導入とベスト プラクティス

設計および導入の考慮事項

ここでは、ITD の設計および導入に関する考慮事項について説明します。

ITD サービスの数

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。フローの両方向でリダイレクトが必要な場合は、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 には別々の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 アドレスを指定する必要があります。

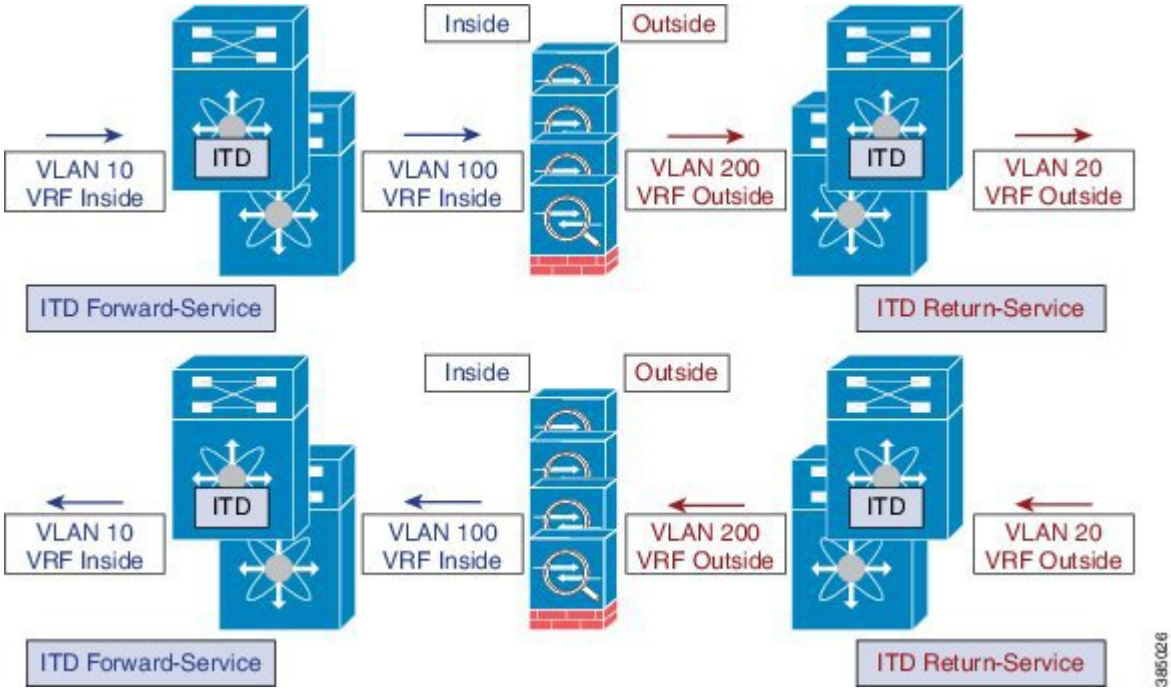
追加 ASA VLAN

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 アプリケーションをイネーブルにすると、すべてのトラフィックを調査する必要があり、サービスでトラフィック フィルタリングは設定しません。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 インターフェイスがスイッチの場合と同じ VLAN に設定されている場合、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に戻るトラフィック

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のペアを使用する必要があります。

図 *1*： *ITD-ASA* 展開の論理ビュー



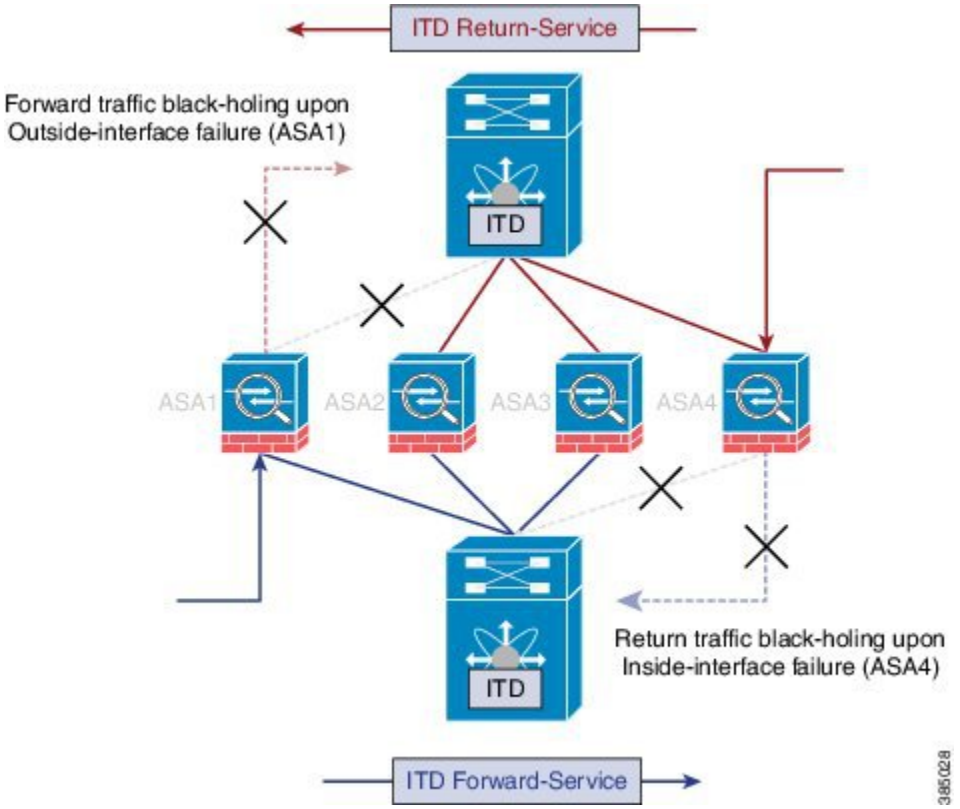
上記の例では、VLAN 10およびVLAN 20がネットワーク上の送信元と宛先への内部および外部インターフェイスの役目を担っており、VLAN 100およびVLAN 200はループフリー トラフィックを可能にするためにASAに対して使用されています。

リンク障害のシナリオ

ASAの内部または外部インターフェイスのいずれか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はブラックホール

化されます。ITD ピア VDC ノード状態同期機能は、VDC 間でノード状態を同期することで ITD から ASA のリモート側を削除するという方法によりこの問題を解決します。

図 *2*：ピア *VDC* 同期を使用しない場合の *ASA* 障害のシナリオ



ITD ピア VDC ノード状態同期機能は、デュアル VDC 非 vPC 単一スイッチ トポロジでのみ現在サポートされています。このような障害が発生した場合にクラスタリングでは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が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、この問題は発生しません。

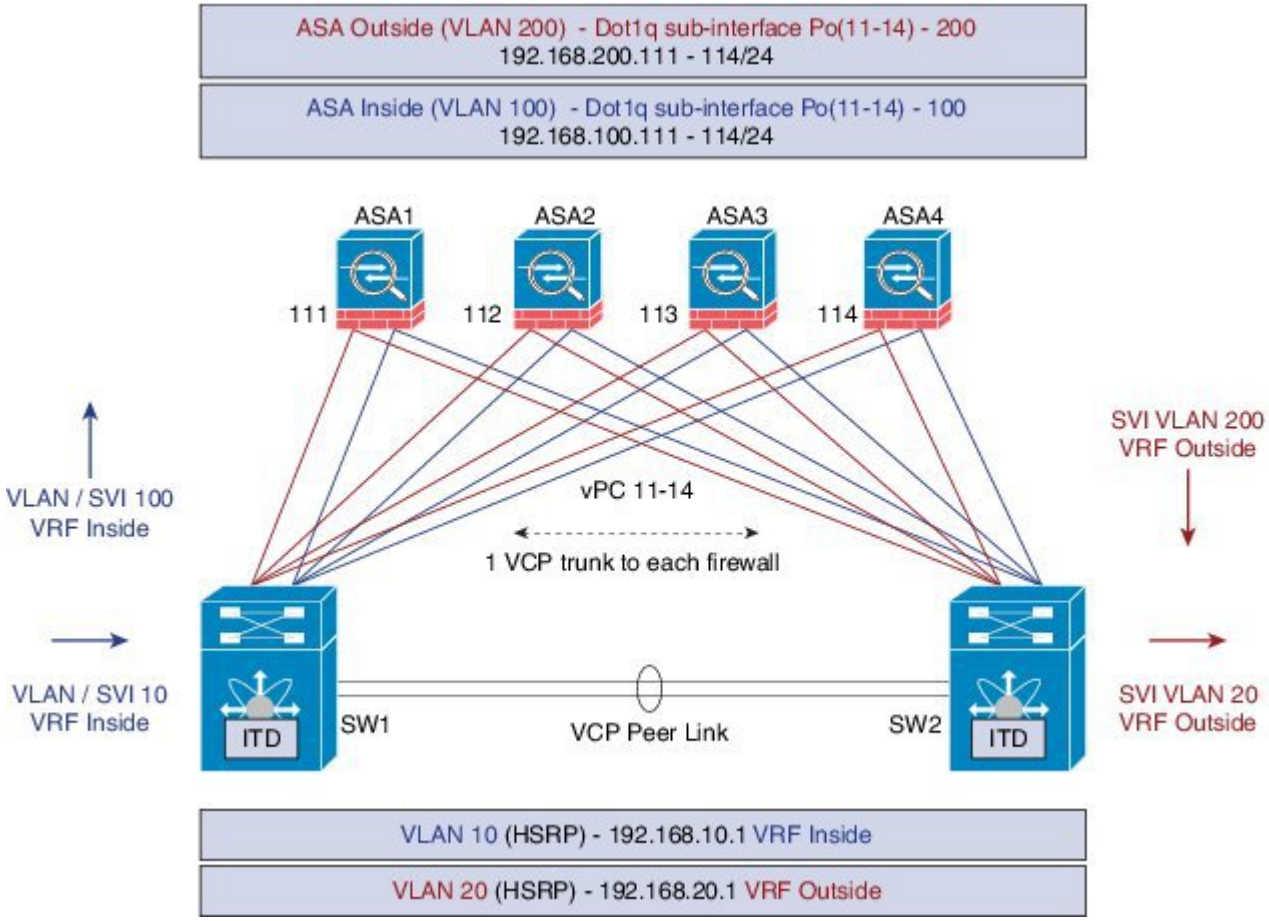
ITD ASA の展開

設定例：Firewall on a Stick

Firewall on a Stick 展開では、ASA とスイッチの接続に 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。次の図を参照してください。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、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 *3*： *vPC* を使用した *Firewall on a Stick*



以下は Nexus 7000 の設定例の抜粋です。この例ではスイッチ（sw1）の設定の一部を示します。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 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 192.168.20.1

interface vlan100
description Inside_Vlan_to_ASA
```

```
vrf member INSIDE
ip address 192.168.100.10/24
hsrp 100
ip 192.168.100.1

interface vlan200
description Outside_Vlan_to_ASA
vrf member OUTSIDE
ip address 192.168.200.10/24
hsrp 200
ip 192.168.200.1

.............................

interface Port-Channel111
 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-Channel41
 description Downstream_vPC_to_Network
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 vpc 41
 no shutdown

interface Port-Channel 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 192.168.100.111
   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 INSIDE
 vrf INSIDE
  #applies ITD service to VRF "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 a 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 Dst-IP
no shutdown

itd OUTSIDE
 vrf OUTSIDE
  #applies ITD service to VRF "OUTSIDE"
device-group FW_OUTSIDE
ingress interface Vlan 10
failaction node reassign
load-balance method dst ip buckets 16
#distributes traffic into 16 buckets
#load balances traffic based on Destination-IP.
#OUTSIDE service uses Dst-IP
no shutdown
```

以下は ASA の設定の抜粋です。次に示す ASA 側の設定は 1 つの ASA（ASA-1）の設定です。同様の設定を他のすべての ASA に拡張する必要があります。

```
interface Port-Channel11
 nameif aggregate
 security-level 100
 no ip address
!
interface Port-Channel11.100
 description INSIDE
 vlan 100
 nameif inside
 security-level 100
 ip address 192.168.100.111 255.255.255.0
!
interface Port-Channel11.200
 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 TenGigabitEthernet0/6
 description CONNECTED_TO_SWITCH_A_VPC
 channel-group 11 mode active
 no nameif
 no security-level

interface TenGigabitEthernet0/7
 description CONNECTED_TO_SWITCH_B_VPC
 channel-group 11 mode active
 no nameif
 no security-level
!
```

上記の設定とトポロジでは次の点に注意してください。

- VLAN 10、20、100、200、およびそれぞれの SVI の適切な VRF へのマッピング。
- ASA（内部および外部）に対する ITD デバイスグループの設定。
- フローの対称性を実現する ITD ロードバランシング設定。
- vPC のシナリオでは、vPC メンバーのいずれか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 の場合と同様にピアリンク経由でピアスイッチを通過します。

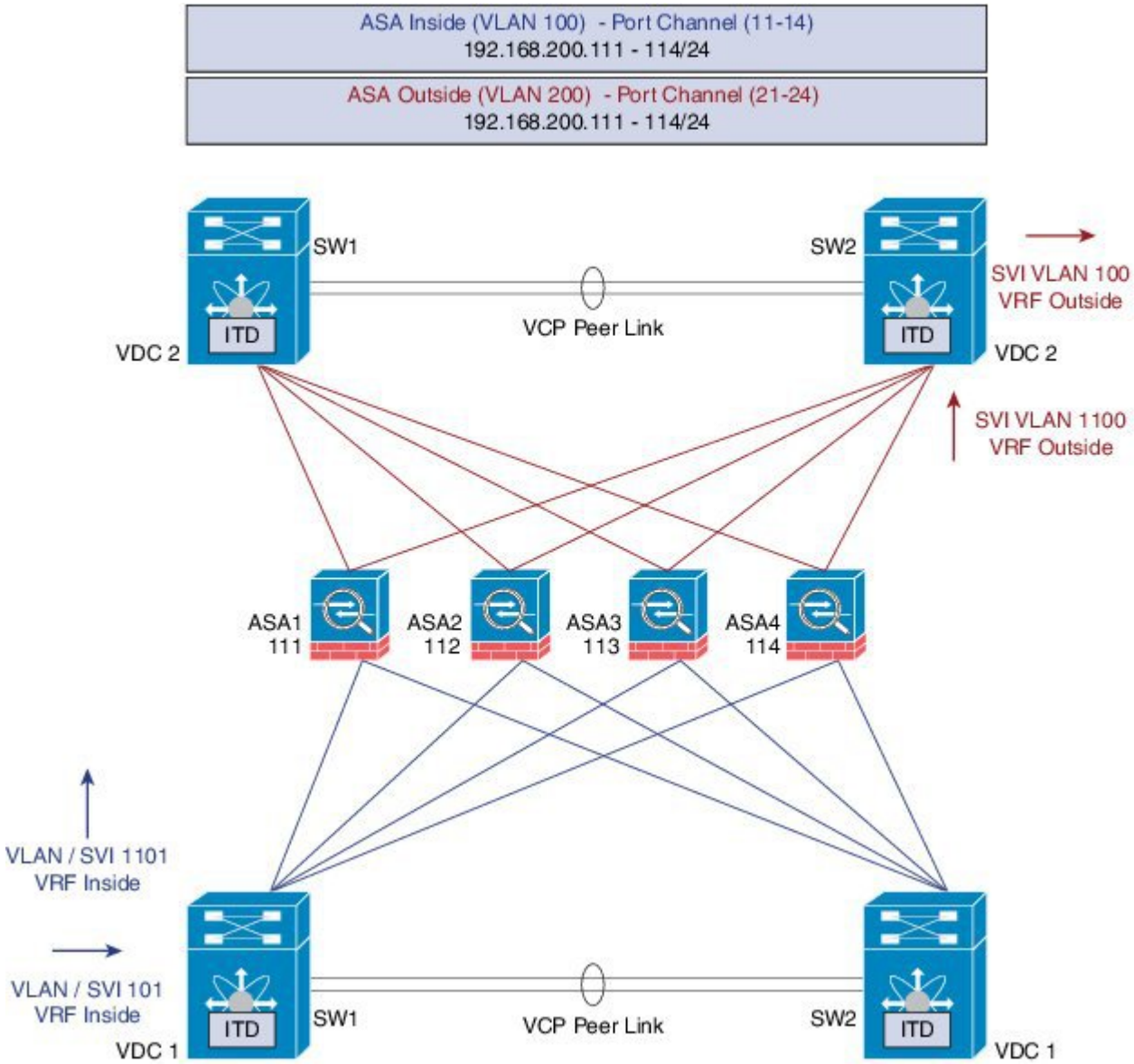
- このトポロジおよび展開方式では、内部および外部インターフェイスが ASA 上の同じ物理または仮想インターフェイス（dot1q サブインターフェイス）に関連付けられているため、物理リンク障害が発生してもトラフィックはブラックホール化されません。
- vPC を介したルーティング プロトコル ネイバーシップをサポートするには（Cisco NX-OS 7.2(0)D1(1) 以降のリリース）、vPC ドメイン内で **layer3 peer-router** コマンドを設定する必要があります。
- 内部と外部の両方のファイアウォール インターフェイスへの接続にレイヤ 3 インターフェイスが使用されるため、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 PBR を介して ASA に転送されるので、ルートは必要ありません。

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

vPC を使用するサンドイッチ モードでは、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。次の図にこのトポロジを示します。なお、Nexus 7000 は現時点でノード状態同期機能をサポートしていません。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。vPC を使用した他のシナリオと同様に、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 *4*：*vPC* を使用したデュアル *VDC 2* スイッチ サンドイッチ モードのファイアウォール



Nexus 7000 での設定手順

単一スイッチ トポロジとこのトポロジの主な違いは、Nexus スイッチと ASA の間に単一リンクではなく vPC ポートチャネルが存在する点です。さらに、前述の例と同じく、スイッチの内部および外部インターフェイスは別の VDC に設定されます。

以下は VDC1 の設定です。

```
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-Channel11
 description To_ASA-1-INSIDE
 switchport mode access
 switchport access vlan 100
 vpc 11

interface Ethernet4/1
 description To_ASA-1-INSIDE
 switchport mode access
 switchport access vlan 100
 channel-group 11 mode active
```

以下は VDC2 の設定です。

```
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-Channel21
 description To_ASA-1-OUTSIDE
 switchport mode access
 switchport access vlan 200
 vpc 11

interface Ethernet4/25
 description To_ASA-1-OUTSIDE
 switchport mode access
 switchport access vlan 200
 channel-group 21 mode active
```

ASA での設定手順

以下は ASA の設定の抜粋です。

```
interface Port-Channel11
 description INSIDE
 vlan 100
 nameif inside
 security-level 100
 ip address 192.168.100.111 255.255.255.0

interface Port-Channel21
 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 TenGigabitEthernet0/6
 description CONNECTED_TO_SWITCH0-A-VPC
 channel-group 11 mode active
 no nameif
 no security-level

interface TenGigabitEthernet0/7
 description CONNECTED_TO_SWITCH-B-VPC
```

```
 channel-group 11 mode active
 no nameif
 no security-level

interface TenGigabitEthernet0/8
 description CONNECTED_TO_SWITCH-A-VPC
 channel-group 21 mode active
 no nameif
 no security-level

interface TenGigabitEthernet0/9
 description CONNECTED_TO_SWITCH-B-VPC
 channel-group 21 mode active
 no nameif
 no security-level
```

上記の設定とトポロジでは次の点に注意してください。

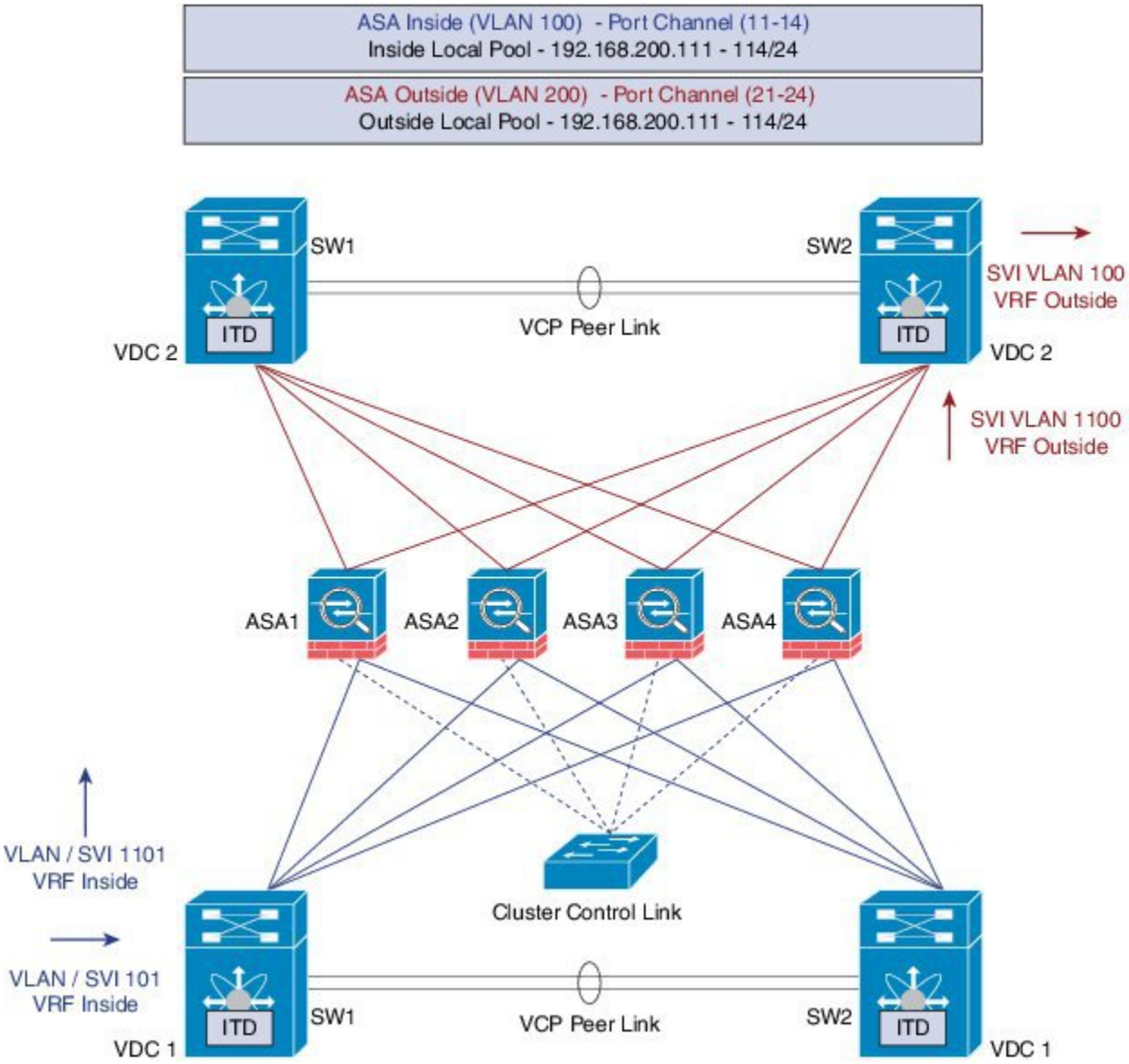
- フローの対称性を実現する ITD ロードバランシング設定。
- vPC のシナリオでは、vPC メンバーのいずれかが動作している限り、ITD は変更されません。vPC レッグに障害が発生したスイッチ上の ITD リダイレクションは、一般的な vPC の場合と同様にピアリンク経由でピアスイッチを通過します。
- このトポロジまたは展開方式では、ASA 上のいずれかのポート チャネルまたは非 VPC での単一の物理リンクに障害が発生すると、トラフィックのブラックホール化が発生する可能性があります。
- Cisco NX-OS 7.2(0)D1(1) 以降のリリースで、vPC を介したルーティング プロトコル ネイバーシップ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 PBR を介して 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、管理およびネットワークへの統合という点で単一

のデバイスの利便性を得られる上に、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。次の図を参照してください。

図 *5*：*vPC* を使用したデュアル *VDC* サンドイッチによる *ASA* クラスタ



ACL クラスタリング

次の表は、ASA デバイスのステータスが変化したときに、ECMP で発生した CCL に対する影響と ITD で発生した影響の比較結果です。

ASA ステータス	ITD	ECMP
安定状態	CCL 上の最小トラフィック。想定されているトラフィック タイプ。 ライン カードとスイッチのタイプに関係なく、全く同じ負荷分散。	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の CCL 上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場合は、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 環境内など）が同じフローを別々の ASA デバイスに送信すると、CCL トラフィックが発生します。
単一 ASA 障害	CCL 上で追加のトラフィックは発生しません。ITD は IP スティッキ性とレジリエント ハッシングを提供します。	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 上で発生します。これにより、クラスタ内のすべての ASA へのある程度のトラフィックが発生することになります。
単一 ASA リカバリ	クラスタ内の 2 台の ASA（バケットを受信するリカバリされた ASA とそのバケットが優先的に提供される ASA）間の CCL 上でトラフィック 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 上で発生する可能性があります。これにより、クラスタ内のすべての ASA へのある程度のトラフィックが発生することになります。
ASA の追加	CCL 上の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 上で発生します。これにより、クラスタ内のすべての ASA へのある程度のトラフィックが発生することになります。

ITD は個々のモード レイヤ 3（L3）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 バケットによってフローを特定します。

L3 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 L3 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が、ITD を使用すれば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 オーナーの実装が使用されます。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 からのバケットに含まれるすべてのフローはデバイス 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適切なバックアップ 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。詳細については、『Cisco ASA Series CLI Configuration Guide, 9.0』を参照してください。

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。ただし、ASA クラスタ メンバーに障害が発生しても既存の接続がタイムアウトしないという確証は、お客様にとって非常に価値があると考えられます。

Nexus 7000 での設定手順

クラスタリングを導入しても ITD 設定は変わりません。ITD Nexus 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 VDC サンドイッチでのファイアウォールと同じ設定です。

ITD 設定は、ノード状態同期が削除されたことを除いて以前の方法とほとんど同じです。

ASA での設定手順

ASA クラスタリングは、PBR 展開シナリオと同様に、次のマニュアルで説明されている L3 クラスタとして設定されます。ASA クラスタの設定に関する詳細情報は、次のリンクで確認できます。次に、レイヤ 3 クラスタリング トポロジのファイアウォールに対する ASA での設定例を示します。詳細については、『Cisco ASA Series CLI Configuration Guide, 9.0』を参照してください。

```
cluster group ASA-CLUSTER-L3
local-unit ASA1
cluster-interface port-channel1 ip 192.168.250.100 255.255.255.0
priority 1
health-check holdtime 1.5
clacp system-mac auto system-priority 1
enable

mac-address pool MAC-INSIDE aaaa.0101.0001 - aaa.0101.0008
mac-address pool MAC-OUTSIDE aaaa.0100.0001 - aaa.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-Channel11
 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-Channel21
 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-Channel31
 description Clustering Interface
 lacp max-bundle 8


interface TenGigabitEthernet0/6
 channel-group 11 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet0/7
 channel-group 11 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet0/8
 channel-group 21 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet0/9
channel-group 21 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet1/0
channel-group 31 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet1/1
channel-group 31 mode active
 no nameif
 no security-level
 no ip address
```

上記の設定に示すように、ポートチャネル 11 と 21 は前述の例の内部または外部インターフェイスに使用されます。ただし、クラスタリング インターフェイス用のポートチャネル 31 が追加されています。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。

設定例：WCCP タイプの ITD シナリオ

Web プロキシを使用した設計

ITD を使用した Web プロキシ導入では、Nexus スイッチがインターネット宛ての Web トラフィックの照合とプロキシ サーバに対するそのロード バランシングを担当します。

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、リダイレクトされてき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。

サービスの数

パケット フローのスライドに示すように、通常は、ITD リダイレクションが VLAN に対向するクライアントの順方向にのみ必要です。以降は、ITD リダイレクションまたは分散を使用せずに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 プロキシ導入を伴う ITD は、1 つの ITD サービスのみが必要で、これが順方向に設定されます。ただし、逆トラフィック リダイレクションの要件がある場合は、トラフィック選択を送信元 L4 ポートに基づく必要があります。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。

プロキシ ヘルス モニタリングのプローブ

Web プロキシ導入に ITD を使用する場合は、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。このことは、障害が発生したプロキシ サーバに送信されたトラフィックがブラックホール化する可能性があるため重要です。プラットフォームごとの最新リリースで現在使用可能なプローブは次のとおりです。

- Nexus 7000（7.2(1)D1(1)）：ICMP、TCP/UDP、DNS
- Nexus 5000：ICMP
- Nexus 9000：ICMP

ロードマップ：プラットフォーム全体のプローブ パリティが今後リリースされる予定です。追加の HTTP プローブについては調査中です。

（注） これらは確定されていませんが、ロードマップ項目になっています。

トラフィック選択要件

ITD のトラフィック フィルタリングまたはトラフィック選択に対して現在サポートされている方式を以下に示します。

- **仮想 IP（Nexus 5000、Nexus 6000、Nexus 7000、および Nexus 9000 でサポートされる）**：

  宛先フィールド専用のトラフィック選択（フィルタリング）に使用される IP+サブネット マスクの組み合わせ。

- **除外 ACL**：

  ITD をバイパスするトラフィックを指定するために使用される ACL。

  この ACL で許可されなかったトラフィックが ITD を通過します。

  除外 ACL 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 VIP より優先されます。

除外 ACL は許可 ACE エントリのみをサポートします。拒否 ACE は除外 ACL 上でサポートされません。

- **ポート数ベースのフィルタリング**

  "Port 80 needs ITD service" のように L4 ポートに基づいてトラフィックを選択する場合は、以下を使用して実行できるようになりました。

  - 一致する宛先ポート：VIP – 0.0.0.0 0.0.0.0 tcp 80（任意の送信元または宛先 IP、一致する宛先ポート 80）
  - 一致する送信元ポート："permit tcp any neq 80 any"（80 以外の任意のポートが ITD をバイパスし、ポート 80 はリダイレクトされる）を含む除外 ACL。
  - 一致する複数のポート番号：ITD 内の複数の VIP 回線をポートごとに 1 つずつ設定できます。

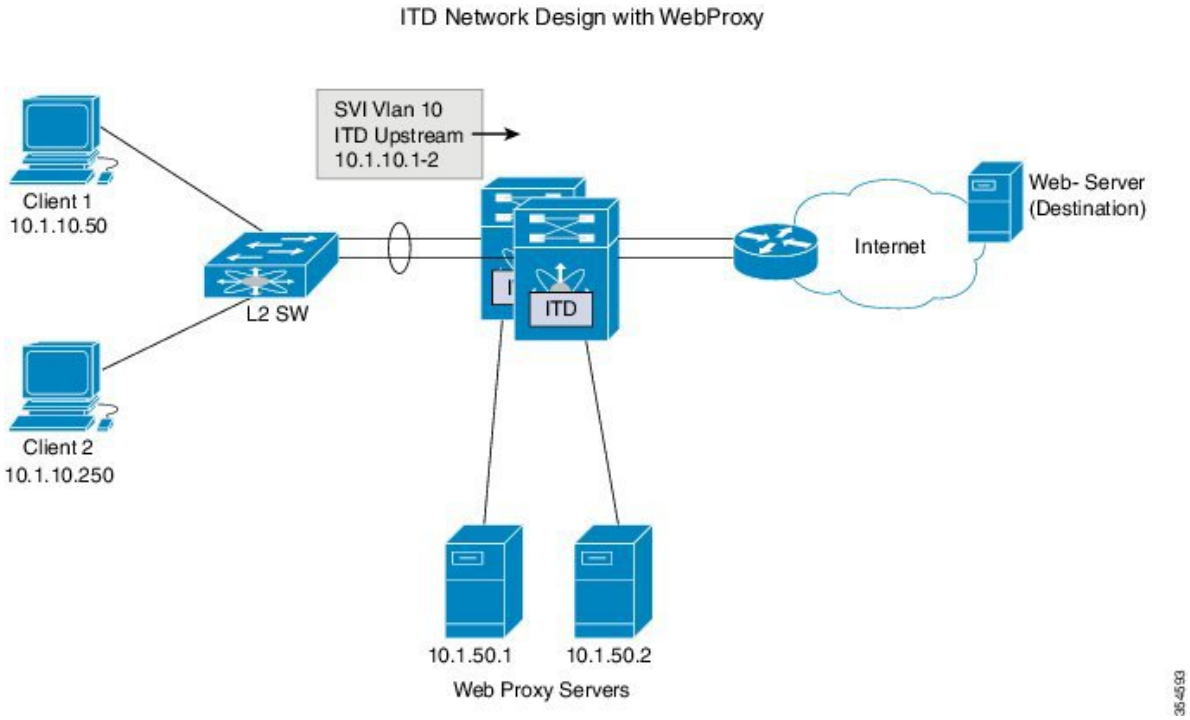
- **包含 ACL**：ロードマップ項目 - Cisco Nexus 7000 リリース 7.3(0)D1(1)、Cisco Nexus 9000 リリース 7.0(3)I3(1)

  "Port 80 needs ITD service" のように L4 ポートに基づいてトラフィックを選択する場合は、以下を使用して実行できるようになりました。

  - ITD が提供する必要のあるトラフィックを許可するために使用される包含 ACL。両方の SRCand DST フィールドを照合することができます。
  - Permit 行だけが許可されます 。一度に使用できるのは VIP と包含 ACL のどちらかで、両方を使用することはできません。
  - ロードバランシング パラメータによって、包含 ACL 内で使用可能な一致の最大長が決定されます。たとえば、発信元ベースの LB と 8 つのバケットを使用した場合に、照合可能な送信元 IP アドレスの最大マスクは /29 です。宛先 LB と 8 つのバケットを使用した場合に、照合可能な宛先 IP の最大マスクは /29 です。

（注） この包含 ACL 機能は、ロードマップ項目で、現在のリリースでは使用できません。ここで提供される情報は、一時的なもので、変更される可能性があります。

図 *6*： ***WebProxy*** を使用した ***ITD*** ネットワーク設計



上の図に示すように、インターネットへの宛先ポート 80/443（ingressVLAN10）は、Web プロキシ サーバ 10.1.50.1/10.1.50.2 に分配されます。

プライベート ネットワーク（10.0.0.0/8、192.168.0.0/16、および 172.16.0.0/20）宛ての VLAN 10 上のトラフィックはプロキシ サーバに送信されません。

```
 itd device-group Web_Proxy_Servers              <<<< Configure ITD Device-group
Web_Proxy_Servers and point to server IP addresses.
  probe icmp
  node ip 10.1.50.1
  node ip 10.1.50.2

ip access-list itd_exclude_ACL                  <<<< Configure Exclude ACL to exclude all
 traffic destined to Private IP addresses.
  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

Itd Web_proxy_SERVICE
  device-group Web_Proxy_Servers                <<<< Apply Exclude ACL.
  exclude access-list itd_exclude_ACL
  virtual ip 0.0.0.0 0.0.0.0 tcp 80             <<<< Any Traffic TO DESTINATION Port-80
redirect to group  Web_Proxy_Servers
```

```
  virtual ip 0.0.0.0 0.0.0.0 tcp 443             <<<< Any Traffic TO DESTINATION Port-443
redirect to group Web_Proxy_Servers
  ingress interface Vlan 10
  failaction node reassign
  load-balance method src ip
  no shutdown
```

リターン トラフィックのリダイレクションが必要な場合は、次の追加の設定が必要になります。

（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。除外 ACL は permit エントリのみをサポートします。

```
ip access-list itd_exclude_return            <<<< Configure Exclude ACL (Return) to exclude
 all but port 80 & 443
  10 permit tcp any range 0 79 any
  20 permit tcp any range 81 442 any
  10 permit tcp any range 444 65535 any

itd Web_proxy_SERVICE                          <<<< Configure Return ITD service for return
 traffic:
  device-group Web_Proxy_Servers
  exclude access-list itd_exclude_return      <<<< Apply Exclude ACL for Return ITD service.
  ingress interface Vlan 20                     <<<<  Internet-facing ingress interface on
the Nexus Switch.
  failaction node reassign
  load-balance method dst ip                    <<<<  Flow symmetry between forward/retrun
flow achieved by flipping LB parameter.
  no shutdown
```

上記の設定に示すように、ポートチャネル 11 と 21 は前述の例の内部または外部インターフェイスに使用されます。ただし、クラスタリング インターフェイス用のポートチャネル 31 が追加されています。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。