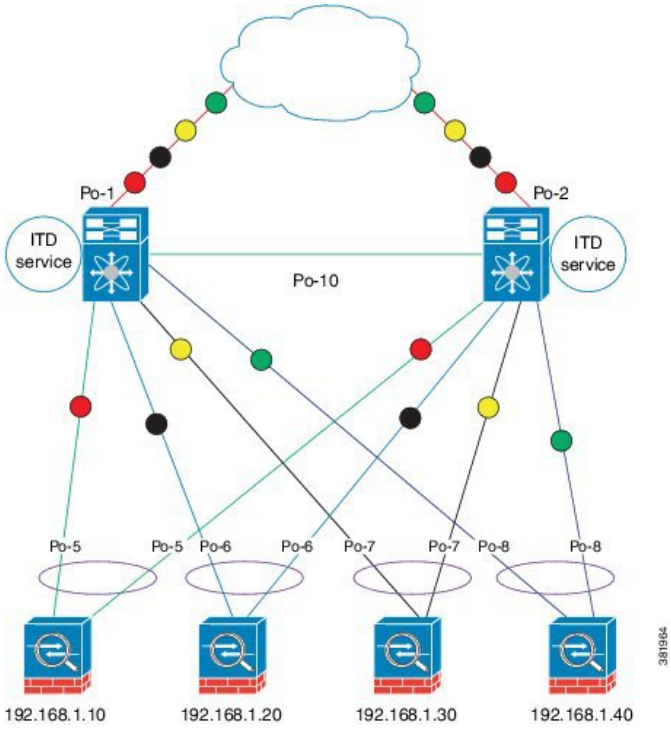
手順 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# device-group DG
switch(config-itd)# no shutdown
```

設定例：vPC でのワンアーム展開モード

以下の設定では次の図に示すトポロジを使用します。

図 *7*：*VPC* でのワンアーム展開モード



デバイス 1

手順 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

手順 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# device-group DG
switch(config-itd)# no shutdown
```

デバイス 2

手順 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

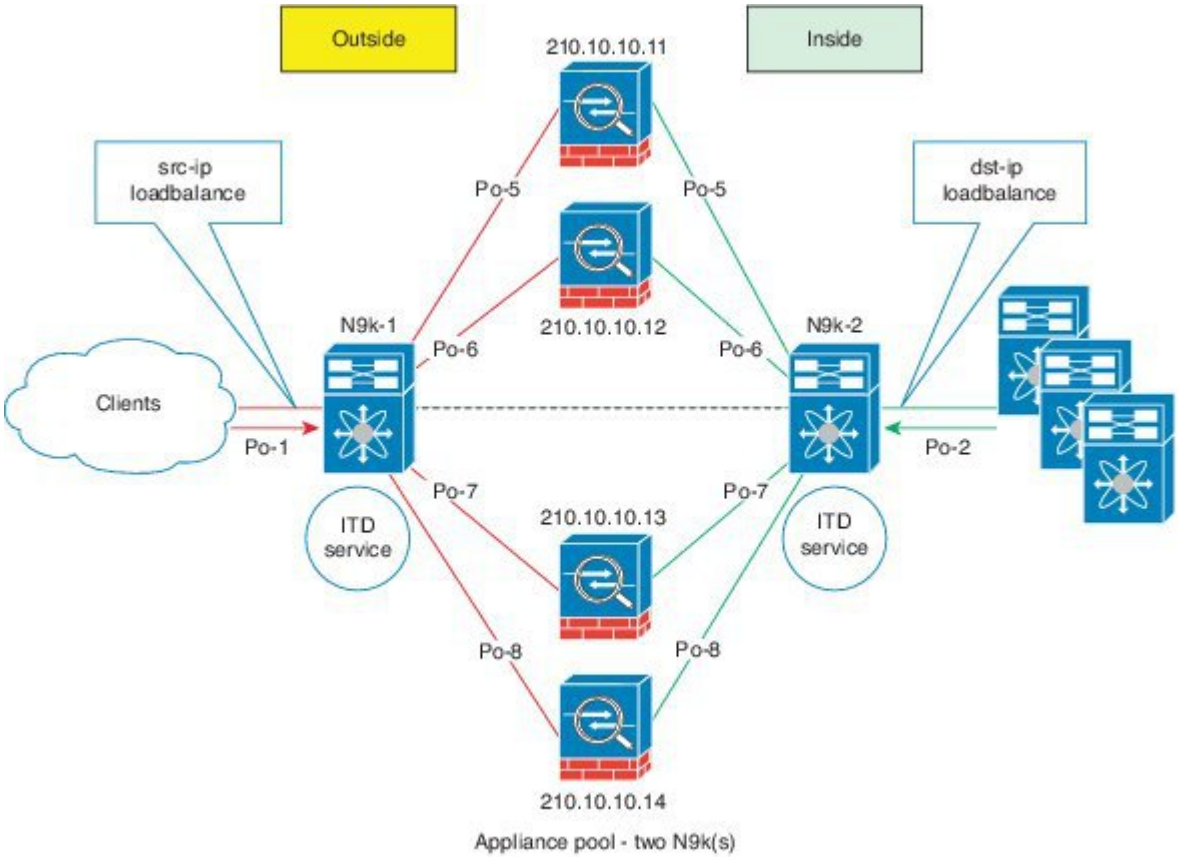
手順 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 2
switch(config-itd)# device-group DG
switch(config-itd)# no shutdown
```

設定例：サンドイッチ展開モード

以下の設定では次の図に示すトポロジを使用します。

図 *8*：サンドイッチ展開モード



デバイス 1

手順 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

手順 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# device-group DG
switch(config-itd)# load-balance method src ip
switch(config-itd)# no shutdown
```

デバイス 2

手順 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 220.10.10.11
switch(config-device-group)# node ip 220.10.10.12
switch(config-device-group)# node ip 220.10.10.13
switch(config-device-group)# node ip 220.10.10.14
switch(config-device-group)# probe icmp
```

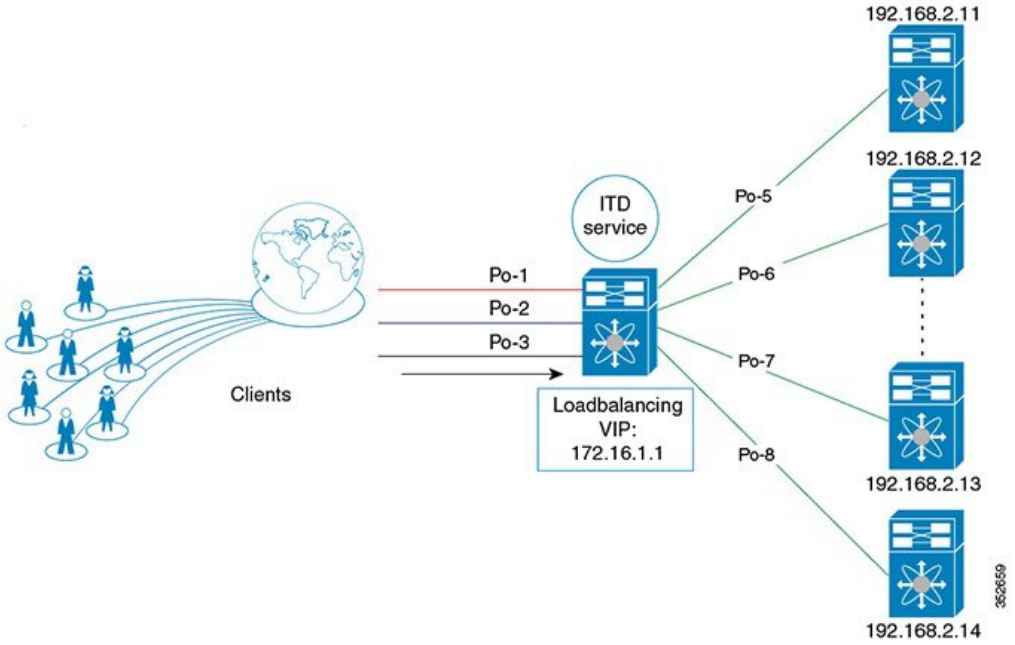
手順 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 2
switch(config-itd)# device-group DG
switch(config-itd)# load-balance method dst ip
switch(config-itd)# no shutdown
```

設定例：サーバ ロードバランシング展開モード

以下の設定では次の図に示すトポロジを使用します。

図 *9*：*VIP* を使用した *ITD* 負荷分散



手順 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

手順 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# ingress interface port-channel 2
switch(config-itd)# ingress interface port-channel 3
switch(config-itd)# device-group DG
Switch(config-itd)# virtual ip 210.10.10.100 255.255.255.255
switch(config-itd)# no shutdown
```

設定例：Web プロキシ展開モード

プロキシ サーバは、クライアントが他のサーバのリソースを要求する際に中継する機能を果たします。Webプロキシサーバは特にローカル ネットワークとインターネット間の中継として動作し

ます。通常、Web プロキシ サーバを利用する場合は、インターネット宛 Web トラフィックのリダイレクト先となるネットワーク デバイスが必要です（フォワード フロー）。ただし以降のパケット転送については、ネットワーク デバイスがパケットを定期的に転送するだけで済みます。

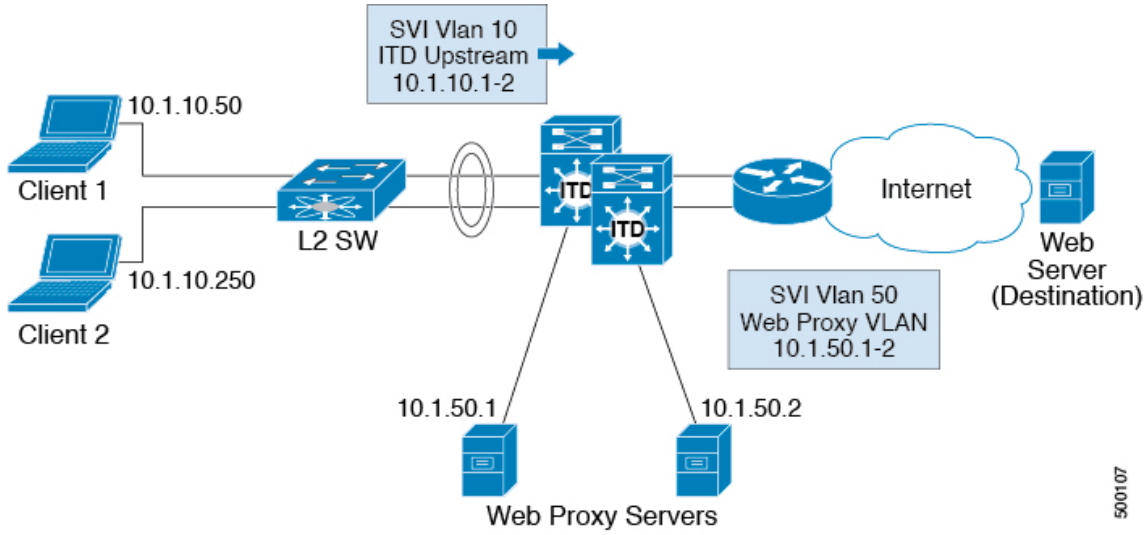
ITD を使用した Web プロキシ展開では、スイッチがインターネット宛 Web トラフィックを照合してプロキシ サーバに対してロード バランスを実行します。プロキシ サーバは Autonomous モードで動作（WCCP から独立してアクティブ-アクティブとして動作）し、リダイレクトされたトラフィックを処理します。ITD が実行するノードの正常性のプローブには、ノードの状態を追跡し、その可用性に基づいて適切にノードを削除または追加する目的があります。冗長性を確保するために、スタンバイ サーバをグループ レベルまたはノード レベルで設定することもできます。

通常はクライアント側 VLAN の順方向でのみ ITD リダイレクションが必要です。以降は、ITD リダイレクションおよび分散なしでパケットがルーティングまたは転送されます。このような Web プロキシ展開での ITD に必要なのは、順方向用に設定した 1 つの ITD サービスのみです。ただし、送信元レイヤ 4 ポートに基づいてトラフィックを選択するリバース トラフィック リダイレクションが必要です。LB パラメータの反転によってフローの対称性も維持する必要があります。

Web プロキシ展開の ITD では、Web プロキシ サーバの可用性を確認するために ITD プローブが使用されます。これが重要である理由は、障害が発生したプロキシ サーバ宛てに送信されたトラフィックは失われてしまうからです。

以下の設定では次の図に示すトポロジを使用します。

図 *10*：*Web* プロキシ展開モード



この例では、インターネットへの宛先ポート 80/443（入力 VLAN 10）は Web プロキシ サーバ 10.1.50.1 と 10.1.50.2 に分散されます。プライベート ネットワーク（10.0.0.0/8、192.168.0.0/16、172.16.0.0/20）を宛先とする VLAN 10 上のトラフィックはプロキシに送信されません。

手順 1：ITD デバイス グループの Web プロキシ サーバを設定し、サーバの IP アドレスを指定します。

```
itd device-group Web_Proxy_Servers
  probe icmp
  node ip 10.1.50.1
```

```
  node ip 10.1.50.2
```

手順 2：プライベート IP アドレス宛てのすべてのトラフィックを除外する除外 ACL を設定します。

```
ip access-list itd_exclude_ACL
  10 permit ip any 10.0.0.0 255.0.0.0
  20 permit ip any 192.168.0.0 255.255.0.0
  30 permit ip any 172.16.0.0 255.255.240.0
```

手順 3：除外 ACL を適用します。

```
Itd Web_proxy_SERVICE
  device-group Web_Proxy_Servers
  exclude access-list itd_exclude_ACL
  virtual ip 0.0.0.0 0.0.0.0 tcp 80  <- Any traffic to destination port 80 is redirected
to the Web_Proxy_Servers group.
  virtual ip 0.0.0.0 0.0.0.0 tcp 443 <- Any traffic to destination port 443 is redirected
to the Web_Proxy_Servers group.
  ingress interface Vlan 10
  failaction node reassign
  load-balance method src ip
  no shutdown
```

何らかの理由でリターン トラフィック リダイレクションも必要な場合は、さらに次の設定手順を実行します。

（注） レイヤ 4 の range 演算子を使用することで可能なのはポート フィルタリングのみです。また、除外 ACL は permit エントリのみをサポートします。

手順 4：ポート 80 と 443 を除くすべてを除外するリターン除外 ACL を設定します。

```
ip access-list itd_exclude_return
  10 permit tcp any range 0 79 any
  20 permit tcp any range 81 442 any
  30 permit tcp any range 444 65535 any
```

手順 5：リターン トラフィック用のリターン ITD サービスを設定し、除外 ACL を適用します。

```
Itd Web_proxy_SERVICE
  device-group Web_Proxy_Servers
  exclude access-list itd_exclude_return
  ingress interface Vlan 20   <- Internet-facing ingress interface on the Nexus switch
  failaction node reassign
  load-balance method dst ip  <- Flow symmetry between forward/return flow achieved by
flipping the LB parameter
  no shutdown
```

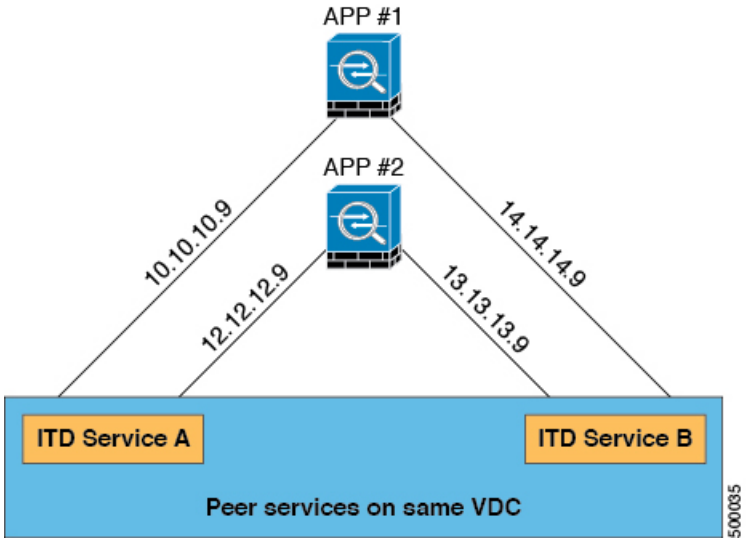
設定例：サンドイッチ モードのピア同期

ITD ピア サービス上のサンドイッチ アプライアンスへのリンクがダウンするたびに、サービスはノードへのリンクがダウンしていることを示す通知を自身のピアに送信します。その後、ピア サービスはトラフィックがそのリンクを通過しないように停止します。

ピア同期を行わないと、次のトポロジで ITD サービス A 上のアプライアンス APP #1 に接続されているリンクがダウンした場合、ITD サービス B にこれが通知されず、サービス B は APP #1 に引き続きトラフィックを送信するため、トラフィックがドロップされます。

以下の設定では次のトポロジを使用します。

図 *11*：サンドイッチ モードのピア同期



デバイス 1

手順 1：デバイス グループを定義します。

```
switch(config)# itd device-group dev-A
switch(config-device-group)# node ip 10.10.10.9 ---> Link to app #1
switch(config-device-group)# node ip 12.12.12.9 ---> Link to app #2
switch(config-device-group)# probe icmp
```

手順 2：ピア同期をイネーブルにして ITD サービスを定義します。

```
switch(config)# itd service-A
switch(config-itd)# device-group dev-A
switch(config-itd)# virtual ip 9.9.9.10 255.255.255.0
switch(config-itd)# ingress interface ethernet 7/4
switch(config-itd)# peer local service service-B
switch(config-itd)# no shutdown

switch(config-itd)# show itd
Name           Probe LB Scheme  Status   Buckets
-------------- ----- ---------- -------- -------
Service-A      ICMP  src-ip     ACTIVE   2

Device Group                                        VRF-Name
--------------------------------------------------- -------------
Dev-A


Route Map                      Interface    Status Track_id
------------------------------ ------------ ------ ---------
Service-A_itd_pool             Eth7/45      UP       3

  Node  IP              Config-State Weight Status     Track_id  Sla_id
  ----------------------- ------------ ------ ---------- --------- ---------
  1     10.10.10.9      Active       1      Peer Down    1         10001

        IP Access List
```

```
      ------------------------------------------------------------------------
      Service-A_itd_bucket_0


  Node  IP                Config-State Weight Status     Track_id  Sla_id
  ----------------------- ------------ ------ ---------- --------- ---------
  2     12.12.12.9        Active       1      OK           2         10002

      IP Access List
      ------------------------------------------------------------------------
      Service-A_itd_bucket_1
```

デバイス 2

手順 1：デバイス グループを定義します。

```
switch(config)# itd device-group dev-B
switch(config-device-group)# node ip 14.14.14.9 ---> Link to app #1
switch(config-device-group)# node ip 13.13.13.9 ---> Link to app #2
switch(config-device-group)# probe icmp
```

手順 2：ピア同期をイネーブルにして ITD サービスを定義します。

```
switch(config)# itd service-B
switch(config-itd)# device-group dev-B
switch(config-itd)# ingress interface ethernet 7/45
switch(config-itd)# peer local service service-A
switch(config-itd)# no shutdown

switch(config-itd)# show itd
Name           Probe LB Scheme  Status   Buckets
-------------- ----- ---------- -------- -------

Device Group                                        VRF-Name
-------------------------------------------------- -------------
Dev-B


Route Map                      Interface    Status Track_id
------------------------------ ------------ ------ ---------
Service-B_itd_pool             Eth7/45      UP       3

  Node  IP                Config-State Weight Status       Track_id  Sla_id
  ----------------------- ------------ ------ ----------   --------- ---------
  1     14.14.14.9        Active       1      Probe Failed    3         10003

      IP Access List
      ------------------------------------------------------------------------
      Service-B_itd_bucket_0


  Node  IP                Config-State Weight Status     Track_id  Sla_id
  ----------------------- ------------ ------ ---------- --------- ---------
  2     13.13.13.9        Active       1      OK           4         10004

      IP Access List
      ------------------------------------------------------------------------
      Service-B_itd_bucket_1
```

設定例：Firewall on a Stick

ITD サービス

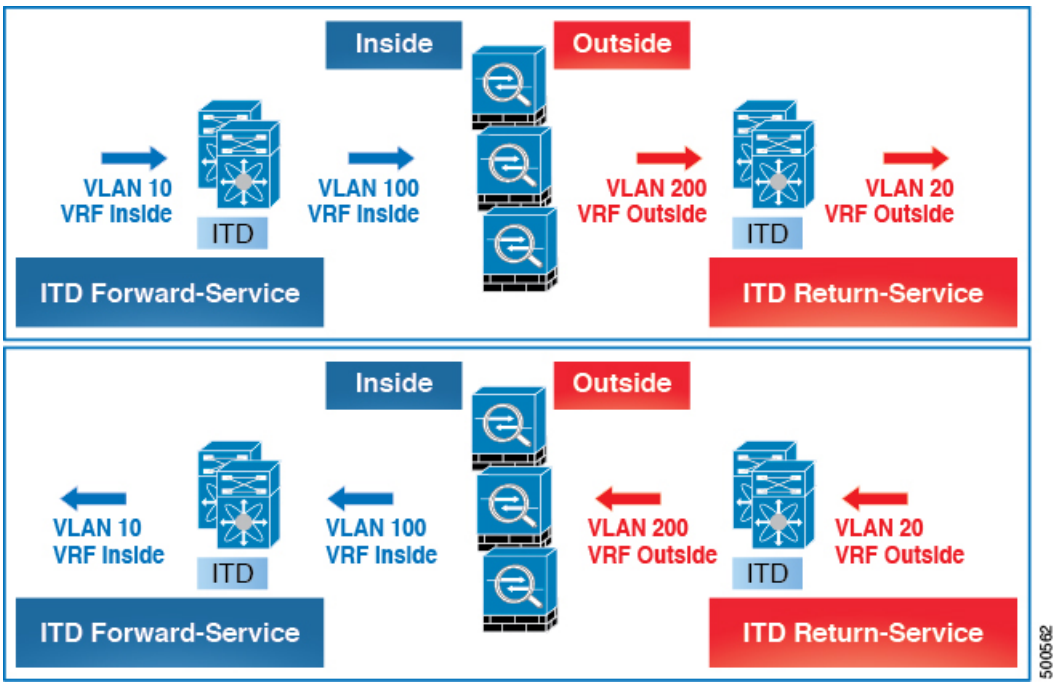
ITD サービスの設定では、トラフィック フローの特定の方向の ITD トラフィック分散を定義します。両方向のフローをリダイレクトする必要がある場合は、次のように 2 つの ITD サービスを設定する必要があります。フォワード トラフィック フローに 1 つ、リターン トラフィック フローに 1 つ。ASA には異なる内部および外部インターフェイス IP アドレスがあるため、2 つの異なるデバイス グループを設定して、対応する内部および外部 IP アドレスも指定する必要があります。

ASA VLAN

ITD のフォワードおよびリターン サービスは Nexus スイッチ上の内部および外部 VLAN SVI に接続されます。ファイアウォールなどのセキュリティ アプリケーションはすべてのトラフィックを調査する必要があるため、サービスではトラフィック フィルタリングが設定されません。その結果として、SVI にヒットするトラフィックは、いずれも対応する ASA インターフェイスにリダイレクトされます。

ASA インターフェイスをスイッチと同じ VLAN に設定すると、そのスイッチ上の別の VLAN に ITD サービスが存在するため、ファイアウォールからスイッチへのトラフィックは ASA にリダイレクトされます。したがって、ファイアウォールと Nexus スイッチの間でトラフィックがループしないように個別の VLAN のペアが必要です。

図 *12*： *ITD ASA* 展開



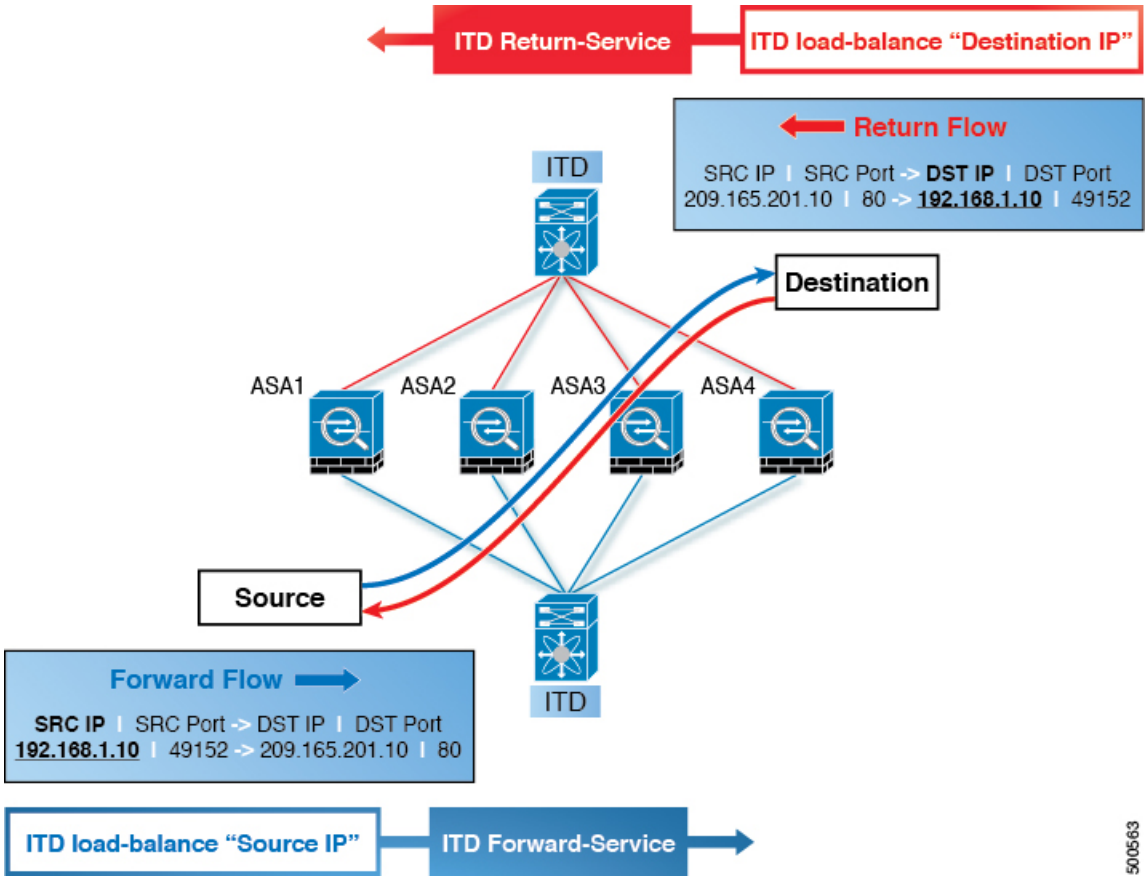
この図に示すVLAN 10および20は、ネットワーク上の送信元と宛先への内部および外部インターフェイスです。VLAN 100および200はループフリー トラフィックを実現するためにASAに対して使用されます。

フローの対称性

通常、ファイアウォールはフォワードとリターンの両方向のトラフィック フローを検査します。検査の性質がステートフルであるため、一般的に非クラスタ化ファイアウォールの通常の動作中はフローの対称性が維持される必要があります。クラスタ化ファイアウォールであっても、トラフィック フローの非対称性はクラスタ制御リンクでフローリダイレクションが増加する原因になります。非対称フローが増加するとファイアウォールに不要なオーバーヘッドが発生し、パフォーマンスに悪影響が及びます。

フローの対称性は、ITDアルゴリズムが持つ固有IPの持続性と決定性という性質を使用して実現できます。ファイアウォールの一般的なITD設定では、フォワード フローとリターン フローに1つずつITDサービスを使用します。この2つのITDサービスをロード バランシング パラメータの値が両方のサービスで一致するように設定すると、フローの対称性が維持されます。

図 *13*： *ITD ASA* 展開でのフローの対称性

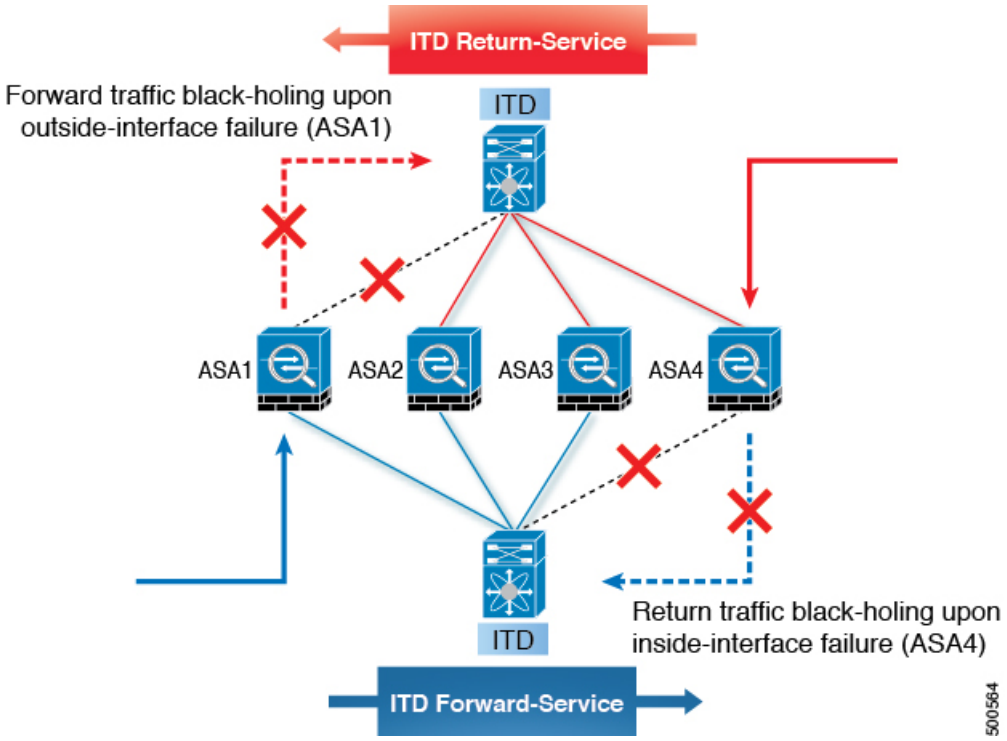


この図は、フォワード フローの送信元 IP アドレスとリバース フローの宛先 IP アドレスが一定に保たれる仕組みを示しています。各 ITD サービスに対して適切なパラメータを選択すると、ITD の IP の持続性によってフローの対称性が確保されます。

リンク障害

ASA の内部または外部インターフェイスに障害が発生すると、トラフィックの出力インターフェイスがダウンするため、その ASA の反対側に着信するトラフィックが失われる可能性があります。ITD ピア スイッチ ノードの状態同期機能では、ITD から ASA のリモート側を削除して、スイッチ間でノード状態を同期することでこの問題を解決できます。

図 *14*： *ASA* 障害のシナリオ



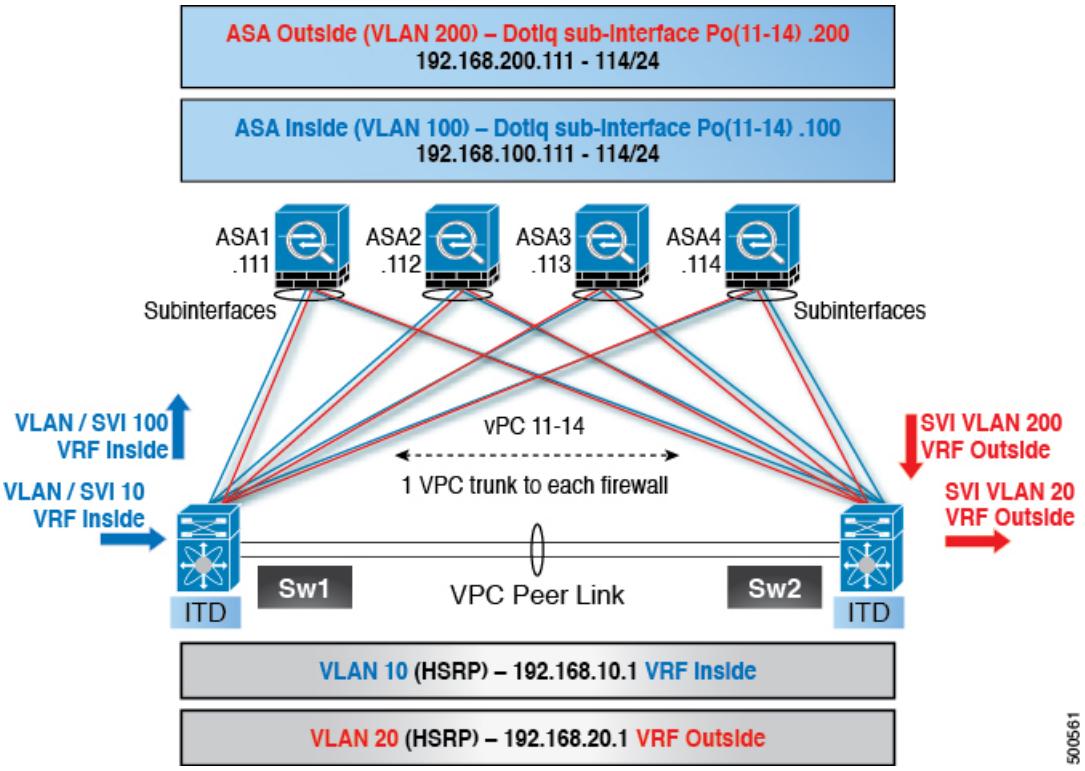
ITD ピア スイッチ ノードの状態同期機能は、デュアルスイッチの非 vPC（または単一スイッチ）トポロジでのみサポートされます。クラスタリングはこのような障害が発生した場合にASAを完全にダウンさせるので、ASA クラスタリングでもこの問題は解決されます。Firewall on a Stick 実装（単一のリンクまたは vPC）では、ASA の内部および外部インターフェイスは同じ物理（または仮想）インターフェイスに属しているため、この問題に対応できません。

設定例

Firewall on a Stick 展開では、ASA とスイッチの接続に通常は vPC ポートチャネル（または単一ポート）トランクが使用されます。この設定では、内部および外部インターフェイスは dot1q サ

ブインターフェイス（VLAN 100 および 200）です。スイッチには内部および外部コンテキストにそれぞれ 2 つの VLAN または SVI があり、インターフェイス間で物理ポートを分割しません。

図 *15*： *Firewall on a Stick*（*vPC* を使用）展開



手順 1：スイッチを設定します。

（注） 次に、スイッチ Sw1 の部分的な設定の例を示します。設定は、適切な方法ですべての ASA に対して同様に拡張する必要があります。他の機能はすでに設定されていると仮定します。

```
interface vlan 10
  description Inside_Vlan_to_Network
  vrf member INSIDE
  ip address 192.168.10.10/24
  hsrp 10
    ip address 192.168.10.1

interface vlan 20
  description Outside_Vlan_to_Network
  vrf member OUTSIDE
  ip address 192.168.20.10/24
  hsrp 20
    ip address 192.168.20.1

interface vlan 100
  description Inside_Vlan_to_ASA
  vrf member INSIDE
  ip address 192.168.100.10/24
  hsrp 100
    ip address 192.168.100.1
```

```
interface vlan 200
  description Outside_Vlan_to_ASA
  vrf member OUTSIDE
  ip address 192.168.200.10/24
  hsrp 200
    ip address 192.168.200.1

interface port-channel 11
  description VPC_TO_ASA1
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  vpc 11
  no shutdown

interface ethernet 4/25
  description Link_To_ITD-ASA-1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  channel-group 11 mode active
  no shutdown

interface port-channel 41
  description Downstream_vPC_to_network
  switchport mode trunk
  switchport trunk allowed vlan 10,20
  vpc 41
  no shutdown

interface ethernet 5/1-4
  description Downstream_vPC_member
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20
  channel-group 41
  no shutdown


itd device-group FW_INSIDE
    #Config Firewall Inside interfaces as nodes
  node ip 192.168.100.111
  node ip 192.168.100.112
  node ip 192.168.100.113
  node ip 192.168.100.114
probe icmp frequency 5 timeout 5 retry-count 1

itd device-group FW_OUTSIDE
    #Config Firewall Outside interfaces as nodes
  node ip 192.168.200.111
  node ip 192.168.200.112
  node ip 192.168.200.113
  node ip 192.168.200.114
probe icmp frequency 5 timeout 5 retry-count 1

itd INSIDE
  vrf INSIDE
    #applies ITD service to VRF 'INSIDE'
  device-group FW_INSIDE
    #FW inside interfaces attached to service.
  ingress interface vlan 10
    #applies ITD route map to vlan 1101 interface
  failaction node reassign
    #To use the next available Active FW if an FW goes offline
  load-balance method src ip buckets 16
    #distributes traffic into 16 buckets
    #load balances traffic based on Source IP.
    #OUTSIDE service uses Dest IP.
  no shut

itd OUTSIDE
  vrf OUTSIDE
    #applies ITD service to VRF 'OUTSIDE'
```

```
  device-group FW_OUTSIDE
  ingress interface vlan 20
  failaction node reassign
  load-balance method dst ip buckets 16
    #load balances traffic based on Dest IP.
    #INSIDE service uses Src IP.
  no shut
```

手順 2：ASA を設定します。

```
interface port-channel 11
  nameif aggregate
  security-level 100
  no ip address

interface port-channel 11.100
  description INSIDE
  vlan 100
  nameif inside
  security-level 100
  ip address 192.168.100.111 255.255.255.0

interface port-channel 11.200
  description OUTSIDE
  vlan 200
  nameif outside
  security-level 100
  ip address 192.168.200.111 255.255.255.0

same-security-traffic permit inter-interface

interface TenGigabitEthernet 0/6
  description CONNECTED_TO_SWITCH-A-VPC
  channel-group 11 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/7
  description CONNECTED_TO_SWITCH-B-VPC
  channel-group 11 mode active
  no nameif
  no security-level
```

次の項目がこのトポロジ例に適用されます。

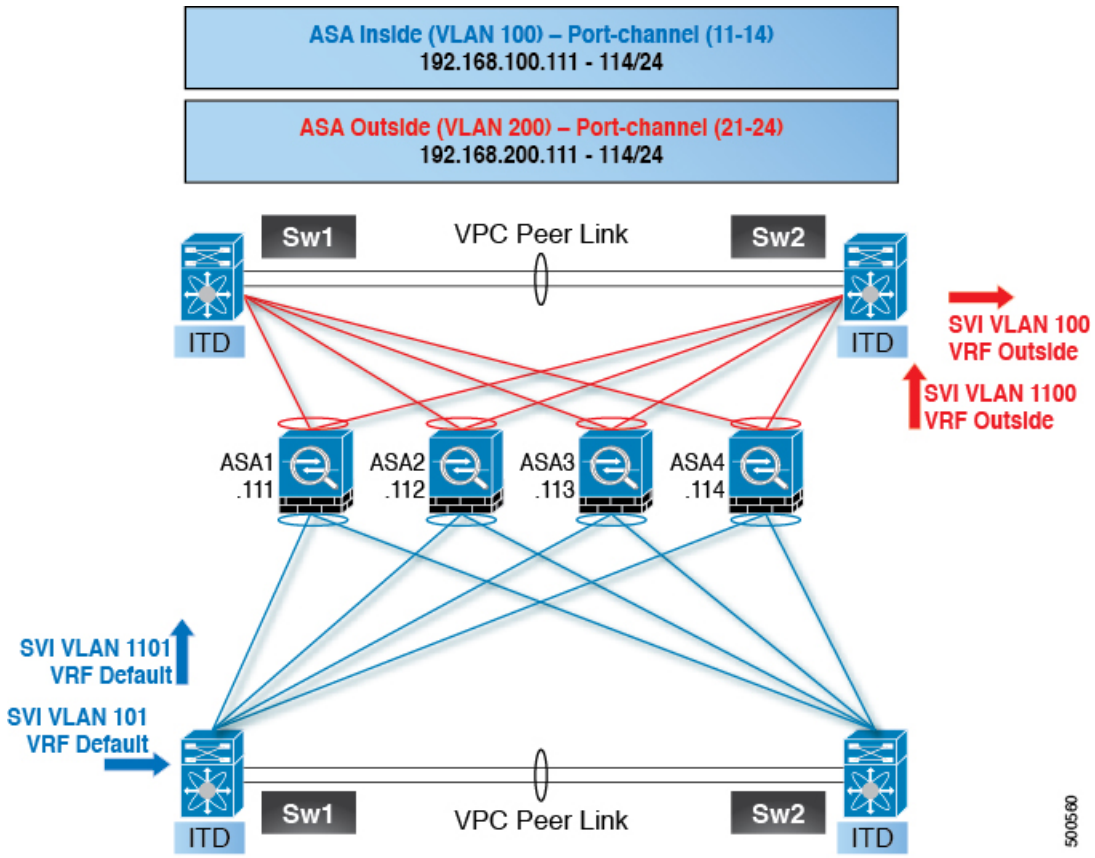
- VLAN 10、20、100、および 200 とそれぞれの SVI を適切な VRF にマップします。
- この例では、ITD のロード バランシング設定を使用してフローの対称性を実現します。
- vPC のシナリオでは、vPC のいずれかのメンバーが動作している限り、ITD は変更されません。vPC レッグに障害が発生したスイッチ上の ITD リダイレクションは、一般的な vPC 展開と同様にピア リンク経由でピア スイッチを通過します。
- このトポロジでは、内部および外部インターフェイスが ASA 上の同じ物理インターフェイスまたは仮想インターフェイス（dot1q サブインターフェイス）に関連付けられているため、物理リンク障害によってトラフィックが失われることはありません。
- vPC を介したルーティング プロトコルのネイバーをサポートするには、vPC ドメイン内で **layer3 peer-router** コマンドを設定する必要があります。
- 内部と外部の両方のファイアウォール インターフェイスへの接続にレイヤ 3 インターフェイスが使用されるため、VRF が必要です。特定の状況でトラフィックがファイアウォールを迂回してルーティング（VLAN 間）しないように、VRF を設定します。

- トラフィックはポリシーベース ルーティングを使用して ASA に転送されるため、ルートは必要ありません。

設定例：vPC を使用したデュアルスイッチ サンドイッチ モードのファイアウォール

vPC を使用したサンドイッチ モードの場合、内部および外部 ASA インターフェイスはそれぞれ別のポートチャネル バンドルに割り当てられます。vPC を使用することで、1 つのリンクに障害が発生してもトラフィック フローは妨げられません。ITD はピア スイッチのリンクを介して ASA への転送を続行します。

図 *16*： *vPC* を使用したデュアルスイッチ サンドイッチ モード



手順 1：2 台のスイッチを設定します。

```
switch #1:
interface vlan 10
  description INSIDE_VLAN
  ip address 192.168.10.10/24

interface vlan 100
  description FW_INSIDE_VLAN
  ip address 192.168.100.10/24
```

```
interface port-channel 11
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  vpc 11

interface ethernet 4/1
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  channel-group 11 mode active


switch #2:
interface vlan 20
  description OUTSIDE_VLAN
  ip address 192.168.20.10/24

interface vlan 200
  description FW_OUTSIDE_VLAN
  ip address 192.168.200.10/24

interface port-channel 21
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  vpc 11

interface ethernet 4/25
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  channel-group 21 mode active
```

手順 2：ASA を設定します。

```
interface port-channel 11
  description INSIDE
  vlan 100
  nameif inside
  security-level 100
  ip address 192.168.100.111 255.255.255.0

interface port-channel 21
  description OUTSIDE
  vlan 100
  nameif outside
  security-level 100
  ip address 192.168.200.111 255.255.255.0

same-security-traffic permit inter-interface

interface TenGigabitEthernet 0/6
  description CONNECTED_TO_SWITCH-A-VPC
  channel-group 11 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/7
  description CONNECTED_TO_SWITCH-B-VPC
  channel-group 11 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/8
  description CONNECTED_TO_SWITCH-A-VPC
  channel-group 21 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/9
  description CONNECTED_TO_SWITCH-B-VPC
```

```
channel-group 21 mode active
no nameif
no security-level
```

次の項目がこのトポロジ例に適用されます。

- この例では、ITD のロード バランシング設定を使用してフローの対称性を実現します。
- vPC のシナリオでは、vPC のいずれかのメンバーが動作している限り、ITD は変更されません。vPC レッグに障害が発生したスイッチ上の ITD リダイレクションは、一般的な vPC 展開と同様にピア リンク経由でピア スイッチを通過します。
- このトポロジでは、ASA 上のいずれかのポート チャネル（または非 vPC トポロジの単一の物理リンク）に障害が発生すると、トラフィックが損失する可能性があります。
- vPC を介したルーティング プロトコルのネイバーをサポートするには、vPC ドメイン内で **layer3 peer-router** コマンドを設定する必要があります。
- トラフィックはポリシーベース ルーティングを使用して ASA に転送されるため、ルートは必要ありません。

設定例：レイヤ 3 クラスタリングのファイアウォール

ASA クラスタは、1 つのユニットとして機能する複数の ASA から構成されます。複数の ASA を単一の論理デバイスとしてグループ化すると、単一のデバイスの利便性（管理、ネットワークへの統合）を得られる上に、複数デバイスによる高いスループットおよび冗長性が実現します。

ITD は個々のモード レイヤ 3 ASA クラスタを対象にロード バランスを実行できます。ITD は各ファイアウォールによって処理されるフローの予測を実現するので、クラスタリングを補完します。OSPF ECMP およびポートチャネル ハッシュ アルゴリズムを利用する代わりに、ITD バケットを使用してこれらのフローを特定できます。

レイヤ 3 クラスタを使用すると、バケットの割り当てに基づいてフロー オーナーを事前に特定できます。通常、ITD およびレイヤ 3 クラスタリングを利用せずに最初のオーナー選択を予測することは不可能です。ITD を使用すると、オーナーを事前に特定できます。

ASA クラスタリングでもバックアップ フロー オーナーが使用されます。クラスタ内の特定のファイアウォールを通過するすべてのフローに対して、別のファイアウォールはそのフローの状態とオーナー ASA を保存します。実際のアクティブなフロー オーナーに障害が発生すると、ITD の Failaction 再割り当てによって、障害のあるオーナー ASA からのすべてのフロー（バケット）はデバイス グループにリストされている次のアクティブ ノードに転送されます。このトラフィックを受信する新しいファイアウォールが受信フローのバックアップ オーナーではない場合、このファイアウォールはバックアップ オーナーからフロー状態の情報を受け取って、トラフィックをシームレスに処理する必要があります。

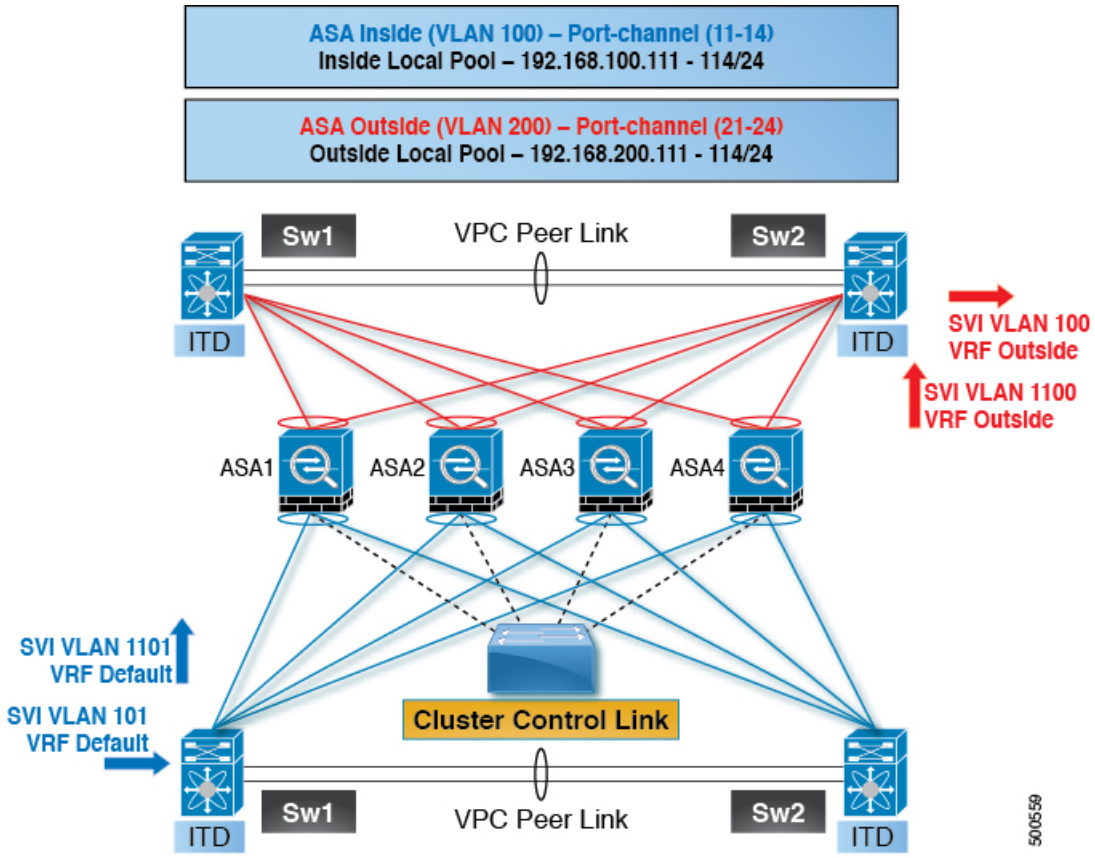
ITD で ASA クラスタリングを使用する際の潜在的な欠点は、バックアップ フローおよび他のクラスタ テーブルの動作により、非クラスタ化ファイアウォールでは消費しないメモリと CPU リソースが消費されることです。したがって、非クラスタ化ファイアウォールを使用すると、ファイアウォールのパフォーマンスが向上する可能性があります。

次の表に、ASA デバイスのステータスが変化したときのクラスタ制御リンク（CCL）に対する影響について、ECMP と ITD を比較した概要を示します。

表 *2*：*ECMP* 対 *ITD*：*CCL* に対する影響の比較概要

ASA ステータス	ITD	ECMP
安定状態	CCL および予想されるトラフィック タイプでの最小トラフィック。 ライン カード タイプおよびスイッチに関係なく完全に同じ負荷分散。	すべての場所で同じライン カード タイプとスイッチ モデルが使用されている場合は CCL での最小トラフィック。 異なるハードウェアが使用されていると、非対称のレベルが高くなって CCL ネットワーク上にトラフィックが発生する可能性があります。ハードウェアごとにハッシュ関数が異なります。 2 台のスイッチ（vPC 環境など）によって同じフローが異なる ASA デバイスに送信され、CCL トラフィックが発生する可能性があります。
単一 ASA 障害	CCL 上に追加トラフィックは発生しません。 ITD は IP スティッキ性および復元ハッシュを提供します。	すべてのフローが再ハッシュされ、追加のトラフィック リダイレクションが CCL で発生します。クラスタ内のすべての ASA デバイスへのトラフィックに影響する場合があります。
単一 ASA リカバリ	クラスタ内の 2 台の ASA デバイス（バケットを受信する回復した ASA とそのバケットを以前に処理した ASA）間の CCL でトラフィック リダイレクションが発生する可能性があります。	追加のトラフィック リダイレクションが CCL で発生する可能性があります。クラスタ内のすべての ASA デバイスへのトラフィックに影響する場合があります。
ASA の追加	CCL 上に最小の追加トラフィック。	すべてのフローが再ハッシュされ、追加のトラフィック リダイレクションが CCL で発生します。クラスタ内のすべての ASA デバイスへのトラフィックに影響する場合があります。

図 *17*：*vPC* を使用したデュアルスイッチ サンドイッチによる *ASA* クラスタ



手順 1：2 台のスイッチを設定します。

（注） クラスタリングを導入しても ITD 設定は変わりません。ITD 設定はトポロジのタイプによって異なります。この例では、vPC トポロジを使用したデュアルスイッチ サンドイッチと同じ設定です。

```
switch #1:
interface vlan 10
  description INSIDE_VLAN
  ip address 192.168.10.10/24

interface vlan 100
  description FW_INSIDE_VLAN
  ip address 192.168.100.10/24

interface port-channel 11
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  vpc 11

interface ethernet 4/1
```

```
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  channel-group 11 mode active


switch #2:
interface vlan 20
  description OUTSIDE_VLAN
  ip address 192.168.20.10/24

interface vlan 200
  description FW_OUTSIDE_VLAN
  ip address 192.168.200.10/24

interface port-channel 21
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  vpc 11

interface ethernet 4/25
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  channel-group 21 mode active
```

手順 2：ASA を設定します。

```
cluster group ASA-CLUSTER-L3
  local-unit ASA1
  cluster-interface port-channel 31
  ip address 192.168.250.100 255.255.255.0
  piority 1
  health-check holdtime 1.5
  clacp system-mac auto system-priority 1
  enable

mac-address pool MAC-INSIDE aaaa.0101.0001 - aaaa.0101.0008
mac-address pool MAC-OUTSIDE aaaa.0100.0001 - aaaa.0100.0008
ip local pool IP-OUTSIDE 192.168.200.111-192.168.200.114
ip local pool IP-INSIDE 192.168.100.111-192.168.100.114

interface port-channel 11
  description INSIDE
  lacp max-bundle 8
  mac-address cluster-pool MAC-INSIDE
  nameif inside
  security-level 100
  ip address 192.168.100.11 255.255.255.0 cluster-pool IP-INSIDE

interface port-channel 21
  description OUTSIDE
  lacp max-bundle 8
  mac-address cluster-pool MAC-OUTSIDE
  nameif outside
  security-level 100
  ip address 192.168.200.11 255.255.255.0 cluster-pool IP-OUTSIDE

interface port-channel 31
  description Clustering Interface
  lacp max-bundle 8

interface TenGigabitEthernet 0/6
  channel-group 11 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 0/7
  channel-group 11 mode active
  no nameif
  no security-level
```

```
  no ip address

interface TenGigabitEthernet 0/8
  channel-group 21 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 0/9
  channel-group 21 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 1/0
  channel-group 31 mode on
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 1/1
  channel-group 31 mode on
  no nameif
  no security-level
  no ip address
```

この例では、ポート チャネル 11 と 21 は内部および外部インターフェイスで使用されます。ポートチャネル31はクラスタリング インターフェイスです。個別インターフェイスは通常のルーテッド インターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メインクラスタIPアドレスは、そのクラスタのための固定アドレスであり、常に現在のマスター ユニットに属します。同様に MAC アドレス プールも設定され、対応する内部または外部ポート チャネルで使用されます。

関連資料

関連項目	マニュアル タイトル
IP SLA	『*Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide*』