Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン フロー

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

このセクションのトピックでは、Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン（SAIE）フローの概要と、 Cisco SD-WAN Manager または CLI を使用してフローを設定する方法について説明します。

Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン フローの概要

Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン（SAIE）フローは、基本ヘッダー情報を過ぎたパケットを調べる機能を提供します。SAIE フローは、特定のパケット

の内容を判別し、その情報を統計目的で記録するか、パケットに対してアクションを実行します。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

利点には、ネットワークトラフィックの可視性の向上が含まれます。これにより、ネットワークオペレータは、使用パターンを理解し、ネットワークパフォーマンス情報を関連付け、利用ベースの課金や許容可能な通信内容管理を提供できます。SAIE フローは、ネットワーク全体のコストを削減することもできます。

一元管理型データポリシーを使用して SAIE フローを設定できます。Cisco SD-WAN Manager ポリシーリストまたは **policy lists app-list** CLI コマンドを使用して、対象のアプリケーションを定義し、**policy data-policy** コマンドでこれらのリストを呼び出します。データポリシーの **action** の一部で、ローカル TLOC またはリモート TLOC を定義することで、ネットワークを通過するアプリケーショントラフィックのパスを制御できます。厳密な制御の場合は、両方を定義できます。

SAIE フローでは、次のプロトコルのリストはサポートされていません。

- Open Shortest Path First（OSPF）
- Border Gateway Protocol（BGP）
- Internet Control Message Protocol（ICMP）
- Bidirectional Forwarding Detection（BFD）

Cisco SD-WAN Manager を使用した Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン フローの設定

Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン（SAIE）フローを設定するには、Cisco SD-WAN Manager ポリシー構成ウィザードを使用します。このウィザードは、ポリシーコンポーネントの作成および編集プロセスをガイドする次のような一連の画面で構成されています。

- [アプリケーションまたは対象グループの作成（Create Applications or Groups of Interest）]：関連する項目をグループ化し、ポリシーの照合やアクションコンポーネントで呼び出すリストを作成します。設定の詳細については、「対象グループの設定」を参照してください。

- [トラフィックルールの設定（Configure Traffic Rules）]：ポリシーのマッチ条件とアクション条件を作成します。設定の詳細については、「トラフィックルールの設定」を参照してください。
- [サイトと VPN にポリシーを適用（Apply Policies to Sites and VPNs）]：ポリシーをオーバーレイネットワークのサイトと VPN に関連付けます。

Cisco SD-WAN アプリケーション インテリジェンス エンジン フローへの一元管理型ポリシーの適用

Cisco SD-WAN アプリケーション インテリジェンス エンジン（SAIE）フローに対する一元管理型データポリシーを有効にするには、オーバーレイネットワーク内のサイトのリストに適用する必要があります。

Cisco SD-WAN Manager で一元管理型ポリシーを適用するには、「*Cisco SD-WAN Manager* を使用した一元管理型ポリシーの設定」を参照してください。

CLI で一元管理型ポリシーを適用するには、次の手順を実行します。

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all |
from-service | from-tunnel)
```

デフォルトでは、データポリシーは Cisco Catalyst SD-WAN コントローラ を通過するすべてのデータトラフィックに適用されます。ポリシーによって、ローカルサイト（つまり、ルータのサービス側）からトンネルインターフェイスに流入するすべてのデータトラフィックが評価されるほか、トンネルインターフェイスを介してローカルサイトに流入するすべてのトラフィックも評価されます。こうした動作は、**all** オプションを含めることで明示的に設定できます。データポリシーをローカルサイトからの流出に対するポリシーにのみ適用させるには、**from-service** オプションを含めます。ポリシーをインバウンドトラフィックにのみ適用させるには、**from-tunnel** オプションを含めます。

同じタイプのポリシーは、重複するサイト ID を含むサイトリストに適用できません。つまり、すべてのデータポリシーでサイトリストを重複させることはできないということです。サイトリストを誤って重複させてしまった場合、Cisco Catalyst SD-WAN コントローラ での設定をコミットしようとしてもできません。

実行中のアプリケーションのモニタリング

Cisco vEdge デバイス で SD-WAN Application Intelligence Engine（SAIE）インフラストラクチャを有効にするには、次のようにデバイスでアプリケーションの可視性を有効にする必要があります。

（注） Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

```
vEdge(config)# policy app-visibility
```

実行中のアプリケーションに関する情報を表示するには、デバイスで **show app dpi supported-applications**、**show app dpi applications**、および **show app dpi flow** コマンドを使用します。

SAIE アプリケーションの表示

次の手順を使用して、ルータ上の Cisco Catalyst SD-WAN ソフトウェアでサポートされているすべてのアプリケーション認識アプリケーションのリストを表示できます。

1. Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. [WAN-Edge] をクリックし、[デバイス（Device）] から Cisco SD-WAN Application Intelligence Engine（SAIE）フローに対応したものを選択します。[Cisco SD-WAN Manager 接続制御（Control Connections）] ページが表示されます。

3. 左側のペインで、[リアルタイム（Real Time）] を選択してデバイスの詳細を表示します。

4. [デバイスオプション（Device Options）] ドロップダウンから、[SAIE アプリケーション（SAIE Applications）] を選択して、デバイスで実行されているアプリケーションのリストを表示します。

5. デバイスの対応アプリケーションのリストを表示するには、[デバイスオプション（Device Options）] ドロップダウンから、[SAIE 対応アプリケーション（SAIE Supported Applications）] を選択します。

Cisco SD-WAN アプリケーション インテリジェンス エンジン フローを設定するためのアクションパラメータ

データトラフィックが一元管理型データポリシーの一致部分の条件に一致した場合、パケットを受け入れたり、ドロップしたり、またはカウントできます。その後、受け入れられたパケットにパラメータを関連付けることができます。

次の手順で、Cisco SD-WAN Manager のメニューからマッチパラメータを設定できます。

- **[設定（Configuration）] > [ポリシー（Policies）] > [一元管理型ポリシー（Centralized Policy）] > [ポリシーの追加（Add Policy）] > [トラフィックルールの設定（Configure Traffic Rules）] > [（アプリケーション認識型ルーティング | トラフィックデータ | Cflowd）（(Application-Aware Routing | Traffic Data | Cflowd)）] > [シーケンスタイプ（Sequence Type）] > [シーケンスルール（Sequence Rule）] > [アクション（Action）]**
- **[設定（Configuration）] > [ポリシー（Policies）] > [カスタムオプション（Custom Options）] > [一元管理型ポリシー（Centralized Policy）] > [トラフィックポリシー（Traffic Policy）] > [（アプリケーション認識型ルーティング | トラフィックデータ | Cflowd）（(Application-Aware Routing | Traffic Data | Cflowd)）] > [シーケンスタイプ（Sequence Type）] > [シーケンスルール（Sequence Rule）] > [アクション（Action）]**。

CLI では、**policy data-policy vpn-list sequence action** コマンドでアクションパラメータを設定します。

一元管理型データポリシーの各シーケンスには、1 つのアクション条件を含めることができます。

アクションでは、最初に一致するデータパケットを受け入れるかドロップするか、およびそれをカウントするかどうかを指定します。

表 *1*:

説明	Cisco SD-WAN Manager	CLI コマンド	値または範囲
パケットを受け入れます。受け入れられたパケットは、ポリシー設定のアクション部分で設定された追加パラメータで変更できます。	[承認（Accept）] をクリック	**accept**	—
受け入れられたパケットまたはドロップされたパケットをカウントします。	**Action Counter** [承認（Accept）] をクリックし、[カウンタ（Counter）] アクションを選択	**count** *counter-name*	カウンタの名前。シスコデバイスで **show policy access-lists counters** コマンドを使用します。
パケットを廃棄します。これがデフォルトのアクションになります。	[ドロップ（Drop）] をクリック	**drop**	—

パケットログを表示するには、**show app log flow** および **show log** コマンドを使用します。

次に、受け入れられたパケットについて、次のパラメータを設定できます。

表 *2*:

説明	Cisco SD-WAN Manager	CLI コマンド	値または範囲
DSCP 値。	[承認（Accept）] をクリックし、[DSCP] アクションを実行	**set dscp** *value*	0 ～ 63
転送クラス。	[承認（Accept）] をクリックし、[転送クラス（Forwarding Class）] アクションを実行	**set forwarding-class** *value*	転送クラス名

説明	Cisco SD-WAN Manager	CLI コマンド	値または範囲
一致するパケットを、色とカプセル化に一致する TLOC に転送 デフォルトでは、TLOC が使用できない場合、トラフィックは代替 TLOC を使用して転送されます。	[承認（Accept）] をクリックし、[ローカルTLOC（Local TLOC）] アクションを実行	**set local-tloc color** *color* [**encap** *encapsulation*]	*color* は次のいずれかになります。 **3g**、**biz-internet**、**blue**、**bronze**、**custom1**、**custom2**、**custom3**、**default**、**gold**、**green**、**lte**、**metro-ethernet**、**mpls**、**private1** ～ **private6**、**public-internet**、**red**、**silver**。 デフォルトでは、*encapsulation* は **ipsec** です。**gre** にすることもできます。
TLOCが色とカプセル化と一致する場合、一致するパケットをリスト内の TLOC の 1 つに転送します。 デフォルトでは、TLOC が使用できない場合、トラフィックは代替 TLOC を使用して転送されます。TLOCが使用できない場合にトラフィックをドロップするには、**restrict** オプションを含めます。	[承認（Accept）] をクリックし、[ローカルTLOC（Local TLOC）] アクションを実行	**set local-tloc-list color** *color* **encap** *encapsulation* [**restrict**]	
パケットの転送先となるネクストホップを設定します。	[承認（Accept）] をクリックし、[ネクストホップ（Next Hop）] アクションを実行	**set next-hop** *ip-address*	IP アドレス
ポリサーを適用します。	[承認（Accept）] をクリックし、[ポリサー（Policer）] アクションを実行	**set policer** *policer-name*	**policy policer** コマンドで設定されたポリサーの名前。
トラフィックを最終的な宛先に配信する前に、一致するパケットをネームサービスに転送します。 TLOC アドレスまたは TLOC のリストは、サービスに到達するためにトラフィックをリダイレクトする必要があるリモート TLOC を識別します。TLOCが複数ある場合、トラフィックは TLOC 間でロードバランシングされます。 VPN 識別子は、サービスが配置されている場所です。 **vpn service** 設定コマンドを使用して、サービスデバイスと同じ場所に配置されているシスコデバイスにサービス自体を設定します。	[承認（Accept）] をクリックし、[サービス（Service）] アクションを実行	**set service** *service-name* [**tloc** *ip-address* | **tloc-list** *list-name*] [**vpn** *vpn-id*]	標準サービス：**FW**、**IDS**、**IDP** カスタムサービス：**netsvc1**、**netsvc2**、**netsvc3**、**netsvc4** TLOC リストは、**policy lists tloc-list** リストで設定されます。

説明	Cisco SD-WAN Manager	CLI コマンド	値または範囲
一致するパケットを、送信元がトランスポート VPN（VPN 0）にある GRE トンネルを使用して到達可能な、指定されたサービスに直接送信します。サービスに到達するために使用される GRE トンネルがダウンしている場合、パケットルーティングは標準ルーティングを使用するようにフォールバックします。サービスへの GRE トンネルが到達できないときにパケットをドロップするには、restrict オプションを含めます。サービス VPN では、**service** コマンドを使用してサービスをアドバタイズする必要もあります。トランスポート VPN（VPN 0）で GRE インターフェイスまたはインターフェイスを設定します。	[承認（Accept）] をクリックし、[サービス（Service）] アクションを実行	**set service** *service-name* [**tloc** *ip-address* | **tloc-list** *list-name*] [**vpn** *vpn-id*]	標準サービス：**FW**、**IDS**、**IDP** カスタムサービス：**netsvc1**、**netsvc2**、**netsvc3**、**netsvc4**
トラフィックをリモート TLOC に転送します。TLOC は、IP アドレス、カラー、およびカプセル化によって定義されます。	[承認（Accept）] をクリックし、[TLOC] アクションを実行	**set local-tloc color** *color* [**encap** *encapsulation*]	TLOC アドレス、色、およびカプセル化
TLOC リスト内のいずれかのリモート TLOC にトラフィックを転送します。	[承認（Accept）] をクリックし、[TLOC] アクションを実行	**set tloc-list** *list-name*	**policy lists tloc-list** リストの名前
パケットが属する VPN を設定します。	[承認（Accept）] をクリックし、[VPN] アクションを実行	**set vpn** *vpn-id*	0 ～ 65530

Default Action

評価されるデータパケットが、データポリシーのマッチ条件のいずれにもマッチしない場合、デフォルトのアクションがパケットに適用されます。デフォルトでは、データパケットがドロップされるようになっています。

Cisco SD-WAN Manager のメニューから、デフォルトアクションを変更できます：**[設定（Configuration）] > [ポリシー（Policies）] > [一元管理型ポリシー（Centralized Policy）] > [ポリシーの追加（Add Policy）] > [トラフィックルールの設定（Configure Traffic Rules）] > [アプリケーション認識型ルーティング（Application-Aware Routing）] > [シーケンスタイプ（Sequence Type）] > [シーケンスルール（Sequence Rule）] > [デフォルトアクション（Default Action）]**。

CLI では、 **policy data-policy vpn-list default-action accept** コマンドを使用してデフォルトのアクションを変更します。

CLI を使用した、Cisco SD-WAN アプリケーション インテリジェンス エンジン フローの設定

次に、SD-WAN アプリケーション インテリジェンス エンジン（SAIE）フローの一元管理型データポリシーを設定するための手順の概要を示します。

（注） Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

1. **apply-policy** コマンドを使用して、データポリシーを適用するオーバーレイ ネットワークサイトのリストを作成します。

```
vSmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id
```

リストには、必要な数のサイト ID を含めることができます。サイト ID ごとに 1 つの **site-id** コマンドを含めます。 連続するサイト ID の場合は、番号をダッシュ（-）で区切って範囲指定できます。

必要に応じて、さらにサイトリストを作成します。

2. データポリシーの対象となるアプリケーションとアプリケーションファミリのリストを作成します。各リストには、1 つ以上のアプリケーション名、または 1 つ以上のアプリケーションファミリを含めることができます。1 つのリストにアプリケーションとアプリケーションファミリの両方を含めることはできません。

```
vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-app-list)# app application-name

vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-applist)# app-family family-name
```

3. 必要に応じて、IP プレフィックスと VPN のリストを作成します。

```
vSmart(config)# policy lists
vSmart(config-lists)# data-prefix-list list-name
vSmart(config-lists-list-name)# ip-prefix prefix/length

vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-list-name)# vpn vpn-id
```

4. 必要に応じて、TLOC のリストを作成します。

```
vSmart(config)# policy
vSmart(config-policy)# lists tloc-list list-name
vSmart(config-lists-list-name)# tloc ip-address color color encap encapsulation
[preference number]
```

5. 必要に応じて、ポリシングパラメータを定義します。

```
vSmart(config-policy)# policer policer-name
vSmart(config-policer)# rate bandwidth
vSmart(config-policer)# burst bytes
vSmart(config-policer)# exceed action
```

6. 次のように、データポリシーのインスタンスを作成し、それをVPNのリストに関連付けます。

```
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy-policy-name)# vpn-list list-name
```

7. 一連のマッチ/ペア シーケンスを次のように作成します。

```
vSmart(config-vpn-list)# sequence number
vSmart(config-sequence-number)#
```

マッチ/アクションペアは、最も小さい番号のペアから始まり、ルートがペアのいずれかの条件にマッチしたときに終了するシーケンス番号の順に評価されます。または、マッチが見つからない場合は、デフォルトのアクション（ルートを拒否するか、そのまま受け入れる）が実行されます。

8. アプリケーションに基づいてマッチパラメータを定義します。

```
vSmart(config-sequence-number)# match app-list list-name
```

9. データパケットの追加のマッチパラメータを定義します。

```
vSmart(config-sequence-number)# match parameters
```

10. 次のように、マッチしたときに実行するアクションを定義します。

```
vSmart(config-sequence-number)# action (accept | drop) [count]
```

11. 受け入れられたパケットに対して実行するアクションを定義します。パケットが通過するトンネルを制御するには、リモートまたはローカル TLOC を定義します。またはトンネルパスを厳密に制御するには、次の両方を設定します。

```
vSmart(config-action)# set tloc ip-address color color encap encapsulation
vSmart(config-action)# set tloc-list list-name
vSmart(config-action)# set local-tloc color color encap encapsulation
vSmart(config-action)# set local-tloc-list color color encap encapsulation [restrict]
```

12. 実行する追加アクションを定義します。

13. 必要に応じて、データポリシー内にマッチ/アクションペアの追加の番号付きシーケンスを作成します。

14. ルートがいずれかのシーケンス条件のどれにもマッチしない場合、そのルートはデフォルトで拒否されています。一致しないプレフィックスを受け入れる場合は、ポリシーのデフォルトアクションを設定します。

```
vSmart(config-policy-name)# default-action accept
```

15. オーバーレイネットワーク内の 1 つ以上のサイトにポリシーを適用します。

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all |
from-service | from-tunnel)
```

トラフィックの分類を確認するには、次の show コマンドを使用します。

- `show app dpi flows`
- `show support dpi flows active detail`
- `show app dpi application`
- `show support dpi flows expired detail`
- `show support dpi statistics`

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。