



Cisco Catalyst SD-WAN ポリシー設定ガイド、Cisco IOS XE Catalyst SD-WAN リリース 17.x

最終更新：2024年10月14日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2024 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	最初にお読みください	1
-------	------------	---

第 2 章	Cisco IOS XE (SD-WAN) の新機能	3
-------	----------------------------	---

第 3 章	ポリシーの概要	5
	ポリシーのアーキテクチャ	8
	一元管理型制御ポリシーのアーキテクチャ	8
	ルートタイプ	10
	一元管理型制御ポリシーを使用しない場合のデフォルト動作	10
	一元管理型制御ポリシーを使用した場合の動作の違い	11
	一元管理型制御ポリシーを使用したトラフィックフローの変更例	12
	プレフィックスと IP ヘッダーに基づく一元管理型ポリシーの構成	16
	Cisco Catalyst SD-WAN コントローラ のポリシーコンポーネント	17
	ポリシーで使用される TLOC 属性	22
	ポリシーで使用される Cisco Catalyst SD-WAN ルート属性	23
	Cisco Catalyst SD-WAN コントローラ ポリシー処理と適用の設計	24
	Cisco Cisco Catalyst SD-WAN コントローラ によるポリシーの運用	25
	制御ポリシー	25
	データポリシー	29
	VPN メンバーシップポリシーの運用	31
	Cisco SD-WAN コントローラ ポリシーの設定と実行	32

第 4 章	一元管理型ポリシー	35
	一元管理型ポリシーの概要	35

一元管理型ポリシーのタイプ	36
Cisco SD-WAN Manager を使用した一元管理型ポリシーの設定	37
ポリシー構成ウィザードの開始	37
一元管理型ポリシーの対象グループの構成	37
WAN Insights (WANI) の Cisco SD-WAN Manager への統合	46
予測パス推奨事項	48
トポロジと VPN メンバーシップの設定	48
既存のトポロジのインポート	52
VPN メンバーシップポリシーの作成	52
トラフィックルールの設定	53
マッチパラメータ：制御ポリシー	60
マッチパラメータ：データポリシー	64
アクションパラメータ：制御ポリシー	70
アクションパラメータ：データポリシー	72
サイトと VPN へのポリシーの適用	77
Cisco IOS XE Catalyst SD-WAN デバイス での NAT フォールバック	78
一元管理型ポリシーのアクティブ化	80
CLI を使用した、一元管理型ポリシーの設定	82
一元管理型ポリシーの設定例	86

第 5 章

ローカライズ型ポリシー	97
ローカライズ型ポリシーの概要	98
ローカライズ型ポリシーのタイプ	98
Cisco SD-WAN Manager を使用したローカライズ型ポリシーの設定	100
ポリシー構成ウィザードの開始	100
ローカライズ型ポリシーの対象グループの構成	100
転送クラス/QoSの設定	104
ACL の設定	106
明示的なアクセスリストと暗示的なアクセスリスト	107
ルートポリシーの設定	109
match パラメータ	110

アクションパラメータ	113
ポリシー設定の構成	115
デバイステンプレートへのローカライズ型データポリシーの適用	115
ローカライズ型ポリシーのアクティブ化	116
CLIを使用した、IPv4 に対するローカライズ型ポリシーの設定	119
CLIを使用した、IPv6 に対するローカライズ型ポリシーの設定	121
ローカライズ型データポリシーの設定例	122
ルータ生成 Cisco SD-WAN Manager トラフィックの QoS	123
ルータ生成 Cisco SD-WAN Manager トラフィックの QoS について	123
ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の制約事項	124
CLI テンプレートを使用した、ルータで生成された Cisco SD-WAN Manager トラフィックの QoS の設定	124
CLIを使用した、ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の確認	125
ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS のトラブルシューティング	127

 第 6 章

サービス側 VPN での DNS リダイレクト	129
サービス側 VPN での DNS リダイレクトについて	130
サービス側 VPN での DNS リダイレクトに関する制約事項	130
サービス側 VPN での DNS リダイレクトの使用例	131
サービス側 VPN での DNS リダイレクトの設定	132
CLIを使用したサービス側 VPN での DNS リダイレクトの設定	136
サービス側 VPN での DNS リダイレクトの確認	137
DNS リダイレクトの設定例	137

 第 7 章

デフォルトの AAR ポリシーと QoS ポリシー	139
デフォルトの AAR ポリシーと QoS ポリシーについて	140
デフォルトの AAR ポリシーと QoS ポリシーの利点	141
デフォルトの AAR ポリシーと QoS ポリシーの前提条件	141
デフォルトの AAR ポリシーと QoS ポリシーに対する制約事項	141
デフォルトの AAR ポリシーと QoS ポリシーに対応したデバイス	142

デフォルトの AAR ポリシーと QoS ポリシーの使用例	142
Cisco SD-WAN Manager を使用したデフォルトの AAR および QoS ポリシーの設定	142
デフォルトの AAR ポリシーと QoS ポリシーのモニター	147

第 8 章

デバイスアクセスポリシー	149
デバイスアクセスポリシーの概要	150
Cisco SD-WAN Manager を使用したデバイスアクセスポリシーの設定	150
CLI を使用したデバイスアクセスポリシーの設定	153
ACL 統計とカウンタの例	153
SNMP サーバーに対する ACL ポリシーの確認	154
SSH に対する ACL ポリシーの確認	156

第 9 章

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	159
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	159
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	160
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	161
実行中のアプリケーションのモニタリング	161
SAIE アプリケーションの表示	162
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	162
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	166

第 10 章

アプリケーション認識型ルーティング	169
アプリケーション認識型ルーティングについて	169
マルチキャストプロトコルに対応したアプリケーション認識型ルーティング	170
マルチキャストプロトコルに関する制約事項	171
アプリケーション認識型ルーティングのコンポーネント	171
SLA クラス	173
トンネルの SLA クラスへの分類	176

損失、遅延、ジッターの測定	176
平均損失、遅延、およびジッターの計算	177
SLA 分類の決定	177
クラスごとのアプリケーション認識型ルーティング	178
クラスごとのアプリケーション認識型ルーティングの概要	178
アプリケーションプローブクラス	179
デフォルトの DSCP 値	180
アプリケーション認識型ルーティングの設定	180
Cisco SD-WAN Manager を使用したアプリケーション認識型ルーティングポリシーの設定	181
最善のトンネルパスの設定	182
最善のトンネルパスの概要	182
最善のトンネルパスに向けた推奨事項	183
最善のトンネルパスに向けたバリエーション設定	183
最善のトンネルパスに向けたバリエーション設定の確認	184
SLA クラスの構成	185
トラフィックルールの設定	187
アプリケーション認識型ルーティングポリシーのデフォルトアクション	193
Cisco Catalyst SD-WAN Manager を介したアプリケーションプローブクラスの設定	194
SLA クラスへのアプリケーションプローブクラスの追加	194
Cisco BFD テンプレートでのデフォルト DSCP の設定	195
サイトと VPN へのポリシーの適用	196
アプリケーション認識型ルーティングポリシーを他のデータポリシーと組み合わせて適用する方法	197
アプリケーション認識型ルーティングポリシーのアクティブ化	199
データプレーントンネルのパフォーマンスのモニター	199
Cisco IOS XE Catalyst SD-WAN デバイスでのアプリケーションの可視性の有効化	201
CLI を使用したアプリケーション認識型ルーティングの設定	202
CLI を使用したアプリケーションプローブクラスの設定	204
アプリケーション認識型ルーティングポリシーの設定例	205

第 11 章	拡張アプリケーション認識型ルーティング	211
	拡張アプリケーション認識型ルーティングについて	212
	拡張アプリケーション認識型ルーティングの概要	213
	PfR 測定	214
	アプリケーション認識型ルーティングの設計と測定	214
	拡張アプリケーション認識型ルーティングの利点	215
	拡張アプリケーション認識型ルーティングのガイドライン	216
	拡張アプリケーション認識型ルーティングを実行していない Cisco IOS XE Catalyst SD-WAN デバイス との互換性	216
	拡張アプリケーション認識型ルーティングに対応したデバイス	217
	拡張アプリケーション認識型ルーティングに関する制約事項	217
	拡張アプリケーション認識型ルーティングの前提条件	217
	拡張アプリケーション認識型ルーティングの設定	217
	Cisco Catalyst SD-WAN Manager の機能テンプレートを使用した拡張アプリケーション認識型ルーティングの設定	217
	Cisco Catalyst SD-WAN Manager の構成グループを使用した、拡張アプリケーション認識型ルーティングの設定	218
	CLI テンプレートを使用した、拡張アプリケーション認識型ルーティングの設定	219
	拡張アプリケーション認識型ルーティングの設定確認	220
	Cisco Catalyst SD-WAN Manager を使用した拡張アプリケーション認識型ルーティングのモニター	221
	拡張アプリケーション認識型ルーティングのトラブルシューティング	222
第 12 章	トラフィック フロー モニタリング	225
	トラフィック フロー モニタリング	226
	トラフィック フロー モニタリングについて	228
	Cflowd を使用したトラフィック フロー モニタリングの概要	229
	Cisco IOS XE Catalyst SD-WAN デバイス のための IPFIX 情報要素	230
	VPN0 インターフェイスに対する Flexible NetFlow	235
	VPN0 インターフェイスでの Flexible Netflow の制限	236
	Flexible NetFlow 分散エクスポート	237

Flexible NetFlow による BFD メトリックのエクスポート	238
BFD メトリックのエクスポートの仕組み	239
SAIE フローを使用した Cflowd トラフィック フロー モニタリング	239
SAIE フローを使用した Cflowd トラフィック フロー モニタリングの利点	240
SAIE フローを使用した Cflowd トラフィック フロー モニタリングの前提条件	240
SAIE フローを使用した Cflowd トラフィック フロー モニタリングに関する制約事項	240
集約データの最大 FNF レコードレートの設定に関する情報	241
トラフィック フロー モニタリングの制約事項	241
ループバックを TLOC として使用する場合のフローテレメトリでの収集ループバックの有効化に関する制約事項	242
トラフィック フロー モニタリングの設定	242
Cisco IOS XE Catalyst SD-WAN デバイスでのトラフィック フロー モニタリングの設定	242
グローバルフローの可視性の設定	242
アプリケーション可視性のグローバルな設定	245
Cflowd モニタリングポリシーの設定	246
Cflowd 情報の表示	250
CLI を使用した、Cflowd トラフィック フロー モニタリングの設定	251
VPN0 インターフェイスでの Flexible NetFlow の設定	252
CLI を使用した BFD メトリックのエクスポートに対する Flexible NetFlow の設定	253
Flexible NetFlow による BFD メトリックのエクスポート設定例	254
Cflowd ポリシーの適用と有効化	255
Cflowd トラフィック フロー モニタリングの設定例	256
CLI コマンドを使用した集約データの最大 FNF レコードレートの設定	261
トラフィック フロー モニタリングの確認	262
収集ループバックの確認	262
デバイスのインターフェイスバインドの確認	264
VPN0 インターフェイスでの Flexible NetFlow 設定の確認	265
BFD メトリックのエクスポートに対する Flexible NetFlow 設定の確認	268
第 13 章	アプリケーションパフォーマンス モニター 271
	アプリケーションパフォーマンス モニターの概要 272

制限事項と制約事項	274
アプリケーションパフォーマンス モニターの設定	274
パフォーマンスモニタリング設定の確認	275

第 14 章 **拡張型ポリシーベースルーティング** 287

ePBR の概要	288
ePBR の設定	289
ePBR のモニター	293

第 15 章 **前方誤り訂正** 295

前方誤り訂正に対応したデバイス	296
ポリシーへの前方誤り訂正の設定	296
前方誤り訂正によるトンネル情報のモニター	297
前方誤り訂正によるアプリケーションファミリ情報のモニター	298
CLI を使用した、前方誤り訂正のステータスのモニター	298

第 16 章 **ノイズの多いチャネルに対するパケット複製** 301

パケット複製について	301
パケット複製の設定	302

第 17 章 **ポリシー構成のタグ付け** 305

ポリシー構成のタグ付けに対応したデバイス	307
ポリシー構成のタグ付けに関する制約事項	307
ポリシー構成のタグ付けについて	308
ポリシー構成のタグ付けの利点	310
CLI テンプレートを使用したポリシー構成のタグ付け設定	311
CLI を使用した Tag-Instances 設定の確認	313

第 18 章 **Cisco IOS XE Catalyst SD-WAN デバイス と ACI の統合** 317

Cisco ACI との統合に関するガイドライン	318
Cisco ACI 登録の確認	319

SLA クラス	319
データプレフィックス	319
VPNs	320
SLA へのデータプレフィックスと VPN のマッピング	320
App-Route-Policy の作成	320
ACI サイトのマッピング	321
ACI サイトのマッピング解除	322
コントローラの削除	322

 第 19 章

カスタム アプリケーション	325
カスタムアプリケーションについて	325
カスタムアプリケーションに関する制約事項	328
Cisco SD-WAN Manager を使用した、カスタムアプリケーションの設定	329
カスタムアプリケーションの確認	331

 第 20 章

サービス挿入	333
サービス挿入に関する情報	334
サービス挿入の制約事項	339
サービス挿入の使用例	340
サービス挿入の設定	340
データポリシーでのサービスチェーンアクションの設定	341
サービスチェーンへのトラフィックステアリング	343
制御ポリシーを使用したトラフィックステアリング	343
データポリシーを使用したトラフィックステアリング	344
インターフェイスアクセス制御リストを使用したトラフィックステアリング	345
Path Preference	346
ユーザー VPN 間でのサービスチェーンの共有	347
送信トラフィックと受信トラフィックの別々のインターフェイス	347
信頼できるトラフィックと信頼できないトラフィックのサービスチェーン	348
2 つのルータ間のサービスチェーン	348
サービスチェーンを介したトラフィックのフォールバックおよび制限動作の設定	349

サービスチェーン内のサービスをルータに接続するためのインターフェイス	349
Software Defined Cloud Interconnect Bring Your Own Service を使用したサービスチェーン	350
CLI テンプレートを使用したサービス挿入の設定	351

第 21 章

サービス チェーニング	353
サービス チェーニングの設定	357
サービスチェーン設定例	359
サービスチェーンのモニター	367

第 22 章

合法的傍受	371
合法的傍受に関する情報	372
合法的傍受の前提条件	375
Cisco Catalyst SD-WAN Manager を使用した合法的傍受のインストール	376
合法的傍受 MIB	377
信頼できるホストへのアクセス制限（暗号化なし）	378
信頼できるメディアエーションデバイスの制限	378
合法的傍受の設定	379
CLI を使用した、合法的傍受の設定	379
合法的傍受トラフィックの暗号化	380
デバイスでの暗号化の設定	380
CLI を使用した、合法的傍受の暗号化設定	381
メディア デバイス ゲートウェイとの静的トンネルの確認	382

第 23 章

合法的傍受 2.0	383
合法的傍受 2.0 について	385
Cisco Catalyst SD-WAN の合法的傍受 2.0 の前提条件	386
Cisco Catalyst SD-WAN の合法的傍受 2.0 の利点	386
合法的傍受 2.0 のワークフローの設定	386
合法的傍受管理者の作成	387
合法的傍受 API ユーザーの作成	387
傍受案件の作成	388

傍受内容の回収 390

Cisco SD-WAN Manager による合法的傍受のための Cisco SD-WAN コントローラ トラブル
シューティング 391

第 24 章

Cisco Catalyst SD-WAN のポリシーに関するトラブルシューティング 393

概要 393

サポート記事 394

フィードバックのリクエスト 395

免責事項と注意事項 395



第 1 章

最初にお読みください



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

参考資料

- [Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations](#) [英語]
- [Cisco Catalyst SD-WAN Device Compatibility](#) [英語]

ユーザーマニュアル

- [User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17](#) [英語]

通信、サービス、およびその他の情報

- **Cisco Profile Manager** で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンストサービス、リモートサービスについては、[シスコサービス](#) にアクセスしてください。
- 安全かつ検証されたエンタープライズクラスのアプリ、製品、ソリューション、サービスをお求めの場合は、[CiscoDevnet](#) にアクセスしてください。

- Cisco Press 出版社による一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。
- リリースで未解決および解決済みのバグをご覧になる場合は、[Cisco Bug Search Tool](#) にアクセスしてください。
- サービス リクエストを送信するには、[シスコ サポート](#) にアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 2 章

Cisco IOS XE (SD-WAN) の新機能



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。



- (注) シスコでは、リリースごとに Cisco Catalyst SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次の表に、コンフィギュレーションガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されている新機能と変更された機能を示します。Cisco Catalyst SD-WAN ソリューションに関する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

[What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x \[英語\]](#)



第 3 章

ポリシーの概要



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

ポリシーは、オーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス 間のデータトラフィックおよびルーティング情報のフローに影響を与えます。

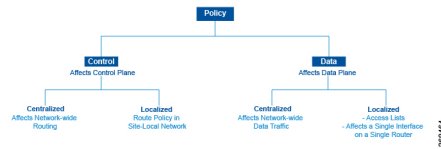
このポリシーは次の内容で構成されます。

- ルーティングポリシー：ネットワークのコントロールプレーンでのルーティング情報のフローに影響します。
- データポリシー：ネットワークのデータプレーンのデータトラフィックのフローに影響します。

企業固有のトラフィック制御要件を実装するには、基本ポリシーを作成し、ポリシー設定インフラストラクチャによってアクティブ化される高度な機能を展開します。

Cisco Catalyst SD-WAN オーバーレイ ネットワーク アーキテクチャがコントロールプレーンをデータプレーンから明確に分離し、一元管理型の機能とローカライズ型の機能の制御を分離しているように、Cisco Catalyst SD-WAN ポリシーも明確に分離されています。ポリシーは、コントロールプレーンまたはデータプレーントラフィックのいずれかに適用され、Cisco SD-WAN コントローラ で一元的に、または Cisco IOS XE Catalyst SD-WAN デバイス でローカルに設定されます。次の図は、制御ポリシーとデータポリシー間、および一元管理型ポリシーとローカルポリシー間の分離を示しています。

図 1: ポリシーのアーキテクチャ



制御ポリシーとデータポリシー

制御ポリシーはルーティングプロトコルポリシーに相当し、データポリシーは一般にアクセス制御リスト（ACL）およびファイアウォールフィルタと呼ばれるものに相当します。

一元管理型ポリシーとローカライズ型ポリシー

Cisco Catalyst SD-WAN ポリシー設計では、一元管理型ポリシーとローカライズ型ポリシーを明確に分離しています。つまり、一元管理型ポリシーは、オーバーレイネットワーク内の一元化された Cisco SD-WAN コントローラでプロビジョニングされ、ローカライズ型ポリシーは、インターネット、MPLS、メトロイーサネットなどのトランスポートネットワークおよびブランチまたはエンタープライズサイト間のネットワークエッジにある、Cisco IOS XE Catalyst SD-WAN デバイスでプロビジョニングされるということです。

一元管理型ポリシー

一元管理型ポリシーとは、Cisco SD-WAN コントローラ上でプロビジョニングされるポリシーのことであり、Cisco Catalyst SD-WAN オーバーレイネットワーク内の一元化されたコントローラです。一元管理型ポリシーは、次の 2 つのコンポーネントで構成されます。

- 制御ポリシー：トラフィックのオーバーレイネットワーク全体のルーティングに影響
- データポリシー：ネットワーク内の VPN セグメント全体のデータトラフィックフローに影響

一元管理型制御ポリシーは、Cisco SD-WAN コントローラのルートテーブルに保存され、Cisco IOS XE Catalyst SD-WAN デバイスにアドバタイズされる情報に影響を与えることによって、トラフィックのネットワーク全体のルーティングに適用されます。一元管理型制御ポリシーの効果は、Cisco IOS XE Catalyst SD-WAN デバイスがオーバーレイネットワークのデータトラフィックを宛先に送信する方法に見られます。



(注) 一元管理型制御ポリシーの設定自体は Cisco SD-WAN コントローラに残り、ローカルデバイスにプッシュされることはありません。

一元管理型データポリシーは、オーバーレイネットワーク内の VPN 全体のデータトラフィックのフローに適用されます。これらのポリシーは、6 タプルの一致（送信元と宛先の IP アドレスとポート、DSCP フィールド、プロトコル）または VPN メンバーシップのいずれかに基づいてアクセスを許可および制限できます。これらのポリシーは、選択した Cisco IOS XE Catalyst SD-WAN デバイスにプッシュされます。

ローカライズ型ポリシー

ローカライズ型ポリシーとは、Cisco IOS XE Catalyst SD-WAN デバイスの CLI または Cisco SD-WAN Manager デバイステンプレートを通じてローカルにプロビジョニングされたポリシーを指します。

ローカライズ型制御ポリシーはルートポリシーとも呼ばれ、サイトローカルネットワーク上の (BGP および OSPF) ルーティング動作に影響します。

ローカライズ型データポリシーを使用すると、アクセスリストをプロビジョニングし、デバイス上の特定のインターフェイスに適用できます。簡易アクセスリストは、一元管理型データポリシーと同じように、6 タプルの照合 (送信元と宛先の IP アドレスとポート、DSCP フィールド、およびプロトコル) に基づいてアクセスを許可および制限します。また、アクセスリストを使用すると、サービスクラス (CoS) のプロビジョニング、ポリシング、を行うことができ、デバイスのインターフェイスおよびインターフェイスキュー間でデータトラフィックが送受信される方法を制御できます。

Cisco Catalyst SD-WAN ポリシーの設計によって、基本ポリシーと高度なポリシーが区別されます。基本ポリシーは、オーバーレイネットワークを通過する基本的なトラフィックフローに影響を与えたり、決定したりすることができます。ここでは、ネットワークを介してトラフィックがルーティングされるパスの管理、パケットの IP ヘッダーのアドレス、ポート、DSCP フィールドに基づくトラフィックの許可またはブロックなどの標準的なポリシータスクを実行します。また、Cisco IOS XE Catalyst SD-WAN デバイスのインターフェイスに出入りするデータトラフィックのフローを制御して、サービスクラス、キューイング、ポリシングなどの機能を有効にすることもできます。

- アプリケーション認識型ルーティング。リアルタイムのネットワークとパスのパフォーマンス特性に基づいて、トラフィックのベストパスを選択します。
- cflowd。トラフィックフローのモニタリング用。

デフォルトでは、中央管理型 Cisco SD-WAN コントローラ またはローカル型 Cisco IOS XE Catalyst SD-WAN デバイスのいずれの Cisco IOS XE Catalyst SD-WAN デバイスにも、いかなるポリシーも設定されていません。ルート情報を配信するコントロールプレーントラフィックがポリシングされていない場合、下記の通りとなります。

- OMP が Cisco IOS XE Catalyst SD-WAN デバイス間で伝播するすべてのルート情報は、オーバーレイネットワークドメイン内のすべての Cisco SD-WAN コントローラ および Cisco IOS XE Catalyst SD-WAN デバイスで共有され、変更されません。
- Cisco IOS XE Catalyst SD-WAN デバイスがローカルサイトネットワーク内で伝播するルート情報に影響を与える BGP または OSPF ルートポリシーは設定されていません。

データプレーントラフィックがポリシングされていない場合、すべてのデータトラフィックは、ローカルの Cisco IOS XE Catalyst SD-WAN デバイスルートテーブルのエントリのみに基づいて宛先に向けられ、オーバーレイネットワーク内のすべての VPN がデータトラフィックを交換できます。

- [ポリシーのアーキテクチャ \(8 ページ\)](#)
- [Cisco Catalyst SD-WAN コントローラのポリシーコンポーネント \(17 ページ\)](#)

- [Cisco Catalyst SD-WAN コントローラ ポリシー処理と適用の設計 \(24 ページ\)](#)
- [Cisco Cisco Catalyst SD-WAN コントローラ によるポリシーの運用 \(25 ページ\)](#)
- [Cisco SD-WAN コントローラ ポリシーの設定と実行 \(32 ページ\)](#)

ポリシーのアーキテクチャ

このトピックでは、オーバーレイネットワーク全体にポリシーを実装するために使用される Cisco Catalyst SD-WAN ポリシーのアーキテクチャについて説明します。これらのポリシーは、Cisco SD-WAN Validator ポリシーまたは一元管理型ポリシーと呼ばれています。理由は、こうしたポリシーが Cisco SD-WAN コントローラ で一元的に設定されるからです。Cisco SD-WAN コントローラ ポリシーは、コントロールプレーントラフィック（オーバーレイ管理プロトコル（OMP）によって伝送され、オーバーレイネットワークのトポロジとステータスを決定するために Cisco SD-WAN コントローラ によって使用されるルーティング更新）とデータプレーントラフィック（オーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス間を行き来するデータトラフィック）の両方のフローに影響を及ぼします。

Cisco Catalyst SD-WAN では、Cisco IOS XE Catalyst SD-WAN デバイスでもルーティングポリシーの作成が可能です。こうしたポリシーは、デバイス上でローカルにルーティングプロトコル（BGP または OSPF）に関連付けられている従来のルーティングポリシーと変わりありません。使用する場合は、従来の感覚で行えます。たとえば、BGP や OSPF を制御して、ルート情報の交換に影響を与えたり、ルート属性を設定したり、パス選択に影響を与えたりする場合と同じ感覚で使用できます。

一元管理型制御ポリシーのアーキテクチャ

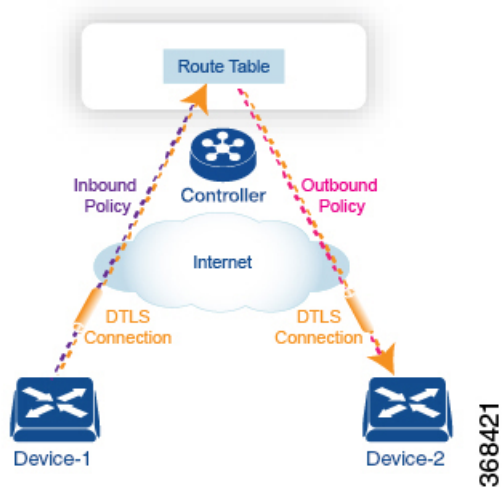
Cisco IOS XE Catalyst SD-WAN ネットワークアーキテクチャでは、一元管理型制御ポリシーは、実質的にネットワークのルーティングエンジンである Cisco SD-WAN コントローラ によって処理されます。Cisco SD-WAN コントローラ は、ネットワーク全体のルートで一元化されたマネージャであり、これらのルートのプライマリルートテーブルを管理します。Cisco SD-WAN コントローラ は、ドメイン内の Cisco IOS XE Catalyst SD-WAN デバイスによってアドバタイズされたルート情報に基づいてルートテーブルを作成し、これらのルートを使用してネットワークトポロジを検出し、ネットワークの宛先へのベストパスを決定します。Cisco SD-WAN コントローラ は、そのルートテーブルからドメイン内のデバイスにルート情報を配布し、デバイスはこれらのルートを使用して、ネットワークを介してデータトラフィックを転送します。このアーキテクチャの結果、ネットワーク全体のルーティングの決定とルーティングポリシーは、ネットワーク内のデバイスによってホップごとに実装されるのではなく、中央機関によって調整されます。

一元管理型制御ポリシーを使用すると、Cisco SD-WAN コントローラ によってアドバタイズされるネットワークルートに影響を与えることができます。このタイプのポリシーは、Cisco SD-WAN コントローラ で一元的にプロビジョニングされ、Cisco SD-WAN コントローラ がプライマリルートテーブルに保存するルート情報と、デバイスに配布するルート情報の両方に影響します。

一元管理型制御ポリシーは、Cisco SD-WAN コントローラ でのみプロビジョニングおよび適用されます。制御ポリシーの設定自体は、オーバーレイネットワーク内のデバイスにプッシュされることはありません。オーバーレイ管理プロトコル (OMP) を使用してデバイスにプッシュされるのは、制御ポリシーの結果です。デバイスはこのポリシーをローカルルートテーブルにインストールし、データトラフィックの転送に使用します。この設計は、ネットワーク管理者が設計したポリシーを使用して、ネットワーク全体のルート配布が常に一元的に管理されることを意味します。これらのポリシーは、一元管理型の Cisco SD-WAN コントローラ によって常に実装され、Cisco IOS XE Catalyst SD-WAN オーバーレイネットワークでルーティングの決定を調整します。

ネットワークドメイン内では、すべての Cisco SD-WAN コントローラ のネットワークトポロジマップを同期する必要があります。これをサポートするには、ドメイン内のすべての Cisco SD-WAN コントローラ で同一のポリシーを設定する必要があります。

図 2: 一元管理型制御ポリシー



ルート情報を含むすべての一元管理型制御プレーントラフィックは、デバイスとそのドメイン内の Cisco SD-WAN コントローラ 間のセキュアで永続的な DTLS 接続内で実行される OMP ピアリングセッションによって伝送されます。OMP ピアリングセッションのエンドポイントは、デバイスのシステム ID によって識別され、ピアリングセッションは、デバイスが配置されているサイトを識別するサイト ID を伝送します。DTLS 接続とその上で実行されている OMP セッションは、2つのピアが動作している限りアクティブなままです。

制御ポリシーは、Cisco SD-WAN コントローラ がデバイスから受信するルートアドバタイズメントに対するインバウンドと、デバイスに送信するアドバタイズメントに対するアウトバウンドの両方に適用できます。インバウンド制御ポリシーは、Cisco SD-WAN コントローラ のローカルルーティングデータベースにインストールされるルートとルート情報、およびこの情報をそのままインストールするか変更するかを制御します。アウトバウンド制御ポリシーは、ルートがルーティングデータベースから取得された後、Cisco SD-WAN コントローラ がアドバタイズする前に適用され、ルート情報がそのままアドバタイズされるか、変更されるかに影響します。

ルートのタイプ

Cisco SD-WAN コントローラ は、OMP によって伝送される Cisco IOS XE Catalyst SD-WAN 固有のルートである OMP ルートからネットワークトポロジを学習します。OMP ルートには次の 3 つのタイプがあります。

- Cisco IOS XE Catalyst SD-WAN OMP ルート：このルートは、デバイスがローカルネットワーク上で実行されているルーティングプロトコルから学習したプレフィックス情報を伝送します。情報には、BGP および OSPF から学習したルート、直接ルート、接続ルート、および静的ルートが含まれます。OMP は、OMP ルート SAFI（後続のアドレスファミリー識別子）を使用して OMP ルートを Cisco SD-WAN コントローラ にアダプタイズします。これらのルートは、一般に単に OMP ルートと呼ばれます。
- TLOC ルート：このルートは、デバイスが WAN またはトランスポートネットワークに接続する物理ポイントであるトランスポートロケーションに関連付けられたプロパティを伝送します。TLOC を識別するプロパティには、WAN インターフェイスの IP アドレスと、特定のトラフィックフローを識別する色が含まれます。OMP は TLOC SAFI を使用して TLOC ルートをアダプタイズします。
- サービスルート：これらのルートは、デバイスが接続されているローカルサイトネットワークで使用可能なネットワークサービス（ファイアウォールや IDP など）を識別します。OMP は、サービス SAFI を使用してこれらのルートをアダプタイズします。

これら 3 種類のルートの違いは、Cisco SD-WAN コントローラ または Cisco IOS XE Catalyst SD-WAN デバイスの CLI にログインしているときに、さまざまな **show sdwan omp** 操作コマンドを使用して表示できます。**show sdwan omp routes** コマンドは情報をプレフィックスでソートして表示し、**show sdwan omp services** コマンドはルート情報をサービスでソートして表示し、**show sdwan omp tlocs** コマンドはルート情報を TLOC でソートします。

一元管理型制御ポリシーを使用しない場合のデフォルト動作

デフォルトでは、一元管理型制御ポリシーは Cisco SD-WAN コントローラ でプロビジョニングされません。これにより、ドメイン内で次のルートアダプタイズメントおよび再配布動作は次のようになります。

- すべての Cisco IOS XE Catalyst SD-WAN デバイスは、サイトローカルネットワークから学習したすべてのルート関連プレフィックスを Cisco SD-WAN コントローラ に再配布します。このルート情報は、デバイスと Cisco SD-WAN コントローラ 間の DTLS 接続を介して伝送される OMP ルートアダプタイズメントによって伝送されます。ドメインに複数の Cisco SD-WAN コントローラ が含まれている場合、デバイスはすべての OMP ルートアダプタイズメントをすべてのコントローラに送信します。
- すべてのデバイスは、OMP を使用して、すべての TLOC ルートをドメイン内の Cisco SD-WAN コントローラ またはコントローラに送信します。
- すべてのデバイスは、デバイスが配置されたローカルサイトで使用可能なネットワークサービス（ファイアウォールや IDP など）をアダプタイズするために、すべてのサービスルートを送信します。これらも OMP によって伝送されます。

- Cisco SD-WAN コントローラは、ドメイン内のすべてのデバイスから受信したすべての OMP、TLOC、およびサービスルートを受け入れ、ルートテーブルにその情報を保存します。Cisco SD-WAN コントローラは、どの OMP ルート、TLOC、およびサービスがどの VPN に属しているかを追跡します。Cisco SD-WAN コントローラは、すべてのルートを使用してネットワークのトポロジマップを作成し、オーバーレイネットワークを通過するデータトラフィックのルーティングパスを決定します。
- Cisco SD-WAN コントローラは、特定の VPN 内の OMP、TLOC、およびサービスルートから学習したすべての情報を、同じ VPN 内のすべてのデバイスに再配布します。
- デバイスは、ルート更新を定期的に Cisco SD-WAN コントローラに送信します。
- Cisco SD-WAN コントローラはルーティングパスを再計算し、ルートテーブルを更新し、新規および変更されたルーティング情報をすべてのデバイスにアドバタイズします。

一元管理型制御ポリシーを使用した場合の動作の違い

すべてのルート情報をドメイン内のすべての Cisco IOS XE Catalyst SD-WAN デバイスに再配布しない場合、または Cisco Catalyst SD-WAN コントローラのルートテーブルに保存されているルート情報や Cisco Catalyst SD-WAN コントローラによってアドバタイズされるルート情報を変更する場合は、一元管理型制御ポリシーを設計してプロビジョニングします。制御ポリシーをアクティブ化するには、インバウンドまたはアウトバウンド方向のオーバーレイネットワーク内の特定のサイトにそのポリシーを適用します。その際、方向は Cisco Catalyst SD-WAN コントローラを基点として考えます。一元管理型制御ポリシーのすべてのプロビジョニングは、Cisco Catalyst SD-WAN コントローラで実行されます。

インバウンド方向に一元管理型制御ポリシーを適用すると、Cisco IOS XE Catalyst SD-WAN デバイスによってアドバタイズされているルートは Cisco Catalyst SD-WAN コントローラのルートテーブルに配置される前にフィルタリングまたは変更されます。プロセスにおける最初のステップとして、ルートは受け入れられるか拒否されます。受け入れられたルートは、受信したルート、または制御ポリシーによって変更されたルートとして、Cisco Catalyst SD-WAN コントローラのルートテーブルにインストールされます。制御ポリシーによって拒否されたルートは、通知なしに破棄されます。

アウトバウンド方向に制御ポリシーを適用すると、Cisco Catalyst SD-WAN コントローラによって Cisco IOS XE Catalyst SD-WAN デバイスに再配布されるルートがフィルタリングまたは変更されます。アウトバウンド方向のポリシーでは最初のステップとして、ルートは受け入れられるか拒否されます。受け入れられたルートの場合、一元管理型制御ポリシーを通じた、Cisco Catalyst SD-WAN コントローラによる配布前のルート変更が可能です。アウトバウンド方向のポリシーによって拒否されたルートはアドバタイズされません。

VPN メンバーシップポリシー

一元管理型データポリシーのもう 1 つのタイプは、VPN メンバーシップポリシーです。これは、Cisco IOS XE Catalyst SD-WAN デバイスが特定の VPN に参加できるかどうかを制御するポリシーです。VPN メンバーシップポリシーは、デバイスのどの VPN のルートであれば受信を許可し、どの VPN のルートなら受信を許可しないかを定義します。

VPNメンバーシップポリシーは一元管理できますが、それは、影響がパケットのヘッダーに対してのみで、Cisco IOS XE Catalyst SD-WAN デバイスがトラフィックの送信に使用するインターフェイスの選択には影響しないからです。一元管理をしていないと、VPNメンバーシップポリシーにより、ある特定のVPNのルートがデバイスが受信できない場合に、Cisco Catalyst SD-WAN コントローラからそのドライバに対し、そうしたルートの転送が決して行われないということが起こります。

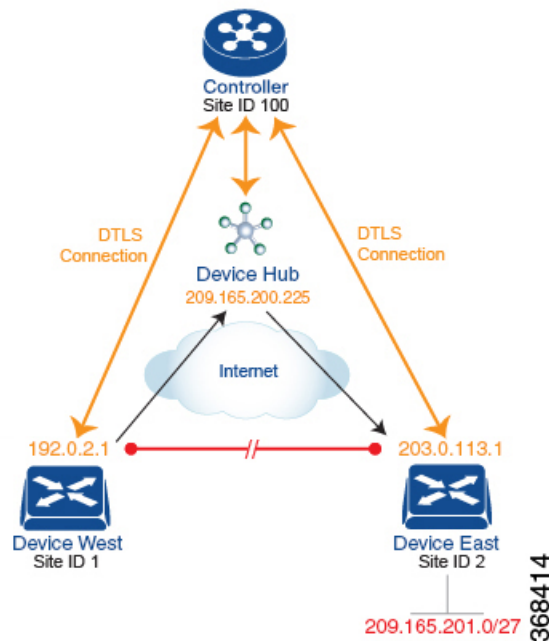
一元管理型制御ポリシーを使用したトラフィックフローの変更例

このセクションでは、一元管理型制御ポリシーを使用して、オーバーレイネットワークを通過するデータトラフィックのフローを変更する方法について基本的な例をいくつか示します。

任意のトポロジの作成

2つのCisco IOS XE Catalyst SD-WAN デバイスの間でデータトラフィックが交換される時、制御ポリシーをプロビジョニングしていない場合、2つのデバイスはそれらの間にIPsecトンネルを確立し、データトラフィックは1つのデバイスから次のデバイスに直接流れます。デバイスが2台のみのネットワーク、またはデバイスの数が少ないネットワークでは、通常、デバイスの各ペア間の接続の確立が問題になることはありません。ただし、このようなソリューションは拡張できません。数百または数千のブランチを持つネットワークでは、IPsecトンネルのフルメッシュを確立すると、各デバイスのCPUリソースに負担がかかります。

図 3: 任意のトポロジ



このオーバーヘッドを最小限に抑える方法の1つは、ハブアンドスポークタイプのトポロジを作成することです。この場合、デバイスの1つがハブサイトとして機能し、すべてのスポークまたはブランチデバイスからデータトラフィックを受信し、トラフィックを適切な宛先にリダイレクトします。この例では、このようなハブアンドスポークトポロジを作成する方法の1つ

を示します。これは、宛先に関連付けられた TLOC のアドレスを変更する制御ポリシーを作成することです。

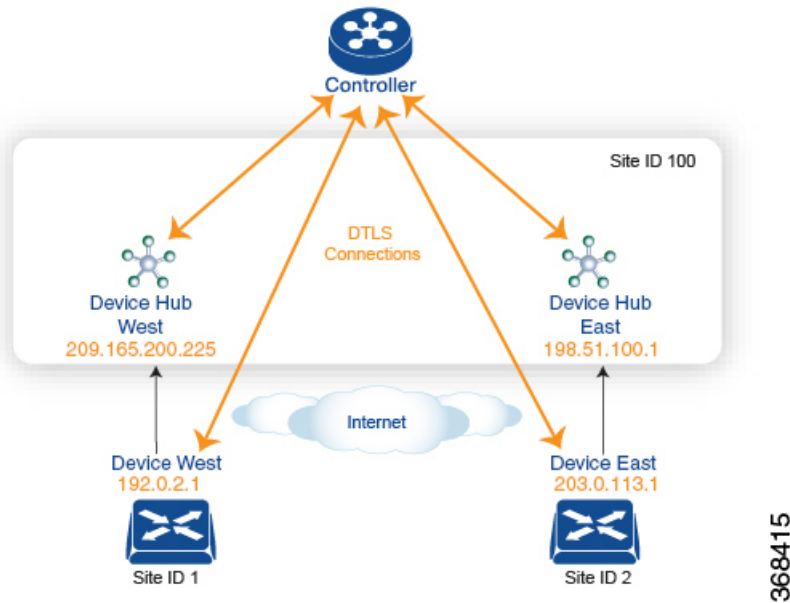
下図は、このようなポリシーがどのように機能するかを示しています。このトポロジには、West と East の 2 つのブランチロケーションがあります。制御ポリシーがプロビジョニングされていない場合、これらの 2 つのデバイスは、デバイス間に IPsec トンネルを作成することで、データトラフィックを直接交換します（赤線で表示）。ここで、West デバイスのルートテーブルには、宛先 TLOC が 203.0.113.1、色が gold（タプル {192.0.2.1, gold}）の East デバイスへのルートが含まれ、East デバイスのルートテーブルには、宛先 TLOC が {203.0.113.1, gold} である West ブランチへのルートが存在します。

ここで、ハブアンドスポークタイプのトポロジを設定するには、制御ポリシーをプロビジョニングして、West および East デバイスがもう一方のデバイス宛てのすべてのデータパケットをハブデバイスに送信するようにします。（制御ポリシーは常に一元管理型であるため、Cisco Catalyst SD-WAN コントローラでプロビジョニングすることに注意してください）。West デバイスでは、ポリシーは単に宛先 TLOC を {203.0.113.1, gold} からハブデバイスの TLOC である {209.165.200.225, gold} に変更し、East デバイスでは、ポリシーは宛先 TLOC を {192.0.2.1, gold} からハブの TLOC である {209.165.200.225, gold} に変更します。ネットワークの West 側と East 側にデータトラフィックを交換する他のブランチサイトがある場合は、これら 2 つの同じ制御ポリシーを適用して、すべてのデータトラフィックをハブを介してリダイレクトすることができます。

トラフィック エンジニアリングの設定

制御ポリシーを使用すると、トラフィック エンジニアリングを設計およびプロビジョニングできます。単純なケースとして、ハブデバイスとして機能する 2 つのデバイスがあるとします。Cisco IOS XE Catalyst SD-WAN デバイス ブランチ宛てのデータトラフィックが常にいずれかのハブデバイスを通過するようにするには、目的のハブデバイスを優先するように TLOC プリファレンス値を設定します。

図 4: トラフィック エンジニアリング トポロジ

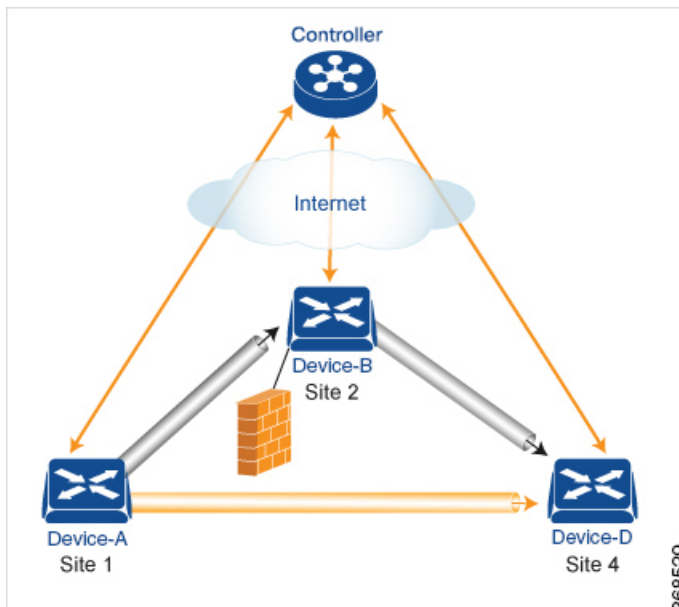


図は、サイト ID 100 に 2 つのハブデバイスがあることを示しています。1 つはネットワークの西側にサービスを提供し、もう 1 つは東側にサービスを提供します。デバイス西ブランチからのデータトラフィックはデバイス西側ハブで処理する必要があり、同様に、デバイス東ブランチからのデータトラフィックはデバイス東側ハブを通過する必要があります。

このトラフィックフローを設計するには、2 つの制御ポリシーをプロビジョニングします。1 つはデバイス西側デバイスが配置されているサイト ID 1 用、もう 1 つはサイト ID 2 用です。サイト ID 1 の制御ポリシーは、デバイス東宛てのトラフィックの TLOC を {209.165.200.225, gold} に変更し、サイト ID 2 の制御ポリシーは、サイト ID 1 宛てのトラフィックの TLOC を {198.51.100.1 gold} に変更します。このトラフィック エンジニアリング ポリシーのもう 1 つの作用は、2 つのハブデバイスを通るトラフィックのロードバランシングです。

このようなトラフィック エンジニアリング ポリシーでは、送信元デバイスから宛先デバイスへのルートがローカルルートテーブルにインストールされ、送信元デバイスと宛先デバイス間のパスが使用可能かどうかに関係なく、トラフィックが宛先に送信されます。最終的な宛先へのパスのエンドツーエンドトラッキングを有効にすると、Cisco Catalyst SD-WAN コントローラは送信元から宛先へのパスをモニターし、そのパスが使用できない場合に送信元デバイスに通知できます。そこで送信元デバイスは、ルートテーブルからそのパスを変更または削除できるのです。

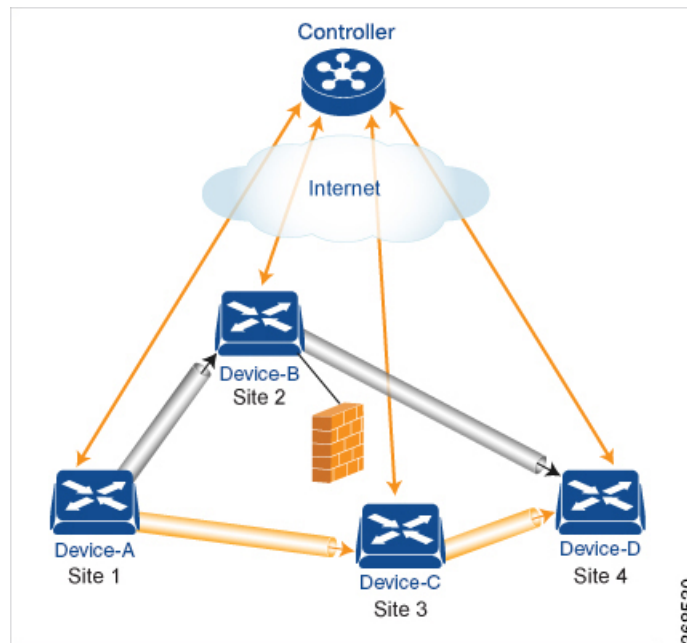
図 5: トラフィック エンジニアリング 2



トラフィック エンジニアリング 2 の図は、エンドツーエンドパス トラッキングを表しています。デバイス A からデバイス D 宛てのトラフィックが最初に中間デバイスであるデバイス B に送信されることを示しているのですが、それは、この中間デバイスがファイアウォールなどのサービスを担っているからでしょう。（サイト 1 のデバイス A に適用される一元管理型制御ポリシーを使用して、このトラフィックエンジニアリングを設定します）。次に、最終的な宛先への直接パスを持つデバイス B がトラフィックをデバイス D に転送します。したがって、この例では、デバイス A とデバイス D の間のエンドツーエンドパスは 2 つのトンネルで構成されます。1 つはデバイス A とデバイス B の間、もう 1 つはデバイス B とデバイス D の間です。Cisco Catalyst SD-WAN コントローラはこのエンドツーエンドパスを追跡し、デバイス B とデバイス D の間のパスの一部が使用できなくなった場合にデバイス A に通知します。

エンドツーエンドパス トラッキングの一部として、中間デバイスを使用した、送信元から最終的な宛先へのトラフィック転送方法は指定できるようになっています。デフォルトの方法は厳密な転送です。この場合、デバイス B にデバイス D への直接パスがあるかどうか、またはデバイス B とデバイス D 間のトンネルが稼働しているかどうかに関わらず、トラフィックは常にデバイス A からデバイス B に送信されます。柔軟な方法としては、一部またはすべてのトラフィックをデバイス A からデバイス D に直接転送するというものもあります。また、1 番目の中間デバイスが到達不能な場合の冗長パスを設けるために 2 番目の中間デバイスを設定し、ECMP 方式を使用して 2 つのデバイス間のトラフィックを転送することもできます。トラフィック エンジニアリング 3 の図では、冗長中間デバイスとして Device-C を追加しています。

図 6: トラフィック エンジニアリング 3



Cisco Catalyst SD-WAN コントローラ で設定する一元管理型制御ポリシーは、OMP ルートおよび OMP TLOC の情報に基づくルーティングポリシーに影響を及ぼします。

複数の Cisco Catalyst SD-WAN コントローラ があるドメインでは、オーバーレイネットワーク内のルーティングを安定させて予測可能な状態のままにしておくために、すべてのコントローラに同じ一元管理型制御ポリシーを設定しておく必要があります。

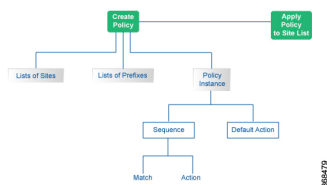
プレフィックスと IP ヘッダーに基づく一元管理型ポリシーの構成

送信元プレフィックスと宛先プレフィックス、および IP パケット内のヘッダーに基づく一元管理型データポリシーは、一連の番号付きの（順番に並んだ）マッチ/アクションペアのシーケンスで構成されます。これらのペアは、シーケンス番号の昇順で評価されます。パケットがマッチ条件のいずれかに一致すると、関連するアクションが実行され、そのパケットに対するポリシー評価が停止します。ポリシーの対象となる項目に対して必要なアクションが実行されるよう、ポリシーを設計する際はこの点に留意するようにしてください。

パケットがポリシー設定のどのシーケンスのパラメータにも一致しない場合、そのパケットはデフォルトではドロップされて廃棄されます。

構成コンポーネント

次の図は、一元管理型データポリシーの構成コンポーネントを示しています。



Cisco Catalyst SD-WAN コントローラ のポリシーコンポーネント

オーバーレイネットワーク全体のポリシーを実装する Cisco SD-WAN コントローラ ポリシーは、Cisco Catalyst SD-WAN 制御コンポーネント に実装されます。Cisco SD-WAN コントローラ は一元化されたデバイスであるため、Cisco SD-WAN コントローラ ポリシーを一元的に管理および維持でき、オーバーレイネットワーク全体でポリシー適用に関する一貫性を確保できます。

Cisco SD-WAN コントローラ ポリシーの実装は、Cisco Catalyst SD-WAN 制御コンポーネント でポリシー全体を設定することで行われます。Cisco SD-WAN コントローラ ポリシー設定は、次の3つの構成要素で実現されます。

- リスト：ポリシーの適用または照合のターゲットを定義します。
- ポリシー定義：制御と転送の側面を制御します。ポリシーには、次のようなさまざまなタイプがあります。
 - app-route-policy (アプリケーション認識型ルーティング用)
 - cflowd-template (cflowd フローモニタリング用)
 - control-policy (ルーティングおよびコントロールプレーン情報用)
 - data-policy (データトラフィック用)
 - vpn-membership-policy (トラフィックの範囲を特定の VPN に制限するため)
- ポリシーの適用：ポリシーの適用対象を制御します。ポリシーの適用はサイトに基づき、サイトリストと呼ばれる特定のリストによって定義されます。

これら3つの構成要素を組み合わせることで Cisco SD-WAN コントローラ のポリシーを作成します。次の表に示すように、ポリシーとは具体的に、1つ以上のリスト、1つのポリシー定義、および少なくとも1つのポリシー適用の組み合わせです。

表 1: Cisco SD-WAN コントローラのポリシーの 3つの構成要素

一覧 (Lists)		ポリシーの定義		ポリシー アプリケーション
data-prefix-list : データポリシーで使用するプレフィックスのリスト prefix-list : 他のポリシーで使用するプレフィックスのリスト site-list : policy と apply-policy で使用する site-id:s のリスト tloc-list : ポリシーで使用する tloc:s のリスト vpn-list : ポリシーで使用する vpn:s のリスト	+	app-route-policy : アプリケーション認識型ルーティングの sla-classes とともに使用 cflowd-template : Cisco IOS XE Catalyst SD-WAN デバイスで cflowd エージェントを設定 control-policy : OMP ルーティング制御を制御 data-policy : VPN 全体のポリシーベースルーティングを提供 vpn-membership-policy : ノード全体の VPN メンバーシップを制御	+	apply-policy : site-list とともに使用して、ポリシーが適用される先を決定
=				
Cisco SD-WAN コントローラ で設定され、Cisco SD-WAN コントローラ または Cisco IOS XE Catalyst SD-WAN デバイス のいずれかで適用されるポリシー定義を完了します。				

一覧 (Lists)

リストとは、関連する項目をまとめて参照できるよう、グループ化する方法です。リストに含める項目の例に、プレフィックス、TLOC、VPN、オーバーレイネットワークサイトなどがあります。Cisco SD-WAN コントローラのポリシーでは、ポリシー定義の作成時と適用時の 2か所でリストを呼び出します。関連項目の定義をポリシーの定義から分離するということは、リストの項目を追加または削除できる際、変更を 1か所でのみ行えるということです。ポリシー定義を使用して変更する必要はありません。したがって、ネットワークに 10 個のサイトを追加し、それらに既存のポリシーを適用する場合は、サイト識別子をサイトリストに追加するだけで適用できます。また、ルールが適用されるプレフィックスや VPNなどを手動で変更することなく、ポリシー規則を変更することもできます。

表 2: リストのタイプ

リストのタイプ	使用方法
data-prefix-list	data-policy で使用され、トラフィック照合用にプレフィックスおよび上位層ポートを個別にまたはまとめて定義します。

リストのタイプ	使用方法
prefix-list	control-policy で使用され、RIB エントリに一致するプレフィックスを定義します。
site-list	control-policy では送信元サイトを照合するために、apply-policy ではポリシー適用のためのサイトを定義するために使用されます。
tloc-list	control-policy で使用され、RIB エントリに一致する TLOC を定義し、再定義された TLOC を vRoutes に適用します。
vpn-list	control-policy では RIB エントリに一致するプレフィックスを定義するために、data-policy と app-route-policy ではポリシー適用のための VPN を定義するために使われます。

次の設定は、Cisco SD-WAN コントローラ ポリシーリストのタイプを示しています。

```

policy
  lists
    data-prefix-list appl
      ip-prefix 209.165.200.225/27 port 100
    !
    prefix-list pfx1
      ip-prefix 209.165.200.225/27
    !
    site-list sitel
      site-id 100
    !
    tloc-list sitel-tloc
      tloc 209.165.200.225 color mpls
    vpn-list vpn1
      vpn1
    !
  !

```

ポリシーの定義

ポリシーの定義では、ポリシー規則を作成します。マッチ条件（制御ポリシーのルート関連プロパティおよびデータポリシーのデータ関連フィールド）と一致したときに実行するアクションを指定します。ポリシーにはマッチ/アクションのペアが含まれ、このペアには番号が付けられ、順番に検査されます。一致が発生するとアクションが実行され、そのルートまたはパケットのポリシー分析が終了します。ポリシー定義のタイプによっては、特定の VPN にのみ適用されます。

表 3: ポリシー タイプ

ポリシータイプ	使用方法
policy-type	control-policy 、 data-policy 、または vpn-membership でポリシーのタイプを指定できます。各タイプには、特定のシンタックスと、特定のマッチ条件および設定可能なアクションのセットがあります。
vpn-list	ポリシーを適用できる VPN をリストするために data-policy および app-route-policy で使用します。
sequence	ポリシーの各シーケンシャルステップをシーケンス番号で定義します。
match	特定のポリシーシーケンスで一致するエンティティを決定します。
action	直前の match ステートメントに対応するアクションを決定します。
default-action	ポリシーのどのシーケンスでも一致しないエンティティに対して実行するアクションです。デフォルトでは、アクションは拒否に設定されています。

次の設定は、Cisco SD-WAN コントローラ ポリシー定義のコンポーネントを示しています。これらの項目は、ポリシーの設計時に使用すべき論理的な順序でリストされています。また、設定に項目を追加する順序に関係なく、設定ではこの順序で項目が表示されます。

```

policy
  policy-type name
  vpn-list vpn-list
  sequence number
  match
    <route | tloc vpn | other>
  !
  action <accept reject drop>
  set attribute value
  !
  default-action <reject accept>
  !
  !
  !

```

ポリシー アプリケーション

設定コンポーネントは次のとおりです。

コンポーネント	使用方法
site-list	指定されたポリシーが適用されるサイトを決定します。方向 (in out) は、control-policy にのみ適用されます。
policy-type	ポリシータイプは control-policy 、 data-policy 、または vpn-membership で、名前はセクションの site-list で指定されたサイトに適用される設定済みのポリシーを参照します。

ポリシー定義を有効にするには、オーバーレイネットワーク内のサイトに関連付けます。

```

apply-policy
  site-list name
    control-policy name <inout>
  !
  site-list name
    data-policy name
    vpn-membership name
  !
  !
  
```

ポリシーの例

リスト、ポリシー定義、ポリシー適用で構成される完全なポリシーです。次の例では、2つのリスト (**site-list** と **tloc-list**) を作成します。1つのポリシー (制御ポリシー) を定義し、そのポリシーを **site-list** に適用します。この図では、ノード設定で表示される項目がリストされています。通常の設定プロセスでは、最初にリストを作成し (使用するすべてのものをグループ化)、次にポリシー自体を定義し (実行することを定義)、最後にポリシーを適用します (設定したポリシーが適用されるサイトを指定)。

```

apply-policy
  site-list sitel -----> Apply the defined policy towards the sites in site-list
    control-policy prefer_local out
  !
policy
  lists
  site-list sitel
    site-id 100
  tloc-list prefer_sitel ----> Define the lists required for apply-policy and for use
  within the policy
    tloc 192.0.2.1 color mols encaps ipsec preference 400
  control-policy prefer_local
    sequence 10
    match route
      site-list sitele ----->Lists previously defined used within policy
  !
  action accept
    set
      tloc-list prefer_site
  !
  !
  !
  
```

ポリシーで使用される TLOC 属性

トランスポートロケーション (TLOC) は、オーバーレイネットワーク内の特定のインターフェイスを定義します。各 TLOC は、Cisco IOS XE Catalyst SD-WAN デバイス 間の OMP 更新で交換される一連の属性で構成されます。各 TLOC は、IP アドレス、色、およびカプセル化の 3 タプルによって一意に識別されます。他の属性を TLOC に関連付けることができます。

次にリスト表示した TLOC 属性は、Cisco SD-WAN コントローラ のポリシーで照合または設定できます。

表 4:

TLOC 属性	機能	アプリケーションポイント 設定元	アプリケーションポイント 変更元
アドレス (IP アドレス)	インターフェイスが配置されている送信元デバイスのシステム IP アドレスです。	送信元デバイスの設定	control-policy data-policy
キャリア	キャリアタイプの識別子。主に、トランスポートがパブリックかプライベートかを示します。	送信元デバイスの設定	control-policy
色	TLOC タイプの識別子です。	送信元デバイスの設定	control-policy data-policy
ドメイン ID	オーバーレイ ネットワーク ドメインの識別子です。	送信元デバイスの設定	control-policy
カプセル化	トンネルのカプセル化 (IPsec または GRE のいずれか) です。	送信元デバイスの設定	control-policy data-policy
発信元 (Originator)	発信元ノードのシステム IP アドレスです。	任意の発信者の設定	control-policy
[優先順位 (Preference)]	OMP path-selection の設定。値が大きいほど、優先パスが高くなります。	送信元デバイスの設定	control-policy
サイト ID	特定のサイトの ID。サイトには、複数のノードまたは TLOC を設定できます。	送信元デバイスの設定	control-policy
Tag	任意による TLOC 識別子です。	送信元デバイスの設定	control-policy

ポリシーで使用される Cisco Catalyst SD-WAN ルート属性

Cisco Catalyst SD-WAN ルートは、オーバーレイネットワークのルートを定義したものです。標準 IP ルートに似ていますが、TLOC 属性と VPN 属性があります。OMP アップデート時には、Cisco IOS XE Catalyst SD-WAN デバイス でルート交換が行われます。

次にリスト表示したルート属性は、Cisco SD-WAN コントローラ ポリシーで照合または設定できます。

表 5:

ルート属性	機能	アプリケーションポイント 設定元	アプリケーションポイント 変更元
Origin	ルートの送信元 (BGP、OSPF、接続、静的のいずれか)。	送信元デバイス	control-policy
発信元 (Originator)	ルートを伝送するアップデートの送信元。	発信元	control-policy
[優先順位 (Preference)]	OMP path-selection の設定。値が大きいほど、優先パスが高くなります。	送信元デバイスまたはポリシーの設定	control-policy
サービス	ルートに関連付けられているアドバタイズされたサービス。	送信元デバイスの設定	control-policy
サイト ID	特定のサイトの識別子。サイトには、複数のノードまたは TLOC を設定できます。	送信元デバイスの設定	control-policy
Tag	任意による識別。	送信元デバイスの設定	control-policy
TLOC	ルートのネクストホップとして使用される TLOC。	送信元デバイスまたはポリシーの設定	control-policy data-policy
[VPN]	ルートが属する VPN。	送信元デバイスまたはポリシーの設定	control-policy data-policy

Cisco Catalyst SD-WAN コントローラ ポリシー処理と適用の設計

Cisco SD-WAN コントローラ ポリシーがどのように処理および適用されるかを理解することで、ポリシーを適切に設計し、オーバーレイネットワーク全体でポリシーを実装する方法を評価できます。

ポリシーは次のように処理されます。

- ポリシー定義は、番号付きで番号順に並んだ一連のマッチ/アクションペアで構成されます。各ポリシー内では、ペアリングは、最小の番号から始まり、番号順に処理されます。
- 一致があった場合、一致したエンティティはシーケンスの設定されたアクションの対象になり、その後継続的な処理の対象にはなりません。
- シーケンスで一致しないエンティティは、ポリシーのデフォルトアクションの対象になります。デフォルトでは、このアクションは拒否されます。

Cisco SD-WAN コントローラ ポリシーはサイトリストごとに適用されるため、次のようになります。

- サイトリストにポリシーを適用する場合は、各タイプのポリシーを1つだけ適用できます。たとえば、1つの制御ポリシーと1つのデータポリシー、または1つの制御ポリシーを入力し、1つの制御ポリシーを出力することができます。2つのデータポリシーまたは2つのアウトバウンド制御ポリシーを設定することはできません。
- サイトリストは多数のサイトをグループ化したものであるため、1つのサイトを複数のサイトリストに含める場合は注意が必要です。サイトリストにさまざまなサイト識別子が含まれている場合は、重複がないことを確認します。同じサイトが2つのサイトリストに属し、同じタイプのポリシーが両方のサイトリストに適用されている場合、ポリシーの動作は予測できず、致命的となる可能性があります。
- 制御ポリシーは単方向であり、Cisco SD-WAN コントローラ へのインバウンドまたはアウトバウンドのいずれかに適用されます。両方向で制御ポリシーが必要な場合は、2つの制御ポリシーを設定します。
- データポリシーは双方向であり、Cisco IOS XE Catalyst SD-WAN デバイスのサービス側から受信したトラフィック、トンネル側から受信したトラフィック、またはこれらすべての組み合わせに適用できます。
- VPN メンバーシップポリシーは、Cisco SD-WAN コントローラ からの発信トラフィックに常に適用されます。
- 制御ポリシーはCisco SD-WAN コントローラ に残り、コントローラ が送受信するルートに影響します。

- データポリシーは、サイトリスト内の Cisco IOS XE Catalyst SD-WAN デバイスに送信されます。ポリシーは OMP 更新で送信され、デバイスが送受信するデータトラフィックに影響します。
- オーバーレイネットワーク内のいずれかのノードがルーティングを決定する場合、使用可能なすべてのルーティング情報を使用します。オーバーレイネットワークで、ルーティング情報を Cisco IOS XE Catalyst SD-WAN デバイス ノードに配布するのは Cisco Catalyst SD-WAN コントローラ です。
- 複数の Cisco Catalyst SD-WAN コントローラ があるネットワーク展開では、各コントローラが独立して動作し、ルーティング情報を他の Cisco SD-WAN コントローラ およびオーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイスに伝達します。したがって、Cisco SD-WAN コントローラ ポリシーがオーバーレイネットワークで目的の効果を持つようにするには、Cisco SD-WAN コントローラ のそれぞれに同じポリシーを設定し、同じように適用する必要があります。どのポリシーでも、同じポリシーを設定し、すべての Cisco SD-WAN コントローラ に同じように適用する必要があります。



- (注) ポリシーを展開すると、展開ステータスはポリシーのタイムアウト制限である 30 分間のみ更新されます。タイムアウト期間が経過すると、展開タスクのステータスはモニタリングされません。行数が多く、より大きなポリシーを展開し、それが 30 分以上かかる場合、タスクのステータスはモニタリングされません。

Cisco Cisco Catalyst SD-WAN コントローラによるポリシーの運用

大まかに説明すると、制御ポリシーとは、ルーティング情報という、Cisco IOS XE Catalyst SD-WAN ネットワークで OMP アップデートの際に伝送される情報をもとに操作を行うポリシーです。データポリシーはデータトラフィックに影響を及ぼすものであり、VPN メンバーシップは VPN ルーティングテーブルの配布を制御するものです。

基本的な Cisco SD-WAN コントローラ ポリシーは次のとおりです。

- 制御ポリシー
- データポリシー
- VPN メンバーシップ

制御ポリシー

制御ポリシーは標準的なルーティングポリシーに類似し、オーバーレイネットワークのコントロールプレーンのルートおよびルーティング情報に作用します。Cisco SD-WAN コントローラ でプロビジョニングされる一元管理型制御ポリシーは、オーバーレイネットワークを介した

ルーティングパスを決定または影響を与えるネットワーク全体のルーティング決定をカスタマイズするための Cisco Catalyst SD-WAN の技術です。Cisco IOS XE Catalyst SD-WAN デバイスでプロビジョニングされるローカル制御ポリシーを使用すると、サイトローカルブランチまたはエンタープライズ ネットワークで BGP および OSPF によって行われるルーティングの決定をカスタマイズできます。

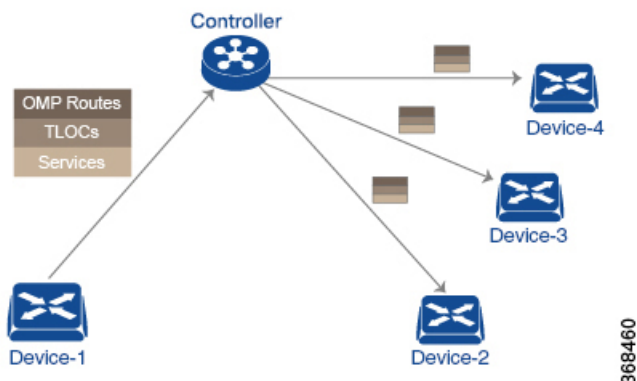
一元管理型制御ポリシーの基礎となるルーティング情報は、Cisco IOS XE Catalyst SD-WAN ルートアドバタイズメントで伝送され、Cisco SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス 間の DTLS または TLS 制御接続で送信されます。一元管理型制御ポリシーによって、Cisco SD-WAN コントローラ の一元管理型ルートテーブルに配置されるルートおよびルート情報、およびオーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイスにアドバタイズされるルートおよびルート情報が決定されます。基本的な一元管理型制御ポリシーはトラフィックエンジニアリングを確立し、トラフィックがネットワークを通過するパスを設定します。高度な制御ポリシーは、オーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイスがファイアウォールやロードバランサなどのネットワークサービスを共有できるようにする、多数の機能をサポートしています。

一元管理型制御ポリシーは、Cisco SD-WAN コントローラ によってオーバーレイネットワーク全体に配信される OMP ルートに影響します。Cisco SD-WAN コントローラ は、Cisco SD-WAN コントローラ とデバイス間の DTLS または TLS 接続内の OMP セッションを介して Cisco IOS XE Catalyst SD-WAN デバイス によってアドバタイズされた OMP ルートから、オーバーレイネットワーク トポロジを学習します。

3つのタイプの OMP ルートは、Cisco SD-WAN コントローラ がネットワークトポロジを決定するために使用する情報を伝送します。

- Cisco Catalyst SD-WAN OMP ルートは IP ルートアドバタイズメントに類似しており、デバイスがローカルサイトから学習したルーティング情報と、ローカルルーティングプロトコル (BGP および OSPF) を Cisco SD-WAN コントローラ にアドバタイズします。これらのルートは、OMP ルートまたはルートとも呼ばれます。
- TLOC ルートは、トランスポートネットワークに接続するインターフェイスの IP アドレス、トラフィックフローを識別するリンクの色、カプセル化タイプなど、オーバーレイネットワーク固有のロケータプロパティを伝送します。(TLOC (トランスポートロケーション) は、Cisco IOS XE Catalyst SD-WAN デバイスがトランスポートネットワークに接続する物理的なロケーションを意味します。IP アドレス、リンクの色、カプセル化によって主に識別されますが、他にも多くのプロパティが TLOC に関連付けられます)。
- サービスルートは、ローカルサイトの VPN メンバーが使用できるファイアウォールなどのネットワークサービスをアドバタイズします。

図 7: 制御ポリシーのトポロジ



デフォルトでは、一元管理型制御ポリシーはプロビジョニングされません。ポリシーがまったく適用されていないネットワークでは、すべての OMP ルートがそのまま Cisco SD-WAN コントローラのルートテーブルに配置され、Cisco SD-WAN コントローラはすべての OMP ルートをそのまま、ネットワークドメイン内の同一 VPN 内のあらゆるデバイスにアドバタイズします。

一元管理型制御ポリシーをプロビジョニングすることで、Cisco SD-WAN コントローラのルートテーブルに配置される OMP ルート、デバイスにアドバタイズされるルート情報、および OMP ルートの変更をルートテーブルへの配置前またはアドバタイズ前にするかどうかに影響を与えることができます。

Cisco IOS XE Catalyst SD-WAN デバイスは、Cisco SD-WAN コントローラから学習したすべてのルート情報をそのままローカルルートテーブルに配置して、データトラフィックの転送時に使用します。Cisco SD-WAN コントローラの役割はネットワーク内の一元化されたルーティングシステムであるため、Cisco IOS XE Catalyst SD-WAN デバイスは、Cisco SD-WAN コントローラから学習した OMP ルート情報を変更することはできません。

Cisco SD-WAN コントローラはデバイスから OMP ルートアドバタイズメントを定期的に受信し、オーバーレイネットワークを介してルーティングパスを再計算および更新した後、新しいルーティング情報をデバイスにアドバタイズします。

Cisco SD-WAN コントローラでプロビジョニングした一元管理型制御ポリシーはCisco SD-WAN コントローラに残り、デバイスにダウンロードされることはありません。ただし、一元管理型制御ポリシーの結果としてのルーティングの決定は、ルートアドバタイズメントの形でデバイスに渡されるため、制御ポリシーの影響は、デバイスがデータトラフィックを宛先に転送する方法に反映されます。

デバイス上でローカルにプロビジョニングされるローカライズ型制御ポリシーは、ルートポリシーと呼ばれます。このポリシーは、通常のドライバで設定するルーティングポリシーに似ており、サイトとローカル間ネットワークでの BGP および OSPF ルーティング動作を変更できるようにします。一元管理型制御ポリシーはオーバーレイネットワーク全体のルーティング動作に影響しますが、ルートポリシーはローカルブランチのルーティングにのみ適用されます。

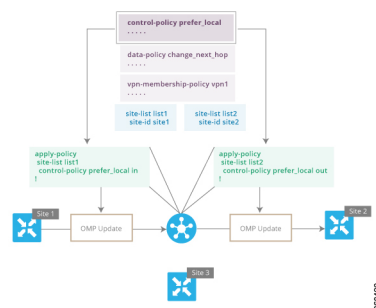
Cisco IOS XE Catalyst SD-WAN デバイスは OMP アップデートを定期的に交換し、オーバーレイネットワークに関するルーティング情報を伝送します。これらのアップデートには、ルート属性とトランスポートロケーション (TLOC) 属性の 2 つが含まれます。

Cisco SD-WAN コントローラは、OMP アップデートによるこれらの属性からオーバーレイネットワークのトポロジとステータスを判断し、オーバーレイネットワークに関するルーティング情報をルートテーブルにインストールします。次に、コントローラは OMP アップデートを送信することで、ネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイスにオーバーレイトポロジをアドバタイズします。

制御ポリシーは、OMP アップデートに含まれるルート属性と TLOC 属性を調べて、ポリシーに一致する属性を変更できます。制御ポリシーによる変更は、インバウンドまたはアウトバウンドのいずれかの方向に適用されます。

この図は、Cisco SD-WAN コントローラ に設定された **prefer_local** という制御ポリシーを、サイト 1 (site-list list1 経由) とサイト 2 (site-list list2 経由) に適用したものです。

図 8: 制御ポリシーのトポロジ



```
Device# apply-policy
site-list list1
control-policy prefer_local in
!
```

左上の矢印は、ポリシーがサイト 1、具体的にはサイト 1 のエントリを含む **site-list list1** に適用されていることを示しています。コマンド **control-policy prefer_local** は、Cisco IOS XE Catalyst SD-WAN デバイス から Cisco SD-WAN コントローラ に入ってくる OMP アップデートにポリシーを適用するために使用されます。これは、コントローラからはインバウンドにあたります。**in** キーワードは、**inbound** ポリシーを示します。そのため、サイト 1 のデバイスが Cisco SD-WAN コントローラ に送信するすべての OMP アップデートにおいて、「prefer_local」制御ポリシーは、アップデートが Cisco SD-WAN コントローラ のルートテーブルに到達する前に適用されます。OMP アップデートのルートまたは TLOC 属性がポリシーと一致する場合、Cisco SD-WAN コントローラ が OMP アップデート情報をルートテーブルにインストールする前に、ポリシーアクションの結果としての変更が発生します。

Cisco SD-WAN コントローラ のルートテーブルは、オーバーレイネットワークのトポロジを決定するために使用されます。次に、Cisco SD-WAN コントローラ はこのトポロジ情報を OMP アップデートを介してネットワーク内のすべてのデバイスに配信します。ポリシーをインバウンド方向に適用すると、Cisco SD-WAN コントローラ で使用可能な情報に影響を与えるためです。これはネットワークトポロジとネットワークの到達可能性を決定し、ルート属性と TLOC 属性をコントローラのルートテーブルに配置する前に変更します。

```

apply-policy
site-list list2
control-policy prefer_local out
!

```

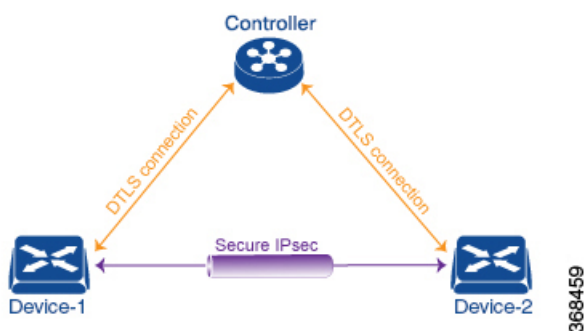
上の図の右側では、**control-policy prefer_local out** コマンドにより「prefer_local」ポリシーがサイト2に適用されています。コマンドの **out** キーワードは、**outbound policy** を示します。これは、Cisco SD-WAN コントローラ がサイト2のデバイスに送信する OMP アップデートにポリシーが適用されることを意味します。ポリシーに起因する変更は、Cisco SD-WAN コントローラのルートテーブルからの情報が OMP アップデートに配置された後、デバイスがアップデートを受信する前に発生します。方向はここでも、Cisco SD-WAN コントローラの観点からはアウトバウンドであることに注意してください。

Cisco SD-WAN コントローラ 上の一元化されたルートテーブルに影響し、オーバーレイネットワーク内のすべてのデバイスにアドバタイズされるルート属性に広く影響するインバウンドポリシーとは対照的です。アウトバウンド方向に適用される制御ポリシーは、サイトリストに含まれる個々のデバイス上のルートテーブルにのみ影響します。

同じ制御ポリシー（**prefer_local** ポリシー）が、インバウンドとアウトバウンドの両方の OMP アップデートに適用されます。ただし、同じポリシーをインバウンドとアウトバウンドに適用した場合の影響は異なります。図に示す使用方法は、Cisco IOS XE Catalyst SD-WAN 制御ポリシー設計のアーキテクチャと構成の柔軟性を示しています。

データポリシー

データポリシーは、パケットの IP ヘッダー内のフィールド、またはトラフィックが送受信されるルータインターフェイスのいずれかに基づいて、ネットワークを通過するデータトラフィックのフローに影響を与えます。データトラフィックは、隣接する図に紫色で示されている Cisco IOS XE Catalyst SD-WAN デバイス 間の IPsec 接続を介して移動します。

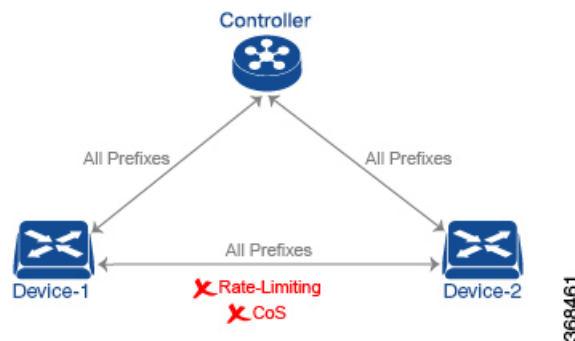


この Cisco IOS XE Catalyst SD-WAN アーキテクチャでは、次の2種類のデータポリシーを実装します。

- パケットの IP ヘッダー（5 タプルと呼ばれる）の送信元アドレスと宛先アドレス、ポート、および DSCP フィールドに基づいて、そしてネットワークセグメンテーションと VPN メンバーシップを基に、データトラフィックのフローを制御する一元管理型データポリシー。こうしたタイプのデータポリシーは、Cisco SD-WAN コントローラ で一元的にプロビジョニングされ、ネットワーク全体のトラフィックフローに影響を与えます。

- Cisco IOS XE Catalyst SD-WAN デバイス 上のインターフェイスおよびインターフェイスキューに出入りするデータトラフィックのフローを制御するローカライズ型データポリシー。このタイプのデータポリシーは、アクセスリストを使用してローカルにプロビジョニングされます。トラフィックを分類し、異なるクラスを異なるキューにマッピングできます。また、トラフィックをミラーリングし、データトラフィックの送受信レートをポリシーリングすることもできます。

デフォルトでは、一元管理型データポリシーはプロビジョニングされません。そのため、VPN 内のすべてのプレフィックスは、その VPN 内のどこからでも到達可能になります。一元管理型データポリシーをプロビジョニングすると、送信元と宛先間のアクセスを制御する 6 タプルフィルタを適用できます。



一元管理型制御ポリシーと同様に、一元管理型データポリシーを Cisco SD-WAN コントローラにプロビジョニングすると、その設定は Cisco SD-WAN コントローラに残ります。データポリシーの効果は、Cisco IOS XE Catalyst SD-WAN デバイスによるデータトラフィックを宛先に転送する方法に反映されます。ただし、制御ポリシーとは異なり、一元管理型データポリシーは読み取り専用でデバイスにプッシュされます。これらはルータの構成ファイルには追加されませんが、ルータの CLI から表示できます。

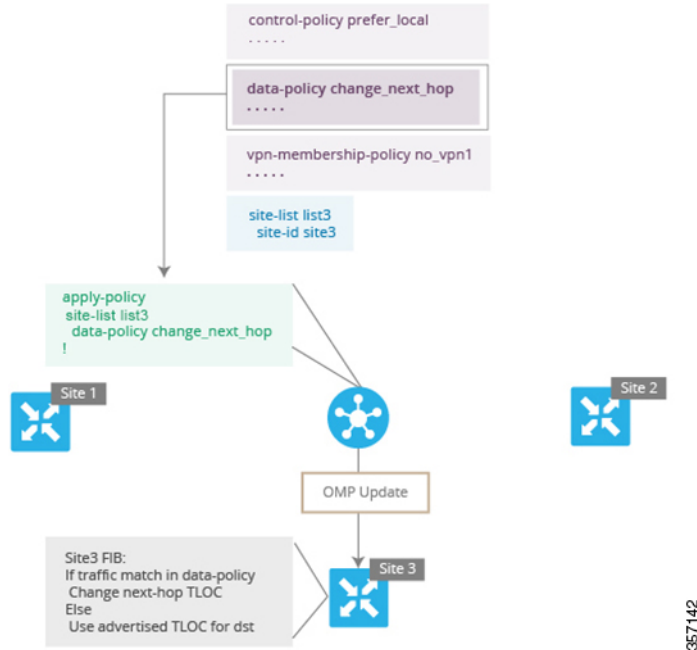
Cisco IOS XE Catalyst SD-WAN デバイスにアクセスリストがプロビジョニングされていない場合、すべてのデータトラフィックは、インターフェイスのキューの 1 つを使用して、ラインレートで同じ重要度をもって送信されます。アクセスリストを使用すると、サービスクラスをプロビジョニングできます。これにより、データトラフィックを重要度で分類して、複数のインターフェイスキューに展開させ、さまざまなクラスのトラフィックの送信レートを制御できるようになります。ポリシーもプロビジョニングできます。

データポリシーは、送信元と宛先のアドレスとポート、プロトコル、DSCP 値を参照してデータパケットのヘッダー内のフィールドを調査します。マッチするパケットについては、さまざまな方法でネクストホップを変更するか、パケットにポリシーを適用します。データポリシーが Cisco SD-WAN コントローラで設定および適用されると、ポリシーが適用されるサイトリスト内の Cisco IOS XE Catalyst SD-WAN デバイスに OMP アップデートで送信されます。データトラフィックを送受信するときに、マッチ操作とその結果に伴うアクションがデバイス上で実行されます。

データポリシートポロジの図では、「change_next_hop」という名前のデータポリシーが、サイト 3 を含むサイトのリストに適用されます。Cisco SD-WAN コントローラがサイト 3 のデバイスに送信する OMP 更新には、このポリシー定義が含まれています。デバイスは、ポリシーに

マッチするデータトラフィックを送受信すると、ネクストホップを指定された TLOC に変更します。マッチしないトラフィックは、元のネクストホップ TLOC に転送されます。

図 9: データポリシートポロジ



データポリシーの `apply-policy` コマンドで、デバイスから見た方向を指定します。図の「all」方向では、トンネルインターフェイスを通過するインバウンドおよびアウトバウンドデータトラフィックに対し、ポリシーが適用されます。`data-policy change_next_hop from-tunnel` コマンドを使用してポリシーのスパンをインバウンドトラフィックのみに制限したり、`data-policy change_next_hop from-service` コマンドを使用してアウトバウンドトラフィックのみに制限したりできます。

VPN メンバーシップポリシーの運用

VPN メンバーシップポリシーは、その名前が示すように、特定の Cisco IOS XE Catalyst SD-WAN デバイスに配布される VPN ルートテーブルに影響します。VPN メンバーシップポリシーのないオーバーレイネットワークでは、Cisco Catalyst SD-WAN コントローラはすべての VPN のルートをすべてのデバイスにプッシュします。ビジネス使用モデルで特定の VPN への特定のデバイスの参加を制限する場合は、VPN メンバーシップポリシーを使用してこの制限を適用します。

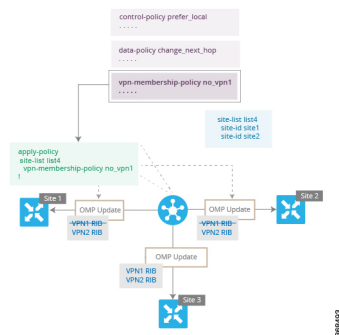
下図のVPN メンバーシップトポロジは、VPN メンバーシップポリシーの仕組みを示しています。このトポロジには、3つの Cisco IOS XE Catalyst SD-WAN デバイスがあります。

- サイト 1 および 2 の Cisco IOS XE Catalyst SD-WAN デバイスは、VPN 2 のみにサービスを提供します。

- サイト 3 の Cisco IOS XE Catalyst SD-WAN デバイスは、VPN 1 と VPN 2 の両方にサービスを提供します。

この図では、サイト 3 のデバイスは Cisco SD-WAN コントローラ からすべてのルート更新を受信します。これは、これらの更新が VPN 1 と VPN 2 の両方に対するものであるためです。ただし、他の Cisco IOS XE Catalyst SD-WAN デバイスは VPN 2 のみにサービスを提供するため、これらに送信されたルート更新をフィルタリングし、VPN 1 に関連付けられているルートを削除して、VPN 2 に適用されるルートのみを送信できます。

図 10: VPN メンバーシップトポロジ





ここでは、VPN メンバーシップポリシーを適用するときに方向が設定されていないことに注意してください。Cisco SD-WAN コントローラは、Cisco IOS XE Catalyst SD-WAN デバイスの外部に送信する OMP 更新に常にこのタイプのポリシーを適用します。

Cisco SD-WAN コントローラ ポリシーの設定と実行

すべての Cisco SD-WAN コントローラ ポリシーの設定は、ポリシーの定義とリストの組み合わせを使用して、Cisco IOS XE Catalyst SD-WAN デバイスに対して行われます。すべての Cisco SD-WAN コントローラ ポリシーの適用も、apply-policy とリストを組み合わせ、Cisco IOS XE Catalyst SD-WAN デバイスに対して行われます。ただし、次の図に示すように、実際の Cisco SD-WAN コントローラ ポリシーが実行される場所はポリシーのタイプによって異なります。

図 11: Cisco SD-WAN コントローラ ポリシー

 Controller	Action	App-route Policy	Cflowd Template	Control Policy	Data Policy	VPN Membership Policy
	Configure	✓	✓	✓	✓	✓
	Apply	✓	✓	✓	✓	✓
	Execute			✓		✓

 Device	Action	App-route Policy	Cflowd Template	Control Policy	Data Policy	VPN Membership Policy
	Configure					
	Apply					
	Execute	✓	✓		✓	

366503

制御ポリシーと VPN メンバーシップポリシーの場合、ポリシー設定全体は Cisco SD-WAN コントローラに残り、ポリシーにマッチするルートまたはVPNの結果として実行されるアクションは Cisco SD-WAN コントローラ で実行されます。

他の3つのポリシータイプ（アプリケーション認識型ルーティング、cflowd テンプレート、およびデータポリシー）の場合、ポリシーは OMP 更新で Cisco IOS XE Catalyst SD-WAN デバイスに送信され、ポリシーの結果として実行されるアクションはデバイスで実行されます。



第 4 章

一元管理型ポリシー



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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、さまざまなタイプの一元管理型ポリシー、一元管理型ポリシーのコンポーネント、Cisco SD-WAN Manager および CLI を使用した一元管理型ポリシーの設定方法に関する概要を提供します。

- [一元管理型ポリシーの概要 \(35 ページ\)](#)
- [Cisco SD-WAN Manager を使用した一元管理型ポリシーの設定 \(37 ページ\)](#)
- [CLI を使用した、一元管理型ポリシーの設定 \(82 ページ\)](#)
- [一元管理型ポリシーの設定例 \(86 ページ\)](#)

一元管理型ポリシーの概要

一元管理型ポリシーとは、Cisco SD-WAN コントローラ 上でプロビジョニングされるポリシーのことであり、Cisco Catalyst SD-WAN オーバーレイネットワーク内の一元管理型コントローラです。

一元管理型ポリシーのタイプ

一元管理型制御ポリシー

一元管理型制御ポリシーは、Cisco Catalyst SD-WAN コントローラ のルートテーブルに保存され、Cisco IOS XE Catalyst SD-WAN デバイス にアドバタイズされる情報に影響を与えることによって、トラフィックのネットワーク全体のルーティングに適用されます。一元管理型制御ポリシーの効果は、Cisco IOS XE Catalyst SD-WAN デバイス がオーバーレイネットワークのデータトラフィックを宛先に送信する方法に見られます。



(注) 一元管理型制御ポリシーの設定自体は Cisco Catalyst SD-WAN コントローラ に残り、ローカルデバイスにプッシュされることはありません。

一元管理型データポリシー

一元管理型データポリシーは、オーバーレイネットワーク内の VPN 全体のデータトラフィックのフローに適用されます。これらのポリシーは、6タプルの一致（送信元と宛先の IP アドレスとポート、DSCP フィールド、プロトコル）または VPN メンバーシップのいずれかに基づいてアクセスを許可および制限できます。これらのポリシーは、選択した Cisco IOS XE Catalyst SD-WAN デバイス にプッシュされます。

パケットヘッダーフィールドに基づく一元管理型データポリシー

データトラフィックに影響を与えるポリシーの決定は、パケットヘッダーフィールド、具体的には送信元と宛先の IP プレフィックス、送信元と宛先の IP ポート、プロトコル、および DSCP に基づいて行うことができます。

このタイプのポリシーは、ネットワーク内のトラフィックフローを変更するためによく使用されます。次に、一元管理型データポリシーで実行できる制御のタイプの例をいくつか示します。

- ローカルサイト外の任意の宛先にトラフィックを送信できる送信元のセット。たとえば、このようなデータポリシーによって拒否されたローカル送信元は、ローカルネットワーク上のホストとのみ通信できます。
- ローカルサイト外の特定の宛先セットにトラフィックを送信できる送信元のセット。たとえば、このタイプのデータポリシーに一致するローカル送信元は、あるパスを介して音声トラフィックを送信し、別のパスを介してデータトラフィックを送信できます。
- ローカルサイト外の任意の宛先、または特定の宛先の特定のポートにトラフィックを送信できる送信元アドレスと送信元ポート。

Cisco SD-WAN Manager を使用した一元管理型ポリシーの設定

一元管理型ポリシーを設定するには、Cisco SD-WAN Manager の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操作で構成されています。

- [対象グループの作成 (Create 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。
- [トポロジとVPNメンバーシップの設定 (Configure Topology and VPN Membership)] : ポリシーによって適用されるネットワーク構造を作成します。
- [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。
- [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。
- 一元管理型ポリシーをアクティブ化します。
一元管理型ポリシーを有効にするには、ポリシーをアクティブ化する必要があります。

Cisco SD-WAN Manager を使用して一元管理型ポリシーを設定するには、このセクションに続く手順で示すステップを実行します。

ポリシー構成ウィザードの開始

ポリシー構成ウィザードを開始するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、[**Configuration**] > [**Policies**] を選択します。
2. [**Centralized Policy**] をクリックします。
3. [**Add Policy**] をクリックします。

ポリシー構成ウィザードが表示され、[対象グループの作成 (Create Groups of Interest)] ウィンドウが表示されます。

一元管理型ポリシーの対象グループの構成

[対象グループの作成 (Create Groups of Interest)] で、次のセクションの説明に従って、一元管理型ポリシーで使用するリストタイプの新しいグループを作成します。

アプリケーションの構成

1. 対象グループのリストで、[アプリケーション (Application)] をクリックします。

2. [新しいアプリケーションリスト (New Application List)]をクリックします。
3. リストの名前を入力します。
4. [アプリケーション (Application)]または[アプリケーションファミリ (Application Family)]を選択します。

アプリケーションには、サードパーティのコントローラ、**ABC News**、**Mircosoft Teams** など、1つ以上のアプリケーションの名前を指定できます。Cisco IOS XE Catalyst SD-WAN デバイスでは、約 2300 の異なるアプリケーションをサポートしています。サポートされているアプリケーションを一覧表示するには、CLI で ? と入力します。

アプリケーションファミリは、次のうちの1つ以上となります：**antivirus**、**application-service**、**audio_video**、**authentication**、**behavioral**、**compression**、**database**、**encrypted**、**erp**、**file-server**、**file-transfer**、**forum**、**game**、**instant-messaging**、**mail**、**microsoft-office**、**middleware**、**network-management**、**network-service**、**peer-to-peer**、**printer**、**routing**、**security-service**、**standard**、**telephony**、**terminal**、**thin-client**、**tunneling**、**wap**、**web**、および **webmail**。

5. [選択 (Select)]ドロップダウンの[検索 (Search)]フィルタで、必要なアプリケーションまたはアプリケーションファミリを選択します。
6. [Add]をクリックします。

いくつかのアプリケーションリストは事前設定済みです。これらのリストを編集または削除することはできません。

Microsoft_Apps—Excel、Skype、XboxなどのMicrosoftアプリケーションが含まれます。Microsoftアプリケーションの完全なリストを表示するには、[エン트리 (Entries)]列のリストをクリックします。

Google_Apps—Gmail、Google マップ、YouTubeなどのGoogleアプリケーションが含まれます。Googleアプリケーションの完全なリストを表示するには、[エン트리 (Entries)]列のリストをクリックします。

カラーの設定

1. 対象グループのリストで、[色 (Color)]をクリックします。
2. [新しいカラーリスト (New Color List)]をクリックします。
3. リストの名前を入力します。
4. [色の選択 (Select Color)]ドロップダウンの[検索 (Search)]フィルタで、必要な色を選択します。

色は 3g、biz-internet、blue、bronze、custom1 ~ custom3、default、gold、green、lte、metro-ethernet、mpls、private1 ~ private6、public-internet、red、silver から選択できます。

5. [Add]をクリックします。

1つのリストで複数の色を構成するには、ドロップダウンから複数の色を選択します。

コミュニティの設定

表 6: 機能の履歴

機能名	リリース情報	説明
コミュニティの照合および設定機能	<p>Cisco SD-WAN リリース 20.5.1</p> <p>Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a</p> <p>Cisco vManage リリース 20.5.1</p>	<p>この機能では、制御ポリシーを使用してコミュニティを照合および設定できます。制御ポリシーは Cisco IOS XE Catalyst SD-WAN デバイスデバイス上で定義および適用され、コミュニティを操作します。</p> <p>この機能を使用すると、操作可能なルーティングポリシーを基に単一または複数の BGP コミュニティタグをプレフィックスと照合し、割り当てることができます。</p>

コミュニティリストは、ルートマップの **match** 句で使用するコミュニティのグループ作成に使用されるリストです。コミュニティリストは、ルートの受け入れ、優先、配布、またはアドバタイズの制御に使用できます。また、コミュニティリストは、ルートのコミュニティの設定、追加または変更にも使用できます。

1. [対象グループ (Group of Interest)] リストで、[コミュニティ (Community)] をクリックします。
2. [新しいコミュニティリスト (New Community List)] をクリックします。
3. コミュニティリストの名前を入力します。
4. [標準 (Standard)] または [拡張 (Expanded)] を選択します。
 - 標準コミュニティリストは、コミュニティやコミュニティ番号の指定に使用されません。
 - 拡張コミュニティ リストは正規表現によるフィルタ コミュニティに使用されます。正規表現は、コミュニティ属性にマッチするパターンを指定するために使用されません。
5. [コミュニティの追加 (Add Community)] フィールドに、次のいずれかの形式で、1つ以上のデータプレフィックスをコンマで区切って入力します。
 - **aa:nn** : 自律システム (AS) 番号とネットワーク番号。各番号は、1 ~ 65535 の範囲の 2 バイト値です。
 - **internet** : このコミュニティのルートはインターネットコミュニティにアドバタイズされます。このコミュニティは、すべての BGP 対応ネットワークングデバイスで構成されます。
 - **local-as** : このコミュニティのルートはローカル AS 番号の外にはアドバタイズされません。

- **no-advertise** : NO_ADVERTISE コミュニティをルートにアタッチします。このコミュニティのルートは他の BGP ピアにはアドバタイズされません。
- **no-export** : NO_EXPORT コミュニティをルートにアタッチします。このコミュニティのルートは、ローカル AS や BGP コンフェデレーション境界の外にアドバタイズされません。1つのリストに複数の BGP コミュニティを設定するには、複数の **community** オプションを含め、各オプションに1つのコミュニティを指定します。

6. [Add]をクリックします。

データプレフィックスの設定

1. [対象グループ (Groups of Interest)] リストで、[データプレフィックス (Data Prefix)] をクリックします。
2. [新しいデータプレフィックスリスト (New Data Prefix List)] をクリックします。
3. リストの名前を入力します。
4. [IPv4] または [IPv6] を選択します。
5. [データプレフィックスの追加 (Add Data Prefix)] フィールドに、1つ以上のデータプレフィックスをコンマで区切って入力します。
6. [Add]をクリックします。

ポリサーの構成

1. 対象グループリストで、[ポリサー (Policer)] をクリックします。
2. [新しいポリサーリスト (New Policer List)] をクリックします。
3. リストの名前を入力します。
4. ポリシングパラメータを定義します。
 1. [バースト (Burst)] フィールドに、最大トラフィックバーストサイズ (15,000 ~ 10,000,000 バイト) を入力します。
 2. [超過 (Exceed)] フィールドで、バーストサイズまたはトラフィックレートを超えたときに実行するアクションを選択します。[ドロップ (drop)] を選択した場合、パケット損失の優先順位 (PLP) が低く設定されます。
[リマーク (remark)] を選択した場合、パケット損失の優先順位 (PLP) が高く設定されます。
 3. [レート (Rate)] フィールドに、最大トラフィックレートを $0 \sim 2^{64} - 1$ ビット/秒 (bps) の値で入力します。
5. [Add]をクリックします。

プレフィックスの構成

1. 対象グループのリストで、[プレフィックス (Prefix)] をクリックします。
2. [新しいプレフィックスリスト (New Prefix List)] をクリックします。
3. リストの名前を入力します。
4. [プレフィックスの追加 (Data Prefix)] フィールドに、1つ以上のデータプレフィックスをコンマで区切って入力します。
5. [Add] をクリックします。

サイトの設定

1. 対象グループのリストで、[サイト (Site)] をクリックします。
2. [新しいサイトリスト (New Site List)] をクリックします。
3. リストの名前を入力します。
4. [サイトの追加 (Add Site)] フィールドに、1つ以上のサイト ID をコンマで区切って入力します。
たとえば、100 または 200 をコンマで区切るか、1 から 4294967295 の範囲で指定します。
5. [Add] をクリックします。

アプリプロブクラスの設定

1. 対象グループのリストで、[アプリケーションプロブクラス (App Probe Class)] をクリックします。
2. [新しいアプリケーションプロブクラス (New App Probe Class)] をクリックします。
3. [プロブクラス名 (Prob Class Name)] フィールドにプロブクラス名を入力します。
4. [転送クラス (Forwarding Class)] ドロップダウンリストから必要な転送クラスを選択します。
5. [エン트리 (Entries)] ペインで、[色 (Color)] ドロップダウンリストから適切な色を選択し、**DSCP** 値を入力します。
必要に応じて、[+] 記号をクリックしてエントリを追加できます。
6. [Save] をクリックします。

SLA クラスの構成

1. 対象グループのリストで、[SLAクラス (SLA Class)] をクリックします。
2. [新しいSLAクラスのリスト (New SLA Class List)] をクリックします。
3. リストの名前を入力します。

4. SLA クラスのパラメータを定義します。
 1. [損失 (Loss)] フィールドに、接続の最大パケット損失を 0 ~ 100% の値で入力します。
 2. [遅延 (Latency)] フィールドに、接続の最大パケット遅延を 0 ~ 1,000 ミリ秒の値で入力します。
 3. [ジッター (Jitter)] フィールドに、接続の最大ジッターを 1 ~ 1,000 ミリ秒の値で入力します。
 4. [アプリケーションプローブクラス (App Probe Class)] ドロップダウンリストから、必要なアプリケーションプローブクラスを選択します。
5. (オプション) [フォールバックのベストトンネル (Fallback Best Tunnel)] チェックボックスをオンにして、最適なトンネル基準を有効にします。

このオプションフィールドは Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a から利用できるため、SLA が満たされていない場合に、使用可能なカラーからベストパスまたは色を選択できます。このオプションを選択すると、ドロップダウンから必要な基準を選択できます。基準には、損失、遅延、およびジッターの値を 1 つ以上組み合わせます。
6. ドロップダウンリストから [基準 (Criteria)] を選択します。使用可能な基準は次のとおりです。
 - 遅延
 - 損失
 - Jitter
 - 遅延、損失
 - 遅延、ジッター
 - 損失、遅延
 - 損失、ジッター
 - ジッター、遅延
 - ジッター、損失
 - 遅延、損失、ジッター
 - 遅延、ジッター、損失
 - 損失、遅延、ジッター
 - 損失、ジッター、遅延
 - ジッター、遅延、損失
 - ジッター、損失、遅延

7. 選択した基準の損失バリエーション（％）、遅延バリエーション（ミリ秒）、およびジッターバリエーション（ミリ秒）を入力します。
8. [Add]をクリックします。

TLOC の設定

1. 対象グループのリストで、[TLOC] をクリックします。
2. [新しいTLOCリスト (New TLOC List)] をクリックします。[TLOCリスト (TLOC List)] ポップアップが表示されます。
3. リストの名前を入力します。
4. [TLOC IP] フィールドに、TLOC のシステム IP アドレスを入力します。
5. [色 (Color)] フィールドで、TLOC の色を選択します。
6. [カプセル化 (Encap)] フィールドで、カプセル化のタイプを選択します。
7. [プリファレンス (Preference)] フィールドで、必要に応じて、TLOC に関連付けるプリファレンスを選択します。
指定できる範囲は 0 ~ 4294967295 です。
8. [TLOC の追加 (Add TLOC)] をクリックして、別の TLOC をリストに追加します。
9. [Save] をクリックします。



(注) `set tloc` および `set tloc-list` コマンドを使用するには、`set-vpn` コマンドを使用する必要があります。

TLOC ごとに、アドレス、色、カプセル化を指定します。必要に応じて、TLOC アドレスに関連付けるプリファレンス値 (0 ~ 232 - 1) を設定します。アクションの受け入れ条件で TLOC リストを適用する場合、複数の TLOC が使用可能でマッチ条件を満たす場合、最も高いプリファレンス値を持つ TLOC が使用されます。2つ以上の TLOC が最も高いプリファレンス値である場合、トラフィックは ECMP 方式によってそれらの間で送信されます。

IPsec 設定がエッジルータのローカル優先カラーで設定されている場合、ローカル TLOC およびカラーは、ローカルカラーの設定で設定された集中型ポリシーと重複しません。ローカル TLOC 設定を持つエッジルータが優先されます。この場合、集中型ポリシーで設定された優先 TLOC は考慮されません。

VPN の設定

1. 対象グループのリストで、[VPN] をクリックします。
2. [新しいVPNリスト (New VPN List)] をクリックします。
3. リストの名前を入力します。

- [VPNの追加 (Add VPN)] フィールドに、1つ以上の VPNID をコンマで区切って入力します。
たとえば、100 または 200 をコンマで区切るか、1 から 65530 の範囲で指定します。
- [Add] をクリックします。

リージョンの設定

最小リリース : Cisco vManage リリース 20.7.1

マルチリージョンファブリック（以前の階層型 SD-WAN）のリージョンのリストを設定するには、[管理 (Administration)] > [設定 (Settings)] でマルチリージョンファブリックが有効になっていることを確認します。

- 対象グループのリストで、[リージョン (Region)] をクリックします。
- [New Region List] をクリックします。
- [リージョンリスト名 (Region List Name)] フィールドに、リージョンのリスト名を入力します。
- [リージョンの追加 (Add Region)] フィールドに、1つ以上のリージョンをコンマで区切って入力するか、範囲を入力します。
たとえば、リージョン 1、3 をコンマで指定するか、範囲 1 から 4 を指定します。
- [Add] をクリックします。

[次へ (Next)] をクリックして、ウィザードの [トポロジと VPN メンバーシップの設定 (Configure Topology and VPN Membership)] に移動します。

優先カラーグループの設定

表 7: 機能の履歴

機能名	リリース情報	説明
優先するデータプレーントンネルの優先グループを選択します。	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能により、アプリケーション認識型ルーティング (AAR) の優先カラーとバックアップ優先カラーのランク付けのサポートが追加されます。Cisco IOS XE Catalyst SD-WAN デバイスの色またはパスの設定に基づいて、最大 3 段階の優先順位を設定できます。

トランスポート設定の順序を設定して、転送トラフィックの優先順位を選択できます。

[Preferred Color Group] は、オーバーレイトラフィックでのみサポートされ、DIA トラフィックではサポートされません。

- 対象グループのリストで、[優先カラーグループ (Preferred Color Group)] をクリックします。

2. [New Preferred Color Group] をクリックします。
3. [優先カラーグループ名 (Preferred Color Group Name)] フィールドに、優先カラーグループの名前を入力します。
4. [プライマリカラー (Primary Colors)] ペインで、次の手順を実行します。
 1. [カラーの設定 (Color Preference)] ドロップダウンリストでカラーの設定を選択します。
 2. [パスの設定 (Path Preference)] ドロップダウンリストでパスの設定を選択します。

フィールド	説明
Preferred Color Group Name	優先カラーグループの名前を入力します。
Color Preference	<p>ドロップダウンリストでカラーの設定を選択します。次のオプションがあります。</p> <ul style="list-style-type: none"> • デフォルト • 3g • biz-internet • ブルー • bronze • custom1 • custom2 など <p>複数の色を選択できます。</p>
Path Preference	<p>ドロップダウンリストでパスの設定を選択します。次のオプションがあります。</p> <ul style="list-style-type: none"> • [Direct Path] : 送信先デバイスと宛先デバイス間のダイレクトパスのみを使用します。 • [マルチホップパス (Multi Hop Path)] : マルチリージョンファブリックネットワークでは、ダイレクトパスが使用可能な場合でも、コアリージョンを含むマルチホップパスを送信先デバイスと宛先デバイス間で使用します。 • [All Paths] : 送信先デバイスと宛先デバイス間の任意のパスを使用します。 <p>(注) このオプションは、パス設定をまったく構成しないことと同じです。ポリシーをマルチリージョンファブリックネットワーク以外に適用する場合は、このオプションを使用します。</p>

5. [セカンダリカラー (Secondary Colors)] ペインで、次の手順を実行します。
 1. [カラーの設定 (Color Preference)] ドロップダウンリストでカラーの設定を選択します。
 2. [パスの設定 (Path Preference)] ドロップダウンリストでパスの設定を選択します。
6. [ターシャリカラー (Tertiary Colors)] ペインで、次の手順を実行します。
 1. [カラーの設定 (Color Preference)] ドロップダウンリストでカラーの設定を選択します。
 2. [パスの設定 (Path Preference)] ドロップダウンリストでパスの設定を選択します。
7. [Add]をクリックします。

色のランク付けを設定する場合は、次のガイドラインが役立ちます。

- プライマリ設定は必須であり、各優先順位レベルで少なくとも1つの優先パスまたはカラーを設定する必要があります。両方を設定することもできます。
- 複数のカラーを設定できます。
- パスの設定がされていない場合、すべてのパスは使用可能な優先色によって制約されます。
- パスの設定の制約内でカラーが設定されていない場合は、すべての色を使用できます。
- 設定は優先順位の高い順に適用され、トラフィックを転送するパスまたはカラーを決定します。

プライマリカラー、セカンダリカラー、およびターシャリカラーがダウンしている場合、パケットはドロップされません。トラフィックは通常のルーティング設定にフォールバックし、他の色がアップしているかどうかを選択します。

WAN Insights (WANI) の Cisco SD-WAN Manager への統合

表 8: 機能の履歴

機能名	リリース情報	説明
WAN Insights ポリシーの自動化	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	この機能を使用すると、Cisco SD-WAN Analytics で使用可能な推奨事項を Cisco SD-WAN Manager AAR ポリシーに適用し、適用された推奨事項を Cisco SD-WAN Manager で表示させることができます。

Cisco SD-WAN Analytics は、Cisco Catalyst SD-WAN 向けのクラウドベースの分析サービスであり、アプリケーションとネットワークのパフォーマンスについて包括的なインサイトを提供するものです。分析サービスは、Cisco DNA Advantage と Cisco DNA Premier ソフトウェアをサブスクリプションすると利用できます。Cisco SD-WAN Analytics では、トラフィックフローに関するメタデータを収集してクラウドストレージに保存し、収集したデータに基づいて分析を生成します。予測パス分析によって生成されるパスの推奨事項は、長期に渡るインサイトに基づいています。これらの推奨事項は、Cisco SD-WAN Manager で手動で作成するポリシーに変換し、ネットワークに適用する必要があります。

予測パス推奨事項は、アクティブな推奨事項を実用的な一元管理型 AAR ポリシーに適用して、Cisco Catalyst SD-WAN ネットワーク内の転送に関する決定に影響を与えられる機能です。推奨事項は AAR ポリシーの一部として適用されてから、Cisco SD-WAN コントローラにプッシュされます。予測パス推奨事項の SD-WAN ネットワークへの適用にあたっては、AAR ポリシーの TLOC 設定として適用されます。

予測パス推奨事項の使用に関する詳細は、「[予測パスの推奨事項](#)」を参照してください。

予測パス推奨事項の適用

Cisco SD-WAN Analytics に予測パスの推奨事項がある場合は、次の手順を実行して、推奨事項をアプリケーション認識型ルーティングポリシーに適用します。

1. Cisco SD-WAN Manager メニューで、右上隅にあるベルのアイコンをクリックします。[通知 (Notifications)] ペインにアクティブなアラームが表示されます。
2. [通知 (Notifications)] ペインに [アクティブな推奨事項 (Active Recommendations)] がある場合は、サイトをクリックして推奨事項を確認します。または、Cisco SD-WAN Manager メニューから [分析 (Analytics)] > [予測ネットワーク (Predictive Networks)] の順にクリックして確認することもできます。
3. [アクティブな推奨事項 (Active Recommendations)] をクリックし、[適用 (Apply)] をクリックします。
4. [予測パス推奨事項の適用 (Apply Predictive Path Recommendations)] ウィンドウで、[適用に進む (Proceed to Apply)] をクリックして新しい推奨事項を適用します。

適用された推奨事項は、Cisco SD-WAN Manager によって生成された設定で確認し、Cisco SD-WAN コントローラにプッシュできます。

考慮すべき点

- Cisco SD-WAN Manager は、ログイン時に推奨事項をプルします。推奨事項を更新する場合は、ページを更新するか、ログインし直します。
- Cisco SD-WAN Manager は、一部の AAR ポリシーにのみ関連付けられているアプリケーションリストの推奨事項をサポートします。特定のアプリケーションリストに AAR ポリシーが存在しない場合、推奨事項は無効であり、ポリシー処理は実行されません。

- WAN Insights は、AAR ポリシーが定義されていない場合でも、標準アプリケーショングループの推奨事項を生成します。ただし、AAR ポリシーが定義されていないため、ポリシーの自動化は実行されません。
- 同じサイトとアプリケーションリストに対し、WANIによって、適用される推奨事項の終端が生成され、なおかつ別の推奨事項も生成される場合、推奨事項は設定に基づいて適用されます。
- Cloud OnRamp for SaaS に対する WANI 推奨事項の適用はサポートされていません。

予測パス推奨事項

WAN Insights (WANI) を使用すれば、現在のネットワーク設定のパフォーマンスを追跡し、ポリシーとパスを調整して最高のユーザー体験を実現できます。予測パスの推奨事項は、AAR ポリシーの TLOC 設定に影響を及ぼします。

WAN Insights は、アプリケーショントラフィックの最適なパスを見つけるために、統計モデルを使用して Cisco Catalyst SD-WAN の履歴データを調査する予測ネットワーク最適化ツールです。WANI では、アプリケーショントラフィックフロー中にエクスポートされたテレメトリデータを分析し、SLA 違反（低品質のパフォーマンスなど）の発生する可能性を減らすパスについて、長期的な推奨事項を生成します。

予測ネットワークは、アプリケーションの SLA 違反を検出するために、AAR ポリシーで定義されている各アプリケーションリストに SLA を関連付けます。これは、特定のサイトおよび TLOC で SLA 違反の可能性を計算し、推奨事項を生成するために使用されます。

データポリシーに関する対象グループの構成の詳細については、「[一元管理型ポリシーの対象グループの構成](#)」を参照してください。

トポロジと VPN メンバーシップの設定

[トポロジとVPNメンバーシップの設定 (Configure Topology and VPN Membership)] ウィンドウを初めて開くと、デフォルトで [トポロジ (Topology)] ウィンドウが表示されます。

トポロジと VPN メンバーシップを設定するには、次の手順を実行します。

ハブアンドスポーク

1. [トポロジの追加 (Add Topology)] ドロップダウンで、[ハブアンドスポーク (Hub-and-Spoke)] を選択します。
2. ハブアンドスポークポリシーの名前を入力します。
3. ポリシーの説明を入力します。
4. [VPN リスト (VPN Lists)] フィールドで、ポリシーの VPN リストを選択します。
5. 左側のペインで、[ハブアンドスポークの追加 (Add Hub-and-Spoke)] をクリックします。テキスト文字列 [マイハブアンドスポーク (My Hub-and-Spoke)] を含むハブアンドスポーク ポリシー コンポーネントが左側のペインに追加されます。

6. [マイハブアンドスポーク (My Hub-and-Spoke)]のテキスト文字列をダブルクリックし、ポリシーコンポーネントの名前を入力します。
7. 右側のペインで、次のようにネットワークトポロジにハブサイトを追加します。
 1. [ハブサイトの追加 (Add Hub Sites)]をクリックします。
 2. [サイトリスト (Site List)]フィールドで、ポリシーコンポーネントのサイトリストを選択します。
 3. [Add]をクリックします。
 4. ポリシーコンポーネントにさらにハブサイトを追加するには、これらの手順を繰り返します。
8. 右側のペインで、ネットワークトポロジにスポークサイトを追加します。
 1. [スポークサイトの追加 (Add Spoke Sites)]をクリックします。
 2. [サイトリストフィールド (Site List Field)]で、ポリシーコンポーネントのサイトリストを選択します。
 3. [Add]をクリックします。
 4. ポリシーコンポーネントにさらにスポークサイトを追加するには、これらの手順を繰り返します。
9. 必要に応じて手順を繰り返して、ハブアンドスポークポリシーにコンポーネントを追加します。
10. [ハブアンドスポークポリシーの保存 (Save Hub-and-Spoke Policy)]をクリックします。

[メッシュ (Mesh)]

1. [トポロジの追加 (Add Topology)]ドロップダウンで、[メッシュ (Mesh)]を選択します。
2. メッシュリージョンポリシーコンポーネントの名前を入力します。
3. メッシュリージョンポリシーコンポーネントの説明を入力します。
4. [VPNリスト (VPN Lists)]フィールドで、ポリシーのVPNリストを選択します。
5. [新しいメッシュリージョン (New Mesh Region)]をクリックします。
6. [メッシュリージョン名 (Mesh Region Name)]フィールドに、個々のメッシュリージョンの名前を入力します。
7. [サイトリスト (Site List)]フィールドで、メッシュ領域に含める1つ以上のサイトを選択します。
8. [Add]をクリックします。
9. メッシュリージョンをさらにポリシーに追加するには、これらの手順を繰り返します。

10. [メッシュトポロジの保存 (Save Mesh Topology)] をクリックします。

カスタム制御 (ルートおよびTLOC) : 一元管理型ルート制御ポリシー (OMP ルートの照合用)

1. [トポロジの追加 (Add Topology)] ドロップダウンで、[カスタム制御 (ルートおよびTLOC) (Custom Control (Route & TLOC))] を選択します。
2. 制御ポリシーの名前を入力します。
3. ポリシーの説明を入力します。
4. 左側のペインで、[シーケンスタイプ (Sequence Type)] をクリックします。[カスタム制御ポリシーの追加 (Add Custom Control Policy)] ポップアップウィンドウが表示されます。
5. [ルート (Route)] を選択します。テキスト文字列 [ルート (Route)] を含むポリシーコンポーネントが左側のペインに追加されます。
6. [ルート (Route)] のテキスト文字列をダブルクリックし、ポリシーコンポーネントの名前を入力します。
7. 右側のペインで、[シーケンスルール (Sequence Rule)] をクリックします。[マッチ/アクション (Match/Actions)] ボックスが開き、デフォルトで [マッチ (Match)] が選択されています。
8. [マッチ (Match)] ボックスの下に表示されるボックスから、目的のポリシー照合タイプを選択します。次に、そのマッチ条件の値を選択または入力します。必要に応じて、シーケンスルールの追加のマッチ条件を設定します。
9. [Actions] をクリックします。デフォルトでは、[拒否 (Reject)] オプションが選択されています。受け入れられたパケットで実行するアクションを設定するには、[受け入れ (Accept)] オプションをクリックします。次に、アクションを選択するか、アクションの値を入力します。
10. [Save Match and Actions] をクリックします。
11. 必要に応じて、[シーケンスルール (Sequence Rule)] をクリックして、シーケンスルールをさらに設定します。並べ替えるには、ドラッグアンドドロップします。
12. 必要に応じて、[シーケンスタイプ (Sequence Type)] をクリックして、シーケンスをさらに設定します。並べ替えるには、ドラッグアンドドロップします。
13. [制御ポリシーの保存 (Save Control Policy)] をクリックします。

カスタム制御 (ルートおよびTLOC) : 一元管理型TLOC制御ポリシー (TLOCルートの照合用)

1. [トポロジの追加 (Add Topology)] ドロップダウンで、[カスタム制御 (ルートおよびTLOC) (Custom Control (Route & TLOC))] を選択します。
2. 制御ポリシーの名前を入力します。

3. ポリシーの説明を入力します。
4. 左側のペインで、[シーケンスタイプ (Sequence Type)] をクリックします。[カスタム制御ポリシーの追加 (Add Custom Control Policy)] ポップアップウィンドウが表示されません。
5. [TLOC] を選択します。テキスト文字列 [TLOC] を含むポリシーコンポーネントが左側のペインに追加されます。
6. [TLOC] のテキスト文字列をダブルクリックし、ポリシーコンポーネントの名前を入力します。
7. 右側のペインで、[シーケンスルール (Sequence Rule)] をクリックします。[マッチ/アクション (Match/Actions)] ボックスが開き、デフォルトで [マッチ (Match)] が選択されています。
8. [マッチ (Match)] ボックスの下に表示されるボックスから、目的のポリシー照合タイプを選択します。次に、そのマッチ条件の値を選択または入力します。必要に応じて、シーケンスルールの追加のマッチ条件を設定します。
9. [Actions] をクリックします。デフォルトでは、[拒否 (Reject)] オプションが選択されています。受け入れられたパケットで実行するアクションを設定するには、[受け入れ (Accept)] オプションをクリックします。次に、アクションを選択するか、アクションの値を入力します。
10. [Save Match and Actions] をクリックします。
11. 必要に応じて、[シーケンスルール (Sequence Rule)] をクリックして、シーケンスルールをさらに設定します。並べ替えるには、ドラッグアンドドロップします。
12. 必要に応じて、[シーケンスタイプ (Sequence Type)] をクリックして、シーケンスをさらに設定します。並べ替えるには、ドラッグアンドドロップします。
13. [制御ポリシーの保存 (Save Control Policy)] をクリックします。

一元管理型制御ポリシーは、マッチとアクションがペアになったシーケンスで構成されています。シーケンスには番号が付けられ、ポリシー内のマッチとアクションのペアごとにルートやTLOCの分析順序が設定されます。



- (注) シーケンスには、ポリシー用に **match app-list** または **dns-app-list** を設定させられますが、両方を設定することはできません。ポリシーに対して **match app-list** と **dns-app-list** の両方を設定することはできない仕組みになっています。

NAT DIA フォールバックと DNS リダイレクションは、データポリシーで同時にサポートされません。

一元管理型制御ポリシーの各シーケンスには、1つのマッチ条件（ルートまたはTLOC用）と1つのアクション条件を含めることができます。

Default Action

選択されたルートやTLOCが、一元管理型制御ポリシーのマッチ条件のいずれにもマッチしない場合、デフォルトアクションが適用されます。デフォルトでは、ルートまたはTLOCが拒否されるようになっています。

選択されたデータパケットが、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。

既存のトポロジのインポート

1. [トポロジの追加 (Add Topology)] ドロップダウンで、[既存のトポロジのインポート (Import Existing Topology)] をクリックします。[既存のトポロジのインポート (Import Existing Topology)] ポップアップが表示されます。
2. トポロジのタイプを選択します。
3. [ポリシータイプ (Policy Type)] で、インポートするトポロジの名前を選択します。
4. [ポリシー (Policy)] ドロップダウンで、インポートするポリシーを選択します。



(注) ポリシー構成ウィザードでは、他の一元管理型ポリシー（データ、制御、またはアプリケーション認識型ルーティング）のインスタンスのように、設定済みのポリシーをインポートすることはできません。ポリシー全体を設定する必要があります。

5. [Import] をクリックします。

[次へ (Next)] をクリックして、ウィザードの [トラフィックルールの設定 (Configure Traffic Rules)] に移動します。

VPN メンバーシップポリシーの作成

1. [ネットワークトポロジの指定 (Specify your network topology)] エリアで、[VPNメンバーシップ (VPN Membership)] をクリックします。
2. [VPNメンバーシップポリシーの追加 (Add VPN Membership Policy)] をクリックします。



(注) 一度に追加できる VPN メンバーシップは1つだけなので、すべてのサイトリストと VPN リストを1つのポリシーに含める必要があります。

[VPNメンバーシップポリシーの追加 (Add VPN Membership Policy)] ポップアップが表示されます。

3. VPN メンバーシップポリシーの名前と説明を入力します。

4. [サイトリスト (Site List)] フィールドで、サイトリストを選択します。
5. [VPN リスト (VPN Lists)] フィールドで、VPN リストを選択します。
6. [リストの追加 (Add List)] をクリックして、VPNメンバーシップに別のVPNを追加します。
7. [Save] をクリックします。
8. [次へ (Next)] をクリックして、ウィザードの [トラフィックルールの設定 (Configure Traffic Rules)] に移動します。

トラフィックルールの設定

表 9: 機能の履歴

機能名	リリース情報	説明
ICMP メッセージと のポリシー照合	Cisco IOS XE リリース 17.4.1 Cisco vManage リリース 20.4.1	これは、一元管理型データポリシー、ローカライズ型データポリシー、およびアプリケーション認識型ルーティングポリシー向けに ICMP メッセージのリストを指定する場合に使用可能な新しいマッチ条件に対応できるようにする機能です。

[トラフィックルールの設定 (Configure Traffic Rules)] ウィンドウを初めて開くと、デフォルトで、[アプリケーション認識型ルーティング (Application-Aware Routin)] が選択されています。

作成済みの AAR ルーティングポリシーについては、このページで確認することもできます。このページには、ポリシーの名前、タイプ、モード、説明、更新者、最終更新の詳細など、ポリシーに関連するさまざまな情報が記載されています。



- (注) [モード (Mode)] 列を参照すると、ポリシーのセキュリティステータスが確認できます。ステータスは、ポリシーが統合セキュリティで使用されているかどうかを見分けるのに役立ちます。モードステータスは、セキュリティポリシーにのみ適用され、一元管理型またはローカライズ型ポリシーには関係ありません。

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) フローのトラフィックルールの設定の詳細については、[「Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン」](#) を参照してください。



- (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。

一元管理型データポリシーのトラフィックルールを設定するには、次の手順を実行します。

1. [トラフィックデータ (Traffic Data)] をクリックします。
2. [ポリシーの追加 (Add Policy)] ドロップダウンをクリックします。
3. [Create New] をクリックします。[データポリシーの追加 (Add Data Policy)] ウィンドウが表示されます。
4. データポリシーの名前と説明を入力します。
5. 右側のペインで、[シーケンスタイプ (Sequence Type)] をクリックします。[データポリシーの追加 (Add Data Policy)] ポップアップウィンドウが開きます。
6. 作成するデータポリシーのタイプを [アプリケーションファイアウォール (Application Firewall)]、[QoS]、[トラフィックエンジニアリング (Traffic Engineering)]、[カスタム (Custom)] から選択します。



(注) 同じマッチ条件に対して複数のデータポリシーのタイプを設定する場合は、カスタムポリシーを設定する必要があります。

7. アプリケーション、ファイアウォール、QoS、トラフィックエンジニアリング、またはカスタムのテキスト文字列を含むポリシーシーケンスが左側のペインに追加されます。
8. 該当するテキスト文字列をダブルクリックして、ポリシーシーケンスの名前を入力します。入力した名前は、左側のペインと右側のペインの両方にある [シーケンスタイプ (Sequence Type)] リストに表示されます。
9. 右側のペインで、[シーケンスルール (Sequence Rule)] をクリックします。[マッチ/アクション (Match/Action)] ボックスが開き、デフォルトで [マッチ (Match)] が選択されています。使用可能なポリシーのマッチ条件は、ダイアログボックスの下に一覧表示されます。

一致条件	手順
なし (すべてのパケットに一致)	マッチ条件を指定しないでください。

一致条件	手順
アプリケーション/アプリケーションファミリー リスト	<ol style="list-style-type: none"> 1. [マッチ (Match)]条件で、[アプリケーション/アプリケーションファミリーリスト (Applications/Application Family List)]をクリックします。 2. ドロップダウンで、アプリケーションファミリーを選択します。 3. アプリケーションリストを作成するには、次の手順を実行します。 <ol style="list-style-type: none"> 1. [新しいアプリケーションリスト (New Application List)]をクリックします。 2. リストの名前を入力します。 3. [アプリケーション (Application)]をクリックして、個々のアプリケーションのリストを作成します。[アプリケーションファミリー (Application Family)]をクリックして、関連するアプリケーションのリストを作成します。 4. [アプリケーションの選択 (Select Application)]ドロップダウンで、目的のアプリケーションまたはアプリケーションファミリーを選択します。 5. [Save] をクリックします。 <p>このマッチ条件は、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 の IPv6 トラフィックに使用できます。</p>
Destination Data Prefix	<ol style="list-style-type: none"> 1. [マッチ (Match)]条件で、[接続先データプレフィックス (Destination Data Prefix)]をクリックします。 2. 接続先プレフィックスのリストと照合するには、ドロップダウンから該当するリストを選択します。 3. 個々の宛先プレフィックスと照合するには、[宛先 : IPプレフィックス (Destination: IP Prefix)]フィールドにプレフィックスを入力します。
宛先ポート	<ol style="list-style-type: none"> 1. [マッチ (Match)]条件で、[接続先ポート (Destination Port)]をクリックします。 2. [宛先ポート (Destination Port)]フィールドにポート番号を入力します。単一のポート番号、ポート番号のリスト (スペースで区切られた番号) 、またはポート番号の範囲 (ハイフン [-] で区切られた2つの番号) を指定します。
DNS アプリケーションリスト (DNS Application List)	<p>スプリット DNS を有効にするには、アプリケーションリストを追加します。</p> <ol style="list-style-type: none"> 1. [マッチ (Match)]条件で、[DNS アプリケーションリスト (DNS Application List)]をクリックします。 2. ドロップダウンで、アプリケーションファミリーを選択します。 <p>このマッチ条件は、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 の IPv6 トラフィックに使用できます。</p>

一致条件	手順
DNS	<p>アプリケーションリストを追加して、スプリットDNS要求を処理します。</p> <ol style="list-style-type: none"> [マッチ (Match)] 条件で、[DNS] をクリックします。 DNS アプリケーションの DNS 要求を処理するには、ドロップダウンで [要求 (Request)] を選択し、アプリケーションの DNS 応答を処理するには [応答 (Response)] を選択します。
[DSCP]	<ol style="list-style-type: none"> [マッチ (Match)] 条件で、[DSCP] をクリックします。 [DSCP] フィールドに、DSCP 値を 0 ～ 63 の数値で入力します。
パケット長 (Packet Length)	<ol style="list-style-type: none"> [マッチ (Match)] 条件で、[パケット長 (Packet Length)] をクリックします。 [パケット長 (Packet Length)] フィールドに、パケット長を 0 ～ 65535 の値で入力します。
PLP	<ol style="list-style-type: none"> [マッチ (Match)] 条件で、[PLP] をクリックして、[パケット損失の優先順位 (Packet Loss Priority)] を設定します。 [PLP] ドロップダウンで、[低 (Low)] または [高 (High)] を選択します。PLP を [高 (High)] に設定するには、[注釈超過 (exceed remark)] オプションのあるポリシーを適用します。
Protocol	<ol style="list-style-type: none"> [マッチ (Match)] 条件で、[プロトコル (Protocol)] をクリックします。 [プロトコル (Protocol)] フィールドに、インターネットプロトコル番号を 0 ～ 255 の数字で入力します。
ICMP Message	<p>ICMP メッセージと照合するには、[プロトコル (Protocol)] フィールドで、インターネットプロトコル番号を 1、58、またはその両方に設定します。</p> <p>(注) このフィールドは、Cisco IOS XE リリース 17.4.1、Cisco vManage リリース 20.4.1 以降で使用できます。</p>
Source Data Prefix	<ol style="list-style-type: none"> [マッチ (Match)] 条件で、[送信元データプレフィックス (Source Data Prefix)] をクリックします。 送信元プレフィックスのリストと照合するには、ドロップダウンから該当するリストを選択します。 個々の送信元プレフィックスと照合するには、[送信元 (Source)] フィールドにプレフィックスを入力します。

一致条件	手順
送信元ポート	<ol style="list-style-type: none"> [マッチ (Match)] 条件で、[送信元ポート (Source Port)] をクリックします。 [送信元 (Source)] フィールドに、ポート番号を入力します。単一のポート番号、ポート番号のリスト (スペースで区切られた番号)、またはポート番号の範囲 (ハイフン [-] で区切られた 2 つの番号) を指定します。
[TCP]	<ol style="list-style-type: none"> [マッチ (Match)] 条件で、[TCP] をクリックします。 [TCP] フィールドで指定できるオプションは [SYN] だけです。

- QoS およびトラフィック エンジニアリングのデータポリシーの場合 : [プロトコル (Protocol)] ドロップダウンリストから [IPv4] を選択すると、ポリシーは IPv4 アドレスファミリのみ適用されます。[IPv6] を選択すると、ポリシーは IPv6 アドレスファミリのみ適用されます。ポリシーを IPv4 と IPv6 のアドレスファミリに適用するには、[両方 (Both)] を選択します。
- 1 つ以上の **マッチ** 条件を選択するには、ボックスをクリックし、説明に従って値を設定します。



(注) すべてのポリシーシーケンスタイプですべてのマッチ条件を使用できるわけではありません。

- マッチするデータトラフィックに対して実行するアクションを選択するには、[アクション (Actions)] ボックスをクリックします。
- マッチするトラフィックをドロップするには、[ドロップ (Drop)] をクリックします。使用可能なポリシーアクションが右側に表示されます。
- マッチするトラフィックを受け入れるには、[受け入れ (Accept)] をクリックします。使用可能なポリシーアクションが右側に表示されます。
- 説明に従ってポリシーアクションを設定します。



(注) すべての一致条件ですべてのアクションを使用できるわけではありません。



- (注) IPv4 パケットに UDP または TCP データグラムの先頭以外のフラグメントが含まれている場合、UDP または TCP ヘッダーがないため、使用可能な L4 ポート情報はありません。このようなフラグメントの場合、destination-port または source-port の一致は無視されます。

次の例では、宛先ポート 161 へのすべての UDP パケットと、IPv4 ヘッダーのプロトコル ID フィールドが 17 に設定され、IPv4 ヘッダーにフラグメントオフセットが設定されているその他の IPv4 パケットがドロップされます。

```
policy
app-visibility
access-list SDWAN_101
sequence 100
match
  destination-port 161
  protocol 17
!
action drop
!
```

アクション条件	説明	手順
カウンタ	条件にマッチするデータパケットをカウントします。	<ol style="list-style-type: none"> 1. [アクション (Action)]条件で、[カウンタ (Counter)]をクリックします。 2. [カウンタ名 (Counter Name)]フィールドに、パケットカウンタを保存するファイルの名前を入力します。
[DSCP]	条件がマッチするデータパケットに DSCP 値を割り当てます。	<ol style="list-style-type: none"> 1. [アクション (Action)]条件で、[DSCP] をクリックします。 2. [DSCP] フィールドに、DSCP 値を 0 ～ 63 の数値で入力します。
Forwarding Class	条件がマッチするデータパケットに転送クラスを割り当てます。	<ol style="list-style-type: none"> 1. [マッチ (Match)]条件で、[転送クラス (Forwarding Class)]をクリックします。 2. [転送クラス (Forwarding Class)]フィールドで、クラス値を 32 文字以内で入力します。

アクション条件	説明	手順
Log	<p>サポートされる最小リリース : Cisco vManage リリース 20.11.1 および Cisco IOS XE リリース 17.11.1a</p> <p>ロギングを有効にするには、[ログ (Log)] をクリックします。</p> <p>(DP、AAR、または ACL) データポリシーパケットにログアクションが設定されている場合、ログが生成され、syslog に記録されます。グローバルな log-rate-limit により、すべてのログがログに記録されるわけではありません。パケットヘッダーが最初にログに記録される際、syslog メッセージが生成され、その後もフローがアクティブである限り、5分ごとに syslog メッセージが生成されます。</p>	<ol style="list-style-type: none"> 1. [アクション (Action)] 条件で、[ログ (Log)] をクリックしてロギングを有効にします。
Policer	<p>条件がマッチするデータパケットにポリサーを適用します。</p>	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件で、[ポリサー (Policer)] をクリックします。 2. [ポリサー (Policer)] ドロップダウンフィールドで、ポリサーの名前を選択します。

アクション条件	説明	手順
損失の修正	<p>条件がマッチするデータパケットに損失の修正を適用します。</p> <p>前方誤り訂正（FEC）では、冗長データの送信によってリンク上で失われたパケットが回復されるため、受信者はデータの再送信を要求することなくエラーを訂正できます。</p> <p>FECはIPSecトンネルでのみサポートされ、GREトンネルではサポートされません。</p> <ul style="list-style-type: none"> • [FEC 適応（FEC Adaptive）]：対応するパケットは、通過するトンネルが測定された損失に基づいて信頼できないと見なされた場合にのみ、FECの対象となります。 <p>[FEC適応（FEC Adaptive）]を選択すると、追加の[損失しきい値]フィールドが表示され、FECを自動的に有効にするためのパケット損失のしきい値を指定できます。</p> <p>適応FECは、パケット損失が2%になると機能し始めます。この値は設定可能です。</p> <p>1～5%の損失しきい値を指定できます。デフォルトのパケット損失しきい値は2%です。</p> <ul style="list-style-type: none"> • [FEC 常時（FEC Always）]：対応するパケットは常にFECの対象となります。 • [パケット複製（Packet Duplication）]：単一のトンネルを経由して重複パケットを送信します。複数のトンネルが使用可能な場合、重複パケットは、最適なパラメータを使用してトンネル経由で送信されます。 	<ol style="list-style-type: none"> 1. [マッチ（Match）]条件で、[損失の修正（Loss Correction）]をクリックします。 2. [損失の修正（Loss Correction）]フィールドで、[FEC 適応（FEC Adaptive）]、[FEC 常時（FEC Always）]、または[パケット複製（Packet Duplication）]を選択します。
[Save Match and Actions] をクリックします。		

16. 必要に応じて、追加のシーケンスルールを作成します。ルールをドラッグアンドドロップして再配置します。
17. [データポリシーの保存（Save Data Policy）]をクリックします。
18. [次へ（Next）]をクリックして、ウィザードの[サイトとVPNにポリシーを適用（Apply Policies to Sites and VPNs）]に移動します。

マッチパラメータ：制御ポリシー

OMP および TLOC ルートの場合、次の属性を一致させることができます。

一致条件	説明
カラーリスト	<p>1つ以上の色。使用できる色は、3g、biz-internet、blue、bronze、custom1、custom2、custom3、default、gold、green、lte、metro-ethernet、mpls、private1～private6、public-internet、red、silver です。</p>
コミュニティ リスト	<p>1つ以上の BGP コミュニティのリスト。[コミュニティリスト (Community List)] フィールドでは、次の項目を指定できます。</p> <ul style="list-style-type: none"> • aa:nn : AS 番号とネットワーク番号。各番号は、1 ～ 65535 の範囲の 2 バイト値です。 • internet : このコミュニティのルートはインターネットコミュニティにアドバタイズされます。このコミュニティは、すべての BGP 対応ネットワークングデバイスで構成されます。 • local-as : このコミュニティのルートは、ローカル AS 番号以外ではアドバタイズされません。 • no-advertise : NO_ADVERTISE コミュニティをルートにアタッチします。このコミュニティのルートは他の BGP ピアにはアドバタイズされません。 • no-export : NO_EXPORT コミュニティをルートにアタッチします。このコミュニティのルートは、ローカル AS や BGP コンフェデレーション境界の外にアドバタイズされません。1つのリストに複数の BGP コミュニティを設定するには、複数の community オプションを含め、各オプションに1つのコミュニティを指定します。
種類	<p>コミュニティタイプを指定します。[標準 (Standard)] を選択してコミュニティとコミュニティ番号を指定するか、[拡張 (Expanded)] を選択して正規表現を使用してコミュニティをフィルタリングします。正規表現は、コミュニティ属性にマッチするパターンを指定するために使用されます。</p>

一致条件	説明
OR 条件	<p>コミュニティリストの各正規表現文字列をルートのコミュニティ文字列と比較します。</p> <p>OR 条件は複数のコミュニティリストに適用され、すべてのデバイスで有効です。</p> <p>Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降では、コミュニティの [タイプ (Types)] フィールドと [条件 (Criteria)] フィールドを使用できます。</p>
OMP タグ	<p>デバイスのルーティングデータベース内のルートまたはプレフィックスに関連付けられたタグ値。</p> <p>範囲は 0 ~ 4294967295 です。</p>
Origin	ルートが学習されたプロトコル。
発信元 (Originator)	ルートが学習された IP アドレス。
パスタイプ	<p>Cisco 階層型 SD-WAN アーキテクチャでは、パスタイプに応じてルートが照合されます。パスタイプは以下のとおりです。</p> <ul style="list-style-type: none"> • 階層パス：アクセスリージョンから境界ルータへのホップを含むルート。リージョン0を経由して別の境界ルータへと進み、別のアクセスリージョン内のエッジルータへと続きます。 • ダイレクトパス：あるエッジルータから別のエッジルータへのダイレクトパスルート。 • トランスポートゲートウェイパス：トランスポートゲートウェイ機能が有効になっているルータによって再発信されるルート。 <p>(注) このオプションは、Cisco vManage リリース 20.8.1 以降で使用できません。</p>

一致条件	説明
優先順位	プレフィックスの優先度。これは、ルートまたはプレフィックスがローカルサイト（デバイスのルーティングデータベース）に持つプレファレンス値です。プリファレンス値が大きいほど優先されます。指定できる範囲は 0 ～ 255 です。
プレフィックス リスト	1 つ以上のプレフィックス。プレフィックスリストの名前を指定します。
Cisco SD-WAN Manager では使用できません。	個々のサイト識別子。 範囲は 0 ～ 4294967295 です。
サイト	1 つ以上のオーバーレイネットワークのサイト識別子。
[地域 (Region)]	Cisco 階層型 SD-WAN 用に定義されたリージョン。 指定できる範囲は 1 ～ 63 です。 (注) このオプションは、Cisco vManage リリース 20.7.1 以降で使用できません。
ロール (Role)	Cisco 階層型 SD-WAN アーキテクチャでは、デバイスタイプ（境界ルータまたはエッジルータ）に応じて照合が実行されます。 (注) このオプションは、Cisco vManage リリース 20.8.1 以降で使用できません。
TLOC	個々の TLOC アドレス。 (注) <code>set tloc</code> および <code>set tloc-list</code> コマンドを使用するには、 <code>set-vpn</code> コマンドを使用する必要があります。
VPN	個々の VPN 識別子。範囲は 0～65535です。
キャリア	制御トラフィックのキャリア。値は、デフォルト、 <code>carrier1</code> ～ <code>carrier 8</code> です。
ドメイン ID	TLOC に関連付けられたドメイン識別子。 範囲は 0 ～ 4294967295 です。

一致条件	説明
OMP タグ	デバイスのルートテーブル内の TLOC ルートに関連付けられているタグ値。 範囲は 0 ~ 4294967295 です。
サイト	個々のサイトのコントリビュータまたは複数のオーバーレイ ネットワーク サイトの識別子。 範囲は 0 ~ 4294967295 です。

CLI では、**policy control-policy sequence match route** コマンドで一致するように OMP ルート属性を設定し、**policy control-policy sequence match tloc** コマンドで一致するように TLOC 属性を設定します。

マッチパラメータ：データポリシー

一元管理型データポリシーは、IP ヘッダー内の IP プレフィックスとフィールド、およびアプリケーションを照合できます。スプリット DNS を有効にすることもできます。

ポリシー内の各シーケンスには、1 つ以上のマッチ条件を含めることができます。

表 10:

一致条件	説明
省略	すべてのパケットに一致。
アプリケーション/アプリケーションファミリリスト (Application/Application Family List)	アプリケーションまたはアプリケーションファミリ。 このマッチ条件は、Cisco IOS XE リリース17.9.1a および Cisco vManage リリース20.9.1以降の IPv6 トラフィックで使用できます。
Destination Data Prefix	宛先プレフィックス、IP プレフィックス、およびプレフィックス長のグループ。範囲は0から65535です。単一のポート番号、ポート番号のリスト（スペースで区切られた番号）、またはポート番号の範囲（ハイフン [-] で区切られた2つの番号）を指定します。

一致条件	説明
Destination Region (宛先リージョン)	<p>次のいずれかを選択します。</p> <ul style="list-style-type: none"> • [Primary] : 宛先デバイスが送信元と同じプライマリリージョン (アクセスリージョンとも呼ばれる) にある場合、トラフィックに一致します。このトラフィックは、コアリージョンを通過するマルチホップパスを使用して宛先に到達します。 • [Secondary] : 宛先デバイスが送信元と同じプライマリリージョンにないが、送信元と同じセカンダリリージョンにある場合、トラフィックに一致します。このトラフィックは、セカンダリリージョンで説明されているように、ダイレクトトンネルを使用して宛先に到達できます。 • [Other] : 宛先デバイスが送信元と同じプライマリリージョンまたはセカンダリリージョンにない場合、トラフィックに一致します。このトラフィックには、送信元から宛先へのマルチホップパスが必要です。 <p>(注) 最小リリース : Cisco vManage リリース 20.9.1、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a</p>
DNS アプリケーションリスト (DNS Application List)	<p>スプリット DNS を有効にして、アプリケーションごとに DNS 要求と応答を解決および処理します。 app-list リストの名前。このリストは、DNS 要求が処理されるアプリケーションを指定します。</p> <p>このマッチ条件は、Cisco IOS XE リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降の IPv6 トラフィックで使用できます。</p>
DNS	<p>DNS パケットを処理する方向を指定します。アプリケーションによって送信された DNS 要求 (アウトバウンド DNS クエリ用) を処理するには、 dns request を指定します。DNS サーバーからアプリケーションに返される DNS 応答を処理するには、 dns response を指定します。</p>
[DSCP]	DSCP 値を指定します。
パケット長	<p>パケット長を指定します。範囲は 0 から 65535 です。単一の長さ、長さのリスト (スペースで区切られた番号)、または長さの範囲 (ハイフン [-] で区切られた2つの番号) を指定します。</p>
パケット損失優先順位 (PLP) (Packet Loss Priority (PLP))	<p>パケット損失の優先順位を指定します。デフォルトでは、パケットの PLP 値は low です。PLP 値を [high] に設定するには、 [exceed remark] オプションのあるポリシーを適用します。</p>
Protocol	<p>インターネットプロトコル番号を指定します。範囲は 0 ~ 255 です。</p>

一致条件	説明
ICMP メッセージ (ICMP Message)	<p>プロトコル (IPv4) の場合、プロトコル値を1と入力すると、[ICMPメッセージ (ICMP Message)] フィールドが表示され、データポリシーに適用する ICMP メッセージを選択できます。同様に、プロトコル値に58を入力すると、プロトコル IPv6 の [ICMPメッセージ (ICMP Message)] フィールドが表示されます。</p> <p>[プロトコル (Protocol)] で [両方 (Both)] を選択すると場合、[ICMPメッセージ (ICMP Message)] または [ICMPv6メッセージ (ICMPv6 Message)] フィールドが表示されます。</p> <p>(注) このフィールドは、Cisco IOS XEリリース17.4.1、Cisco vManageリリース20.4.1以降で使用できます。</p>
Source Data Prefix	送信元プレフィックスのグループまたは個々の送信元プレフィックスを指定します。
送信元ポート	送信元ポート番号を指定します。範囲は0から65535です。単一のポート番号、ポート番号のリスト（スペースで区切られた番号）、またはポート番号の範囲（ハイフン [-] で区切られた2つの番号）を指定します。
TCP フラグ	TCP フラグの syn を指定します。
トラフィック転送先 (Traffic To)	マルチリージョンファブリックアーキテクチャでは、境界ルータがサービスを提供しているアクセスリージョン、コアリージョン、またはサービス VPN に流れる境界ルータトラフィックを照合します。
	(注) 最小リリース：Cisco vManage リリース 20.8.1



(注) IPv4 パケットに UDP または TCP データグラムの先頭以外のフラグメントが含まれている場合、UDP または TCP ヘッダーがないため、使用可能な L4 ポート情報はありません。このようなフラグメントの場合、destination-port または source-port の一致は無視されます。

次の例では、宛先ポート 161 へのすべての UDP パケットと、IPv4 ヘッダーのプロトコル ID フィールドが 17 に設定され、IPv4 ヘッダーにフラグメントオフセットが設定されているその他の IPv4 パケットがドロップされます。

```

policy
  app-visibility
  access-list SDWAN_101
  sequence 100
  match
    destination-port 161
    protocol 17
  !
  action drop
  !
!
```


表 11: ICMP メッセージのタイプ/コードと対応する列挙値

Type	コード	列挙型
0	0	echo-reply
3		unreachable
	0	net-unreachable
	1	host-unreachable
	2	protocol-unreachable
	3	port-unreachable
	4	packet-too-big
	5	source-route-failed
	6	network-unknown
	7	host-unknown
	8	host-isolated
	9	dod-net-prohibited
	10	dod-host-prohibited
	11	net-tos-unreachable
	12	host-tos-unreachable
	13	administratively-prohibited
	14	host-precedence-unreachable
15	precedence-unreachable	
5		redirect
	0	net-redirect
	1	host-redirect
	2	net-tos-redirect
	3	host-tos-redirect
8	0	echo
9	0	router-advertisement
10	0	router-solicitation
11		time-exceeded
	0	ttl-exceeded
	1	reassembly-timeout

12		parameter-problem
	0	general-parameter-problem
	1	option-missing
	2	no-room-for-option
13	0	timestamp-request
14	0	timestamp-reply
40	0	photuris
54	0	extended-echo
43		extended-echo-reply
	0	echo-reply-no-error
	1	malformed-query
	2	interface-error
	3	table-entry-error
	4	multiple-interface-match

表 12: ICMPv6 メッセージのタイプ/コードと対応する列挙値

Type	コード (Code)	列挙型
1		unreachable
	0	no-route
	1	no-admin
	2	beyond-scope
	3	destination-unreachable
	4	port-unreachable
	5	source-policy
	6	reject-route
	7	source-route-header
2	0	packet-too-big
3		time-exceeded
	0	hop-limit
	1	reassembly-timeout

4		parameter-problem
	0	Header
	1	next-header
	2	parameter-option
128	0	echo-request
129	0	echo-reply
130	0	mld-query
131	0	mld-report
132	0	mld-reduction
133	0	router-solicitation
134	0	router-advertisement
135	0	nd-ns
136	0	nd-na
137	0	redirect
138		router-renumbering
	0	renum-command
	1	renum-result
	255	renum-seq-number
139		ni-query
	0	ni-query-v6-address
	1	ni-query-name
	2	ni-query-v4-address
140		ni-response
	0	ni-response-success
	1	ni-response-refuse
	2	ni-response-qtype-unknown
141	0	ind-solicitation
142	0	ind-advertisement
143		mldv2-report
144	0	dhaad-request
145	0	dhaad-reply
146	0	mpd-solicitation
147	0	mpd-advertisement

148	0	cp-solicitation
149	0	cp-advertisement
151	0	mr-advertisement
152	0	mr-solicitation
153	0	mr-termination
155	0	rpl-control

アクションパラメータ：制御ポリシー

マッチ条件ごとに、ルートまたは TLOC が制御ポリシーに一致した場合に実行する対応するアクションを設定します。

CLI では、**policy control-policy action** コマンドでアクションを設定します。

一元管理型制御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、まず、一致するルートまたは TLOC を受け入れるか拒否するかを指定します。

表 13:

説明	Cisco SD-WAN Manager
ルートを受け入れます。受け入れられたルートは、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によって変更できます。	[承認 (Accept)] をクリック
パケットを廃棄します。	[Reject] をクリックします。

次に、受け入れられるルートまたは TLOC に対して、以下のアクションを設定できます。

アクション条件	説明
エクスポート先	指定した VPN または VPN のリストにルートをエクスポートします（一致ルートマッチ条件の場合のみ）。 範囲は 0 ～ 65535 またはリスト名です。
OMP タグ	ルート、プレフィックス、または TLOC のタグ文字列を変更します。 範囲は 0 ～ 4294967295 です。
優先順位	ルート、プレフィックス、または TLOC のプリファレンス値を指定された値に変更します。プリファレンス値が高いほど優先されます。範囲は 0 ～ 255 です。

アクション条件	説明
Service	<p>トラフィックを宛先に配信する前にトラフィックをリダイレクトするサービスを指定します。</p> <p>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 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。</p> <p>VPN 識別子は、サービスが配置されている場所です。</p> <p>標準サービス：FW、IDS、IDP カスタムサービス：netsvc1、netsvc2、netsvc3、netsvc4</p> <p>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 Cisco IOS XE Catalyst SD-WAN デバイスでサービス自体を設定します。</p>
TLOC	<p>TLOC アドレス、色、およびカプセル化を指定されたアドレスと色に変更します。</p> <p>TLOC ごとに、アドレス、色、およびカプセル化を指定します。<i>address</i> はシステム IP アドレスです。<i>color</i> には次のいずれかの色を指定します：3g、biz-internet、blue、bronze、custom1、custom2、custom3、default、gold、green、lte、metro-ethernet、mpls、private1 ~ private6、public-internet、red、silver。<i>encapsulation</i> は gre または ipsec です。必要に応じて、TLOC アドレスに関連付けるプリファレンス値 (0 ~ 232 - 1) を設定します。アクションの受け入れ条件で TLOC リストを適用する場合、複数の TLOC が使用可能でマッチ条件を満たす場合、最も高いプリファレンス値を持つ TLOC が使用されます。2つ以上の TLOC が最も高いプリファレンス値である場合、トラフィックは ECMP 方式によってそれらの間で送信されます。</p>
TLOC アクション	<p>アクションで指定されたメカニズムを使用して、一致するルートまたは TLOC を直接指定し、最終的な宛先が到達可能かどうかのエンドツーエンドのトラッキングを有効にします。</p> <p>TLOC アクションオプションを設定すると、Cisco Catalyst SD-WAN コントローラ が最終的な宛先デバイスへのパスをエンドツーエンドでトラッキングできるようになります。</p>



(注) **preferences** コマンドは、インバウンドとアウトバウンドのトラフィックをトンネルに向けるためのプリファレンスを制御します。設定は 0 ~ 4294967295 (232-1) の値で、デフォルト値は 0 です。高い値が低い値に優先します。

Cisco vEdge device に 2 つ以上のトンネルがあるとき、すべての TLOC のプリファレンスが同じで、トラフィックフローに影響を与えるポリシーが適用されていない場合、すべての TLOC が OMP にアダプタイズされます。ルータがトラフィックを送受信するときは、ECMP を使用して、トラフィックフローをトンネル間で均等に分散します。

アクションパラメータ：データポリシー

表 14: 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスのパス設定のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	Cisco IOS XE Catalyst SD-WAN デバイスに拡張され、ポリシーアクションに対して1つ以上のローカルトランスポートロケータ (TLOC) を選択することをサポートします。
データポリシーを使用したSIGへのトラフィックリダイレクト	Cisco IOS XE リリース 17.4.1 Cisco vManage リリース 20.4.1	この機能を使用すると、データポリシーの作成時に、アプリケーションリストを他の一致基準とともに定義し、アプリケーショントラフィックをセキュアインターネットゲートウェイ (SIG) にリダイレクトできます。
データポリシーにおけるネクストホップアクションの拡張	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能は、Cisco IOS XE Catalyst SD-WAN デバイスで設定された機能との同等になるよう、一元管理型データポリシーの一致アクション条件を強化します。 next-hop-loose アクションを設定している場合、この機能はネクストホップアドレスを使用できない際に、アプリケーショントラフィックを使用可能なルートにリダイレクトするのに役立ちます。
データポリシーを使用したSIGへのトラフィックリダイレクション：ルーティングへのフォールバック	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能を使用すると、すべてのSIGトンネルがダウンしている場合に、フォールバックメカニズムとして、インターネットに向かうトラフィックがCisco Catalyst SD-WAN オーバーレイを介してルーティングされるように設定できます。
ローカライズ型データポリシーと一元管理型データポリシーの両方のログアクション	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	この機能では、Cisco IOS XE Catalyst SD-WAN デバイスでデータポリシーを設定する際に、データポリシー、アプリケーションルートポリシー、およびローカライズ型ポリシーのログアクションパラメータを設定できます。log パラメータを使用すると、パケットがログに記録され、syslog メッセージを生成できます。フローがアクティブな場合、ログは5分ごとに外部のsyslog サーバーにエクスポートされます。 policy log-rate-limit コマンドを使用して、設定されたレートに従ってポリシーログを制御できます。

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るか、ドロップできます。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。

CLIでは、**policy data-policy vpn-list sequence action** コマンドによって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。

アクション条件	説明
[承認 (Accept)]をクリック	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。
Cflowd	cflowd トラフィックモニタリングを有効にします。
カウンタ	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。カウンタの名前を指定します。Cisco IOS XE Catalyst SD-WAN デバイス 上で show policy access-lists counters コマンドを使用します。
[ドロップ (Drop)]をクリック	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。
ログ	<p>最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a および Cisco vManage リリース 20.11.1</p> <p>ロギングを有効にするには、[ログ (Log)]をクリックします。</p> <p>(DP、AAR、または ACL) データポリシーパケットにログアクションが設定されている場合、ログが生成され、syslog に記録されます。グローバルな log-rate-limit により、すべてのログがログに記録されるわけではありません。パケットヘッダーが最初にログに記録される際、syslog メッセージが生成され、その後もフローがアクティブである限り、5分ごとに syslog メッセージが生成されます。</p> <p>policy log-rate-limit の CLI に関する詳細については、「policy log-rate-limit command in the Cisco Catalyst SD-WAN Qualified Command Reference」ガイドを参照してください。</p>

アクション条件	説明
リダイレクト DNS	<p>DNS 要求を特定の DNS サーバーにリダイレクトします。DNS 要求のリダイレクトはオプションですが、リダイレクトする場合は両方のアクションを指定する必要があります。</p> <p>インバウンドポリシーの場合、redirect-dns host によって、DNS 応答が要求元のサービス VPN に正しく転送されるようになります。</p> <p>アウトバウンドポリシーの場合は、DNS サーバーの IP アドレスを指定してください。</p> <p>(注) Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a 以降のリリースにアップグレードする場合は、nat use-vpn 0 を介してリダイレクト DNS を設定して、DNS をダイレクトインターネットインターフェイス (DIA) にリダイレクトする必要があります。</p> <p>(注) 同じシーケンスのアクションとして redirect-dns でローカル TLOC プリファレンスのみを設定できますが、リモート TLOC は設定できません。</p> <p>(注) リダイレクト DNS と SIG を同時に設定することはできません。</p> <p>NAT DIA フォールバックと DNS リダイレクションは、データポリシーで同時にサポートされません。</p>
TCP 最適化	TCP を微調整してラウンドトリップ遅延を減らし、TCP トラフィックのマッチング全体を向上させます。
セキュア インターネット ゲートウェイ	<p>アプリケーショントラフィックを SIG にリダイレクトします。</p> <p>(注) アプリケーショントラフィックを SIG にリダイレクトするデータポリシーを適用する前に、SIG トンネルを設定しておく必要があります。</p> <p>自動 SIG トンネルの設定の詳細については、「Automatic Tunnels」を参照してください。手動 SIG トンネルの設定の詳細については、「Manual Tunnels」を参照してください。</p> <p>[ルーティングにフォールバック (Fallback to Routing)] チェックボックスをオンにして、すべての SIG トンネルがダウンしている場合に、インターネットに向かうトラフィックを Cisco SD-WAN オーバーレイ経由でルーティングします。このオプションは、Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 で導入されました。</p>



- (注) Cisco IOS XE Catalyst SD-WAN デバイス では、TCP 最適化が削除されると、最適化が進行中のすべてのフローがドロップされます。

次に、受け入れられるパケットに対して以下のパラメータを設定できます。

アクション条件	説明
Cflowd	cflowd トラフィックモニタリングを有効にします。
NAT プールまたは NAT VPN	NAT 機能を有効にして、トラフィックをインターネットやその他の外部接続先に直接リダイレクトできるようにします。ルータごとに最大 31 (1 ~ 31) の NAT プールを設定できます。
[DSCP]	DSCP 値。範囲は 0 ~ 63 です。
Forwarding Class	転送クラスの名前。
ローカル TLOC	色およびカプセル化に一致する TLOC の 1 つにパケットを送信できるようにします。使用できる色は、3g、biz-internet、blue、bronze、custom1、custom2、custom3、default、gold、green、lte、metro-ethernet、mpls、private1~private6、public-internet、red、silver です。 カプセル化オプションは、 ipsec および gre です。 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。 デフォルトでは、カプセル化は ipsec です。
Next Hop	パケットの転送先となるネクストホップ IP アドレスを設定します。 (注) Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a および Cisco vManage リリース 20.5.1 以降では、[ネクストホップが使用できない場合にデフォルトルートを使用 (Use Default Route when Next Hop is not available)] フィールドが、[ネクストホップアクション (Next Hop action)] パラメータの横に表示されます。このオプションは、シーケンスタイプが [トラフィックエンジニアリング (Traffic Engineering)] または [カスタム (Custom)] で、プロトコルが IPv4 または IPv6 のいずれかの場合にのみ使用でき、両方では使用できません。
Policer	ポリサーを適用します。 policy policer コマンドで設定されたポリサーの名前を指定します。

アクション条件	説明
Service	<p>トラフィックを宛先に配信する前にリダイレクトするサービスを指定します。</p> <p>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。</p> <p>VPN 識別子は、サービスが配置されている場所です。</p> <p>標準サービス：FW、IDS、IDP</p> <p>カスタムサービス：netsvc1、netsvc2、netsvc3、netsvc4</p> <p>TLOC リストは、policy lists tloc-list リストで設定されます。</p> <p>vpn service コマンドを使用して、サービスデバイスと併置された Cisco IOS XE Catalyst SD-WAN デバイスでサービス自体を設定します。</p>
TLOC	<p>リスト内のいずれかの TLOC の IP アドレス、色、およびカプセル化に一致するリモート TLOC にトラフィックを転送します。一致する TLOC にプリファレンス値が設定されている場合、その値がトラフィックに割り当てられます。</p>
[承認 (Accept)]をクリックし、[VPN]アクションを実行	<p>パケットが属する VPN を設定します。範囲は 0 ～ 65530 です。</p>



(注) データポリシーは、マッチ条件が「一般 (generic) 」の場合、ルーティングプロトコルパケットを含むローカルで生成されたパケットに適用されます。

設定例：

```
sequence 21
  match
    source-ip 10.0.0.0/8
  action accept
```

このような状況では、ルーティングプロトコルパケットをエスケープするシーケンスを、データポリシーに追加する必要がある場合があります。たとえば、OSPF をスキップするには、次の設定を使用します。

```
sequence 20
  match
    source-ip 10.0.0.0/8
    protocol 89
  action accept
sequence 21
  match
    source-ip 10.0.0.0/8
  action accept
```

次の表では、IPv4 および IPv6 のアクションについて説明します。

表 15:

IPv4 アクション	IPv6 アクション
drop、dscp、next-hop (from-service のみ) /vpn、count、転送クラス、ポリサー (インターフェイス ACL のみ)、App-route SLA (のみ)	該当なし
app-route preferred color、app-route sla strict、cflowd、nat、redirect-dns	該当なし
該当なし	drop、dscp、next-hop/vpn、count、転送クラス、ポリサー (インターフェイス ACL のみ) App-route SLA (のみ)、App-route preferred color、app-route sla strict
ポリサー (DataPolicy)、tcp-optimization、fec-always、	ポリサー (DataPolicy)
tloc、tloc-list (set tloc、set tloc-list)	tloc、tloc-list (set tloc、set tloc-list)
App-Route backup-preferred color、local-tloc、local-tloc-list	App-Route backup-preferred color、local-tloc、local-tloc-list

サイトと VPN へのポリシーの適用

[サイトと VPN にポリシーを適用 (Apply Policies to Sites and VPNs)] ページで、サイトと VPN にポリシーを適用します。

- [ポリシー名 (Policy Name)] フィールドに、ポリシーの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0～9の数字、ハイフン (-)、下線 () のみです。スペースやその他の文字を含めることはできません。
- [ポリシーの説明 (Policy Description)] フィールドに、ポリシーの説明を入力します。最大 2048 文字を使用できます。このフィールドは必須であり、任意の文字とスペースを含めることができます。
- ポリシーを VPN とサイトに関連付けます。VPN とサイトの選択肢は、ポリシーブロックのタイプによって異なります。
 - [トポロジ (Topology)] ポリシーブロックの場合は、[新しいサイトリスト (New Site List)]、[インバウンドサイトリスト (Inbound Site List)]、[アウトバウンドサイトリスト (Outbound Site List)]、または [VPN リスト (VPN List)] をクリックします。トポロジブロックによっては [追加 (Add)] ボタンがない場合があります。1つ以上のサイトリストを選択し、1つ以上の VPN リストを選択します。[Add] をクリックします。

2. [アプリケーション認識型ルーティング (Application-Aware Routing)] ポリシーブロックの場合は、[新しいサイトリスト (New Site List)] と [VPNリスト (VPN list)] をクリックします。1つ以上のサイトリストを選択し、1つ以上の VPN リストを選択します。[Add] をクリックします。
3. [トラフィックデータ (Traffic Data)] ポリシーブロックの場合は、[新しいサイトリストとVPNリスト (New Site List and VPN List)] をクリックします。ポリシーを適用する方向 ([サービスから (From Service)]、[トンネルから (From Tunnel)]、[すべて (All)]) を選択し、1つ以上のサイトリストおよび1つ以上の VPN リストを選択します。[Add] をクリックします。
4. cflowd ポリシーブロックの場合は、[新しいサイトリスト (New Site List)] をクリックします。1つ以上のサイトリストを選択し、[追加 (Add)] をクリックします。
4. [プレビュー (Preview)] をクリックして、設定されたポリシーを表示します。ポリシーは CLI形式で表示されます。
5. [Save Policy] をクリックします。[設定 (Configuration)] > [ポリシー (Policies)] を選択すると、ポリシーテーブルに新しく作成されたポリシーが表示されます。

Cisco IOS XE Catalyst SD-WAN デバイスでの NAT フォールバック

	リリース情報	
Cisco IOS XE Catalyst SD-WAN デバイスでの NAT フォールバック	Cisco IOS XE リリース 17.3.2 Cisco vManage リリース 20.3.2	Cisco IOS XE Catalyst SD-WAN デバイスでは、ダイレクトインターネットアクセス (DIA) の NAT フォールバック機能をサポートしています。NAT フォールバック機能は、DIA ルートに送信されるすべてのトラフィックが必要に応じて代替ルートを使用できるように、ルーティングベースのメカニズムを提供します。このリリースでは、サービス側とトンネル側でフォールバックがサポートされます。



(注) Cisco SD-WAN Manager を使用して NAT DIA フォールバックを設定するには、Cisco SD-WAN Manager によって Cisco Catalyst SD-WAN コントローラ が管理される必要があります。

Cisco SD-WAN Manager を使用して NAT フォールバックを有効にするには、次の手順を実行してデータポリシーを作成および設定します。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [カスタムオプション (Custom Options)] ドロップダウンの [一元管理型ポリシー (Centralized Policy)] で [トラフィックポリシー (Traffic Policy)] を選択します。
3. [トラフィックデータ (Traffic Data)] をクリックします。
4. [ポリシーの追加 (Add Policy)] ドロップダウンから、[新規作成 (Create New)] を選択します。
5. [シーケンスタイプ (Sequence Type)] をクリックし、[カスタム (Custom)] を選択します。
6. [(+)シーケンスルール (Sequence Rule)] をクリックして、新規のシーケンスルールを作成します。
7. マッチ条件を追加したら、[アクション (Actions)]、[承認 (Accept)] の順にクリックします。
8. [NAT VPN] をクリックし、[フォールバック (Fallback)] チェックボックスをオンにします。
9. [アクションの保存と照合 (Save and Match Actions)] をクリックします。
10. [データポリシーの保存 (Save Data Policy)] をクリックします。

既存の一元管理型ポリシーを編集し、ポリシーをインポートします。

1. [一元管理型ポリシー (Centralized Policy)] をクリックし、必要な一元管理型ポリシーの [...] をクリックして [編集 (Edit)] を選択します。
2. [トラフィックルール (Traffic Rules)] をクリックし、[トラフィックデータ (Traffic Data)] を選択します。
3. [ポリシーの追加 (Add Policy)] ドロップダウンから、[既存のインポート (Import Existing)] を選択します。
4. [ポリシー (Policy)] ドロップダウンから、作成した NAT ポリシーを選択します。
5. [ポリシー適用 (Policy Application)] をクリックし、[トラフィックデータ (Traffic Data)] を選択します。
6. [+新しいサイトリストとVPNリスト (+New Site List and VPN List)] をクリックします。
7. 必要に応じて、方向、VPN、およびサイトを選択します。
8. [Add] をクリックします。
9. [ポリシーの変更の保存 (Save Policy Changes)] をクリックします。
10. [VPN] をクリックして、ドロップダウンから [Site] を選択します。



(注) **from-tunnel** トラフィックに設定されたポリシーは、トンネル経由のリターントラフィックとは別に、リターンDIA（アンダーレイ）トラフィックにも適用されます。そのポリシーのシーケンスのいずれも一致しない場合は、そのポリシーのデフォルトシーケンスと一致します。



(注) NAT DIA フォールバックと DNS リダイレクションは、データポリシーで同時にサポートされません。

次の NAT フォールバックアクション/コマンドがサポートされるようになりました。

- アクション : `nat fallback`
- ポリシーを適用する場合 : `direction from-tunnel`

一元管理型ポリシーのアクティブ化

一元管理型ポリシーをアクティブにすると、接続されているすべての Cisco SD-WAN コントローラにそのポリシーが送信されます。一元管理型ポリシーを有効にするには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Policies]** の順に選択します。[一元管理型ポリシー (Centralized Policy)] がデフォルトで選択され、表示されます。
2. 必要なポリシーについて、[...] をクリックし、**[アクティブ化 (Activate)]** を選択します。[ポリシーのアクティブ化 (Activate Policy)] ポップアップが表示されます。ポリシーが適用される到達可能な Cisco SD-WAN コントローラの IP アドレスが一覧表示されます。
3. **[Activate]** をクリックします。

一元管理型ポリシーの表示

一元管理型ポリシーを表示するには、次の手順を実行します。

1. [一元管理型ポリシー (Centralized Policy)] から、ポリシーを選択します。
2. UI ポリシービルダーまたは CLI を使用して作成されたポリシーの場合は、[...] をクリックし、**[表示 (View)]** を選択します。UI ポリシービルダーを使用して作成されたポリシーはグラフィカル形式で表示され、CLI メソッドを使用して作成されたポリシーはテキスト形式で表示されます。
3. Cisco SD-WAN Manager ポリシー構成ウィザードを使用して作成されたポリシーの場合は、[...] をクリックし、**[プレビュー (Preview)]** を選択します。このポリシーはテキスト形式で表示されます。

ポリシーのコピー、編集、削除

ポリシーをコピーするには、次の手順を実行します。

1. [一元管理型ポリシー (Centralized Policy)] から、ポリシーを選択します。
2. 目的のポリシーについて、[...] をクリックし、[コピー (Copy)] を選択します。
3. [ポリシーのコピー (Policy Copy)] ポップアップウィンドウで、ポリシー名とポリシーの説明を入力します。



(注) Cisco IOS XE リリース 17.2 以降では、次のポリシータイプのポリシー名に 127 文字がサポートされています。

- 中央ルートポリシー
- ローカルルートポリシー
- ローカルアクセス制御リスト (ACL)
- ローカル IPv6 ACL
- 中央データポリシー
- 中央アプリケーションルート ポリシー
- QoS マップ
- 書き換えルール

他のすべてのポリシー名は 32 文字をサポートします。

4. [コピー (Copy)] をクリックします。

Cisco SD-WAN Manager ポリシー構成ウィザードで作成したポリシーを編集するには、次の手順を実行します。

1. 目的のポリシーについて、[...] をクリックし、[編集 (Edit)] を選択します。
2. 必要に応じて、ポリシーを編集します。
3. [ポリシーの変更の保存 (Save Policy Changes)] をクリックします。

CLI 方式で作成されたポリシーを編集するには、次の手順を実行します。

1. [カスタムオプション (Custom Options)] ドロップダウンで、[CLIポリシー (CLI Policy)] をクリックします。
2. 目的のポリシーについて、[...] をクリックし、[編集 (Edit)] を選択します。
3. 必要に応じて、ポリシーを編集します。
4. [Update] をクリックします。

ポリシーを削除するには、次の手順を実行します。

1. [一元管理型ポリシー (Centralized Policy)] から、ポリシーを選択します。
2. 目的のポリシーについて、[...] をクリックし、[削除 (Delete)] を選択します。
3. [OK] をクリックして、ポリシーの削除を確認します。

CLI を使用した、一元管理型ポリシーの設定

CLI を使用して一元管理型制御ポリシーを設定するには、次の手順を実行します。

1. 次のように、一元管理型制御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 (**apply-policy** コマンドを使用)。

```
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. 必要に応じて、次のように IP プレフィックスと TLOC、VPN のリストを作成します。

```
vSmart(config)# policy lists
vSmart(config-lists)# prefix-list list-name
vSmart(config-lists-list-name)# ip-prefix prefix/length
vSmart(config)# policy lists
vSmart(config-lists)# tloc-list list-name
vSmart(config-lists-list-name)# tloc address
color color
encap encapsulation
[preference value]
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-list-name)# vpn vpn-id

vsmart(config)# policy lists data-ipv6-prefix-list dest_ip_prefix_list
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# ipv6-prefix 2001:DB8::/32
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# commit
Commit complete.

vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match destination-data-ipv6-prefix-list
dest_ip_prefix_list
vsmart (config-match)# commit
vsmart(config-match)# exit
vsmart(config-sequence-100)# match source-data-ipv6-prefix-list dest_ip_prefix_list
vm9(config-match)# commit
Commit complete.
vm9(config-match)# end

vsmart(config)# policy
vsmart(config-policy)# data-policy data_policy_1
vsmart(config-data-policy-data_policy_1)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 101
vsmart(config-sequence-101)# match source-ipv6 2001:DB8::/32
vsmart(config-match)# exit
```



```
vsmart(config-sequence-101)# match destination-ipv6 2001:DB8::/32
vsmart(config-match)#
```

3. 次のように制御ポリシーインスタンスを作成します。

```
vSmart(config)# policy control-policy policy-name
vSmart(config-control-policy-policy-name)#
```

4. 一連のマッチ/アクションペアのシーケンスを次のように作成します。

```
vSmart(config-control-policy-policy-name)# 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。

5. ルートおよび TLOC のマッチパラメータを次のように定義します。

```
vSmart(config-sequence-number)# match route route-parameter
vSmart(config-sequence-number)# match tloc tloc-parameter
```

6. 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 reject
vSmart(config-sequence-number)# action accept export-to (vpn
vpn-id | vpn-list list-name)
vSmart(config-sequence-number)# action accept set omp-tag
number

vSmart(config-sequence-number)# action accept set
preference value

vSmart(config-sequence-number)# action accept set
service service-name
(tloc ip-address |
tloc-list list-name)
[vpn vpn-id]

vSmart(config-sequence-number)# action accept set tloc
ip-address
color color
[encap encapsulation]
vSmart(config-sequence-number)# action accept set tloc-action
action

vSmart(config-sequence-number)# action accept set tloc-list list-name
```

7. 必要に応じて、制御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。

8. 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。マッチしないルート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
```

9. Cisco Catalyst SD-WAN 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
control-policy
policy-name (in | out)
```

10. 設定するアクションがサービスの場合は、次のように、Cisco IOS XE Catalyst SD-WAN デバイスに必要なサービスを設定して、Cisco Catalyst SD-WAN コントローラがサービスに到達する方法を認識できるようにします。

```
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1 sequence 100
vsmart(config-sequence-100)# action accept set next-hop-ipv6 2001:DB8::/32
vsmart(config-set)#
```

サービスが配置されている VPN と、サービス側デバイスに到達するための 1～4 つの IP アドレスを指定します。複数のデバイスが同じサービスを提供する場合、デバイスはそれらの間でトラフィックをロードバランシングします。Cisco IOS XE Catalyst SD-WAN デバイスはサービスを追跡し、アドレス（またはアドレスの 1 つ）がローカルで、つまりデバイスのローカルサイトで解決でき、OMP を介して学習されない場合にのみ、サービスを Cisco Catalyst SD-WAN コントローラにアドバタイズします。以前にアドバタイズされたサービスが使用できなくなった場合、Cisco IOS XE Catalyst SD-WAN デバイスはサービスアドバタイズメントを撤回します。

次に、VPN メンバーシップ データ ポリシーを設定するための手順について概要を示します。

1. 次のように、VPN メンバーシップ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（**apply-policy** コマンドを使用）。

```
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. 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

vsmart(config)# policy lists data-ipv6-prefix-list dest_ip_prefix_list
vsmart (config-data-ipv6-prefix-list-dest_ip_prefix_list)# ipv6-prefix 2001:DB8:19::1
vsmart (config-data-ipv6-prefix-list-dest_ip_prefix_list)# commit
Commit complete.

vsmart (config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match destination-data-ipv6-prefix-list
dest_ip_prefix_list
vsmart (config-match)# commit
vsmart (config-match)# exit
vsmart (config-sequence-100)# match source-data-ipv6-prefix-list dest_ip_prefix_list
vm9 (config-match)# commit
Commit complete.
vm9 (config-match)# end
```

```
vsmart(config)# policy
vsmart(config-policy)# data-policy data_policy_1
vsmart(config-data-policy-data_policy_1)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 101
vsmart(config-sequence-101)# match source-ipv6 2001:DB8:19::1
vsmart(config-match)# exit
vsmart(config-sequence-101)# match destination-ipv6 2001:DB8:19::1
vsmart(config-match)#
```

3. 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]
```

4. 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
```

5. 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
```

6. 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。

7. 次のように、パケットのマッチパラメータを定義します。

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

8. 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 counter-name] [log]
[tcp-optimization]
vSmart(config-sequence-number)# action accept nat [pool number] [use-vpn 0]
vSmart(config-sequence-number)# action accept redirect-dns (host | ip-address)
vSmart(config-sequence-number)# action accept set parameters

vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1 sequence 100
vsmart(config-sequence-100)# action accept set next-hop-ipv6 2001:DB8:19::1
vsmart(config-set)#
```

9. 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。

10. 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。マッチしないプレフィックス付きルート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
```

11. 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)
```

一元管理型ポリシーの設定例

このトピックでは、Cisco IOS XE Catalyst SD-WAN ドメイン全体のトラフィックフローに影響を与えたり、Cisco IOS XE Catalyst SD-WAN デバイスをインターネット出口ポイントとして設定できる一元管理型データポリシーの設定例をいくつか紹介します。

一般的な一元管理型ポリシーの例

このセクションでは、Cisco Catalyst SD-WAN コントローラ で一元管理型データポリシーを設定してその設定をコミットした後、ポリシーそのものによって、必要な Cisco IOS XE Catalyst SD-WAN デバイ스에 プッシュされることを示す一元管理型データポリシーの一般的な例を紹介します。

ここでは、Cisco Catalyst SD-WAN コントローラ `vm9` で次のような単純なデータポリシーを設定するとします。

```
vm9# show running-config policy
policy
  data-policy test-data-policy
  vpn-list test-vpn-list
  sequence 10
  match
    destination-ip 209.165.201.0/27
    !
  action drop
  count test-counter
  !
  !
  default-action drop
  !
  !
lists
  vpn-list test-vpn-list
  vpn 1
  !
  site-list test-site-list
  site-id 500
  !
  !
  !
```

次に、**test-site-list** という、サイト500を含むサイトリストに、このポリシーを以下のように適用します。

```
vm9# show sdwan running-config apply-policy
apply-policy
  site-list test-site-list
  data-policy test-data-policy
  !
  !
```

Cisco Catalyst SD-WAN コントローラ は設定がアクティブ化されるとすぐに、サイト 500 の Cisco IOS XE Catalyst SD-WAN デバイス にポリシー設定をプッシュします。こうしたデバイスの 1 つである vm5 について、ポリシーが受信されたことが以下から確認できます。

```
vm5# show sdwan policy from-vsmart
policy-from-vsmart
data-policy test-data-policy
vpn-list test-vpn-list
sequence 10
match
destination-ip 209.165.201.0/27
!
action drop
count test-counter
!
!
default-action drop
!
!
lists
vpn-list test-vpn-list
vpn 1
!
!
!
```

アクセス制御

次は、データポリシーによって、送信元から特定の宛先に送信できるパケットタイプを制限する例を示しています。ここでは、サイト 100 の送信元アドレス 192.0.2.1 のホストと VPN 100 は、203.0.113.1 の宛先ホストに TCP トラフィックのみを送信できるようになっています。このポリシーでは、192.0.2.1 によって送信される TCP トラフィックのネクストホップも指定して、TLOC 209.165.200.225、カラーをゴールドに設定しています。他のトラフィックは、**default-action** ステートメントの結果として、すべて受け入れられます。

```
policy
lists
site-list north
site-id 100
vpn-list vpn-north
vpn 100
!
data-policy tcp-only
vpn-list vpn-north
sequence 10
match
source-ip 192.0.2.1/32
destination-ip 198.51.100.1/32
protocol tcp
action accept
set tloc 203.0.113.1 gold
!
default-action accept
!
!
apply-policy
site north data-policy tcp-only
```

トラフィック制限

次の例は、特定のタイプのデータトラフィックが VPN 間で送信されないようにする方法を示しています。このポリシーは、SMTP メールトラフィックを伝送するポート 25 で、209.165.201.0/27 を発信元とするデータトラフィックをドロップします。ただし、このポリシーは、209.165.201.0/27 からの非 SMTP トラフィックを含む、他のすべてのデータトラフィックを受け入れます。

```

policy
  lists
    data-prefix-list north-ones
      ip-prefix 209.165.201.0/27
      port 25
    vpn-list all-vpns
      vpn 1
      vpn 2
    site-list north
      site-id 100
  !
  data-policy no-mail
    vpn-list all-vpns
      sequence 10
      match
        source-data-prefix-list north-ones
      action drop
    !
    default-action accept
  !
!
apply-policy
  site north data-policy no-mail

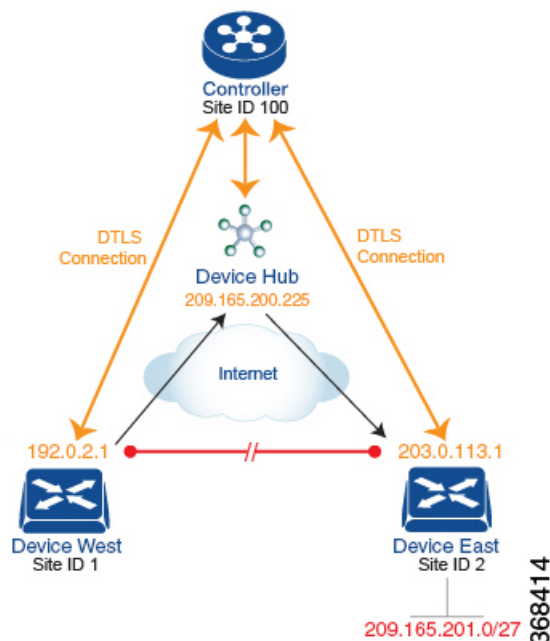
```

トラフィック エンジニアリング

次は、すべてのトラフィックを直接ではなく、デバイスハブを介して Cisco IOS XE Catalyst SD-WAN デバイスに流入させるようにするトラフィック エンジニアリングの例です。

Cisco IOS XE Catalyst SD-WAN オーバーレイネットワークでドメインを設計する一般的な方法の 1 つに、ある Cisco IOS XE Catalyst SD-WAN デバイスから別のデバイスにトラフィックを直接送信するのではなく、データセンターに通常配置されているハブルータを介して、ブランチ宛てのすべてのトラフィックをルーティングするということがあります。これは、1 つのデバイスがハブとして機能し、別のデバイスがスポークであるハブアンドスポーク設計と考えることができます。このような設計では、ローカルブランチ間のトラフィックは、デバイスの起動時にスポークルータとハブルータの間に確立される IPsec 接続を介して移動します。確立された接続を使用すると、デバイスは、互いに IPsec 接続を確立するための時間と CPU サイクルを費やす必要がなくなります。これが多数のデバイスを含む大規模なネットワークだった場合、ルータの各ペア間でフルメッシュの接続を確立すると、ルータの CPU が大量に必要になります。この設計のもう 1 つの特性として、管理という観点から見た場合、ハブルータには、調整したトラフィックフローポリシーを設定した方が簡単はずです。なぜならオーバーレイネットワーク内のハブルータは数が少ない上に、一元管理型データセンターに配置されているからです。

すべてのデバイス スポーク ルータ トラフィックを Cisco ハブルータに転送するには、1 つの方法として、ローカルネットワーク内のルートに関連付けられた TLOC を変更するポリシーを作成するということがあります。次の図のトポロジについて考えてみましょう。



このトポロジには、異なるブランチに2つのデバイスがあります。

- サイト ID 1 のデバイス西。このデバイスの TLOC は、IP アドレス (192.0.2.1)、カラー (ゴールド)、およびカプセル化 (ここでは IPsec) によって定義されます。TLOC の全アドレスを記述するなら、{192.0.2.1, gold, ipsec} となります。カラーは、単にトラフィックのフローを識別し、他のフローと区別するための方法です。
- サイト ID 2 のデバイス東の TLOC アドレスは、{203.0.113.1, gold, ipsec} です。

デバイス西とデバイス東は、Cisco Catalyst SD-WAN コントローラによって配布された OMP ルートから互いの TLOC アドレスを学習します。この例では、デバイス東が、プレフィックス 209.165.201.0/27 を TLOC {203.0.113.1, gold, } で到達可能なものとしてアドバタイズします。ポリシーが何もなければ、デバイス西は 209.165.201.0/27 宛てのトラフィックを TLOC {203.0.113.1, gold, ipsec} にルーティングできるでしょう。つまり、トラフィックは、デバイス西からデバイス東に直接送信されることになるはずということです。

ただし、この設計では、デバイス西からデバイス東へのすべてのトラフィックは、デバイス東に移動する前に、TLOC アドレスが {209.165.200.225, gold, ipsec} であるハブルータを介してルーティングされる必要があります。このトラフィックフローを有効にするには、ルートの TLOC を変更するポリシーを定義します。そこで、プレフィックス 209.165.201.0/27 に関して、プレフィックス 209.165.201.0/27 に関連付けられている TLOC を、デバイス東の TLOC アドレスである {203.0.113.1, gold, ipsec} から、ハブルータの TLOC アドレスである {209.165.200.225, gold, ipsec} に変更するポリシーを作成します。こうしてできるのが、Cisco Catalyst SD-WAN コントローラによってデバイス西にアドバタイズされ、デバイス東の TLOC アドレスではなく、ハブルータの TLOC アドレスを含むプレフィックス 209.165.201.0/27 の OMP ルートです。トラフィックフローの観点から見ると、デバイス西は 209.165.201.0/27 宛てのすべてのトラフィックをハブルータに送信します。

また、デバイスは、Cisco Catalyst SD-WAN コントローラ によってアドバタイズされた OMP ルートからデバイス西およびデバイス東の TLOC アドレスを学習します。デバイスはこれら 2 つの TLOC アドレスを使用する必要があるため、ハブによるデバイスへのトラフィックの転送方法を制御するためのポリシーは必要ありません。

デバイス西（およびネットワークドメイン内の他のデバイス）に対し、プレフィックス 209.165.201.0/27 宛でのトラフィックをデバイスである TLOC 209.165.200.225（ゴールド）に送信するよう指示する場合の、Cisco Catalyst SD-WAN コントローラ でのポリシー設定は次のようになります。

```
policy
  lists
    prefix-list east-prefixes
      ip-prefix 209.165.201.0/27
    site-list west-sites
      site-id 1
  control-policy change-tloc
    sequence 10
    match route
      prefix-list east-prefixes
      site-id 2
    action accept
      set tloc 209.165.200.225 color gold encaps ipsec
  apply-policy
    site west-sites control-policy change-tloc out
```

このポリシーの大まかな英語訳は次のとおりです。

```
Create a list named "east-prefixes" that contains the IP prefix "209.165.201.0/27"
Create a list named "west-sites" that contains the site-id "1"
Define a control policy named "change-tloc"
Create a policy sequence element that:
  Matches a prefix from list "east-prefixes", that is, matches "209.165.201.0/27"
  AND matches a route from site-id "2"
If a match occurs:
  Accept the route
  AND change the route's TLOC to "209.165.200.225" with a color of "gold" and an
  encapsulation of "ipsec"
Apply the control policy "change-tloc" to OMP routes sent by the vSmart
controller to "west-sites", that is, to site ID 1
```

この制御ポリシーは、`apply-policy site` コマンドの `out` オプションで示されるように、アウトバウンドポリシーとして Cisco Catalyst SD-WAN コントローラ で設定されます。このオプションでは、Cisco Catalyst SD-WAN コントローラ はルートテーブルからルートを配布した後に、OMP ルートに TLOC 変更を適用することになります。Cisco Catalyst SD-WAN コントローラ がデバイス西に配布するプレフィックス 209.165.201.0/27 の OMP ルートは、209.165.201.0/27 を TLOC 209.165.200.225（ゴールド）に関連付けます。これが、デバイス西のルートテーブルにインストールされる OMP ルートです。最終的に、デバイス西が 209.165.201.0/27 にトラフィックを送信すると、トラフィックはハブに送信されます。また、デバイス西とデバイス東との間で DTLS トンネルが直接確立されることはありません。

ネットワークの西側に 1 つではなく多数のサイトがあり、その各サイトに独自のデバイスがある場合も、容易にこの同じポリシーをすべてのサイトに適用できます。これを行うには、ただ `site-list west-sites` リストに、すべてのサイトのサイト ID を追加するだけです。ポリシーにたったこれだけの変更を行うだけで、すべての西側サイトから、デバイスを介してプレフィックス

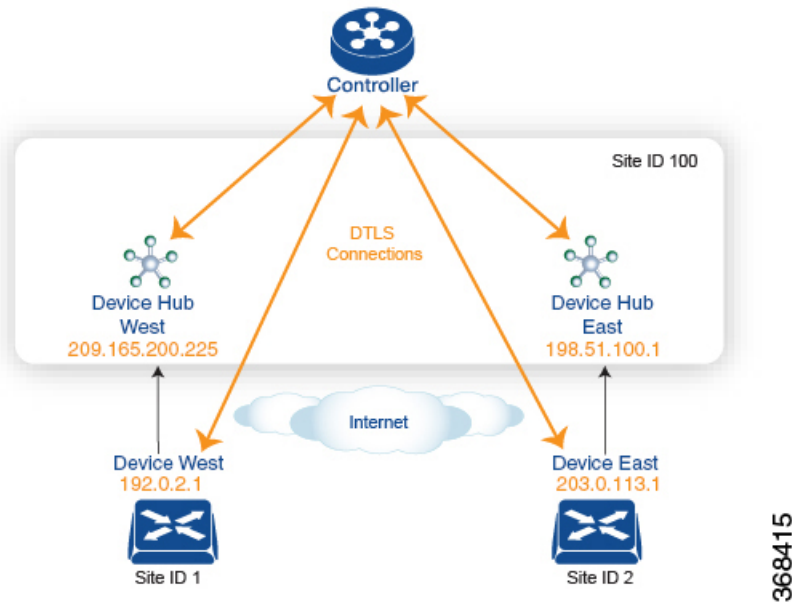
209.165.201.0/27 にバインドさせたトラフィックを送信させることができます。次に例を示します。

```
policy
  lists
    prefix-list east-prefixes
      ip-prefix 209.165.201.0/27
    site-list west-sites
      site-id 1
      site-id 11
      site-id 12
      site-id 13
    control-policy change-tloc
      sequence 10
      match route
        prefix-list east-prefixes
        site-id 2
      action accept
        set tloc 209.165.200.225 color gold encaps ipsec
  apply-policy
    site west-sites control-policy change-tloc out
```

任意のトポロジの作成

前の例で説明したハブアンドスポークスタイルのトポロジに冗長性を持たせる場合、Cisco ハブをもう1つ追加してデュアルホームハブサイトを作成することができます。次の図は、サイト ID 100 に2つのデバイスハブがあることを示しています。すべてのブランチ間トラフィックは、今まで通り、デバイスハブを介してルーティングする必要があります。ただし、今はデュアルホーム接続されたハブがあるため、データトラフィックは2つのハブルータ間で共有する必要があります。

- デバイスハブ西（TLOC 209.165.200.225、ゴールド）。オーバーレイネットワークの西側にあるブランチからのすべてのデータトラフィックは通過させて、このデバイスで処理する必要があります。
- デバイスハブ東（TLOC 198.51.100.1、ゴールド）。同様に、東側のすべてのデータトラフィックはデバイスハブ東を通過させます。



368415

西側のデータトラフィックはデバイスハブ西を介して送信し、東西のトラフィックはデバイスハブ東を介して送信されるようにする場合、Cisco Catalyst SD-WAN コントローラのポリシー設定は次のようになります。

```

policy
  lists
    site-list west-sites
      site-id 1
    site-list east-sites
      site-id 2
    tloc-list west-hub-tlocs
      tloc-id 209.165.200.225 gold
    tloc-list east-hub-tlocs
      tloc-id 198.51.100.1 gold
  control-policy prefer-west-hub
    sequence 10
    match tloc
      tloc-list west-hub-tlocs
    action accept
    set preference 50
  control-policy prefer-east-hub
    sequence 10
    match tloc
      tloc-list east-hub-tlocs
    action accept
    set preference 50
  apply-policy
    site west-sites control-policy prefer-west-hub out
    site east-sites control-policy prefer-east-hub out

```

このポリシー設定に関する説明は次の通りです。

apply-policy 構成コマンドに必要なサイトリストの作成。

- **site-list west-sites** は、オーバーレイネットワークの西側にある、すべてのデバイスの全サイト ID を一覧表示するものです。

- **site-list east-sites** は、ネットワークの東側にあるデバイスのサイト ID を一覧表示するものです。

制御ポリシーのマッチ条件に必要な TLOC リストの作成。

- **west-hub-tlocs** は、西側デバイスからのトラフィックを処理するのに必要なデバイスハブ西の TLOC を一覧表示するものです。
- **east-hub-tlocs** は、東側デバイスからのトラフィックを処理するために、デバイスハブ東の TLOC を一覧表示するものです。

2つの制御ポリシーの定義。

- **prefer-west-hub** は、デバイス西ハブルータの TLOC アドレスである TLOC 209.165.200.225 (ゴールド) を宛先とする OMP ルートに影響を与えるものです。このポリシーによって、OMP ルートのプリファレンス値が 50 に変更されます。この値は十分大きいので、大きなプリファレンス値を持つ OMP ルートは他にないはずですが、プリファレンス値を高く設定することで、サイト 100 宛でのトラフィックがデバイス西ハブルータに転送されます。
- 同様に、**prefer-east-hub** は、デバイス東ハブルータの TLOC アドレスである TLOC 198.51.100.1 (ゴールド) を宛先とする OMP ルートのプリファレンス値を 50 に設定するものなので、サイト 100 宛でのトラフィックをデバイス東ハブルータである 198.51.100.1 に転送します。

制御ポリシーの適用。

- **apply-policy** 構成の最初の行によって、Cisco Catalyst SD-WAN コントローラは、**prefer-west-hub** 制御ポリシーを、**west-sites** リストに掲載されているサイト (ここではサイト ID 1 のみ) に適用させられます。そのため、TLOC 209.165.200.225 宛での OMP ルートのプリファレンス値は 50 に変更され、デバイス西からハブサイトに送信されるトラフィックはデバイス西ハブルータを通過することになります。
- Cisco Catalyst SD-WAN コントローラは、**east-sites** リスト内のデバイスにアドバタイズする OMP ルートに **prefer-east-hub** 制御ポリシーを適用します。これにより、TLOC 198.51.100.1 宛での OMP ルートのプリファレンス値が 50 に変更されるので、デバイス東のトラフィックはデバイス東ハブルータに接続することになります。

コミュニティの例

これは、コミュニティリストへの一元管理型制御ポリシーの設定例です。

```
policy
  lists
    expanded-community-list test
      community 0:110* 100:[7-9]+
      community 0:110* 11:*

    community-list test-com
      community 0:1
      community 0:2
```

```
control-policy test
 sequence 10
  match route
   expanded-community-list test

 action accept
  set
   community 100:2 100:3
  additive
```

これは、標準コミュニティリストの設定例です。

```
Standard Community list

route : 0:1234 0:11 0:12

community-list
 community 0:100
 community 0:1234
 community 0:101
 *MATCH*

route : 0:1234 0:11 0:12
community-list
 community 0:100
 community 0:5678
 community 0:101
 *NO MATCH*
```

これは、拡張コミュニティリストの設定例です。OR マッチで、コミュニティリストの各正規表現文字列をルートのコミュニティストリングと比較します。

```
Expanded Community list
route - 0:1234 0:5678
expanded-community-list:
 community 0:110* 11:
 community 0:110* 100:[7-9]+
 community 0:12[3-7]+
 *MATCH*

route - 0:1234 0:5678
expanded-community-list:
 community 0:111*
 community 0:110* 11:*
 *NO MATCH*
```

EXACT マッチの入力文字列は、コミュニティがソート順になっている必要があります。バイト値でソートし、文字列の先頭と末尾にメタ文字を追加します。

```
route - 0:1234 0:5678
expanded-community-list:
 community ^0:1234 0:5678$
 *MATCH*
```

AND マッチの入力文字列は、コミュニティがソート順になっている必要があります。ソートされたコミュニティ間でブラインドマッチを行うには、「+」を追加します。

```
route - 0:0 0:1234 0:5678 0:9789 0:9800 0:9900 0:9999 1:10
expanded-community-list:
 community 0:1234 .+ 0:9900 .+
 *MATCH*
```

SIG データポリシーのフォールバック

Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 から、**sig-action fallback-to-routing** コマンドを使用して、すべての SIG トンネルがダウンした場合に、インターネットに向かうトラフィックを Cisco Catalyst SD-WAN オーバーレイを介してルーティングさせるように設定することができます。以下は、このフォールバックメカニズムの設定を示した例です。

```
data-policy _VPN10_SIG_Fall_Back
  vpn-list VPN10
    sequence 1
      match
        app-list Google_Apps
        source-ip 0.0.0.0/0
      !
      action accept
        sig
        sig-action fallback-to-routing
      !
    !
  default-action drop
```

ランク付けカラーの優先順位の例

```
policy lists
  preferred-color-group GROUP1_COLORS
    primary-preference
      color-preference biz-internet
      path-preference direct-tunnel
    !
    secondary-preference
      color-preference mpls
      path-preference multi-hop-path
    !
    tertiary-preference
      color-preference lte
    !
  !
  preferred-color-group GROUP2_COLORS
    primary-preference
      color-preference mpls
    !
    secondary-preference
      color-preference biz-internet
    !
  !
  preferred-color-group GROUP3_COLORS
    primary-preference
      color-preference mpls biz-internet lte
    !
```

IPv6 アプリケーションに対するデータポリシーの例

```
policy
  data-policy _VPN1_Data-Policy-For-Ipv6-Traffic
    vpn-list VPN1
      sequence 1
        match
          app-list Msft-0365
          source-ipv6 0::0/0
```

```
        !
        action accept
        !
        !
        default-action drop
        !
        lists
        app-list Msft-0365
            app ms-office-web-apps
        !
        site-list SITE-100
            site-id 100
        !
        vpn-list VPN1
            vpn 1
        !
        !
        !
        apply-policy
        site-list SITE-100
            data-policy _VPN1_Data-Policy-For-Ipv6-Traffic all
        !
        !
        !
```



第 5 章

ローカライズ型ポリシー



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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、さまざまなタイプのローカライズ型ポリシー、ローカライズ型ポリシーのコンポーネント、および Cisco SD-WAN Manager または CLI を使用してローカライズ型ポリシーを設定する方法に関する概要情報を提供します。

- [ローカライズ型ポリシーの概要 \(98 ページ\)](#)
- [Cisco SD-WAN Manager を使用したローカライズ型ポリシーの設定 \(100 ページ\)](#)
- [CLI を使用した、IPv4 に対するローカライズ型ポリシーの設定 \(119 ページ\)](#)
- [CLI を使用した、IPv6 に対するローカライズ型ポリシーの設定 \(121 ページ\)](#)
- [ローカライズ型データポリシーの設定例 \(122 ページ\)](#)
- [ルータ生成 Cisco SD-WAN Manager トラフィックの QoS \(123 ページ\)](#)
- [ルータ生成 Cisco SD-WAN Manager トラフィックの QoS について \(123 ページ\)](#)
- [ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の制約事項 \(124 ページ\)](#)
- [CLI テンプレートを使用した、ルータで生成された Cisco SD-WAN Manager トラフィックの QoS の設定 \(124 ページ\)](#)
- [CLI を使用した、ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の確認 \(125 ページ\)](#)
- [ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS のトラブルシューティング \(127 ページ\)](#)

ローカライズ型ポリシーの概要

ローカライズ型ポリシーとは、Cisco IOS XE Catalyst SD-WAN デバイスの CLI または Cisco SD-WAN Manager デバイステンプレートを通じてローカルにプロビジョニングされたポリシーを指します。

ローカライズ型ポリシーのタイプ

ローカライズ型制御ポリシー

制御ポリシーは、Cisco IOS XE Catalyst SD-WAN オーバーレイネットワークのコントロールプレーントラフィックに作用し、オーバーレイネットワークを通過するルーティングパスの決定に影響を及ぼします。ローカライズ型制御ポリシーは、Cisco IOS XE Catalyst SD-WAN デバイスで設定されるポリシーであり（したがって、ローカル）、デバイスが属するサイトローカルネットワークに対する BGP および OSPF ルーティングの決定に影響を及ぼします。

オーバーレイネットワークに参加するだけでなく、Cisco IOS XE Catalyst SD-WAN デバイスはローカルサイトでネットワークに参加したりするため、他のネットワークデバイスからは通常のルータに見えます。そのため、ローカルサイトのルータとルート情報を交換できるように、Cisco IOS XE Catalyst SD-WAN デバイスで BGP や OSPF などのルーティングプロトコルをプロビジョニングできます。ローカルネットワークでルーティング動作を制御および変更するには、デバイスでルートポリシーと呼ばれる制御タイプのポリシーを設定します。ルートポリシーは、ローカルブランチで実行されるルーティングにのみ適用され、ローカルデバイスのルートテーブルのルートテーブルエントリにのみ影響します。

デバイスで設定するローカライズ型制御ポリシーを使用すると、デバイスが配置されているローカルサイトのネットワークのルーティングポリシーに影響を与えることができます。このタイプの制御ポリシーは、ルートポリシーと呼ばれています。このポリシーは、通常のドライバで設定するルーティングポリシーに似ており、サイトとローカル間ネットワークでの BGP および OSPF ルーティング動作を変更できるようにします。一元管理型制御ポリシーはオーバーレイネットワーク全体のルーティング動作に影響しますが、ルートポリシーはローカルブランチのルーティングにのみ適用されます。

ローカライズ型データポリシー

データポリシーは、Cisco IOS XE Catalyst SD-WAN オーバーレイネットワークのデータプレーンに作用し、ネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス間におけるデータトラフィックの送信の仕方に影響を及ぼします。Cisco Catalyst SD-WAN アーキテクチャでは、2つのタイプのデータポリシーを定義します。一元管理型データポリシーという、データパケットの IP ヘッダーフィールドとネットワークセグメンテーションに基づいてデータトラフィックのフローを制御するタイプと、ローカライズ型データポリシーという、インターフェイス間を行き来するデータトラフィックのフローと Cisco IOS XE Catalyst SD-WAN デバイスでのインターフェイスキューを制御するタイプです。

ローカライズ型データポリシーは、ローカルの Cisco IOS XE Catalyst SD-WAN デバイスにプロビジョニングされるのでこう呼ばれていますが、ある決まったルータインターフェイスに適用されるポリシーで、そうしたインターフェイスによって送受信されるデータトラフィックの処理の仕方に影響を及ぼします。ローカライズ型データポリシーは、アクセスリスト (ACL) とも呼ばれます。アクセスリストを使用すると、サービスクラス (CoS) のプロビジョニングや、データパケットの分類、さまざまなクラスの伝送プロパティの優先順位付けを行うことができます。ポリシーを設定して、パケットミラーリングのプロビジョニングもできます。

IPv4 の場合は、QoS アクションの設定が可能です。

ルータ上の任意の VPN に IPv4 アクセスリストを適用できるほか、ユニキャストおよびマルチキャストトラフィックに作用するアクセスリストの作成もできます。IPv6 アクセスリストの場合は、適用できるのがトランスポート VPN (VPN0) のトンネルインターフェイスのみとなります。

アクセスリストの適用は、インターフェイスのアウトバウンドまたはインバウンド方向のいずれかとなります。アウトバウンド方向に IPv4 ACL を適用すると、ローカルサービス側ネットワークから IPsec トンネルを通過してリモートサービス側ネットワークに向かうデータパケットに影響を及ぼします。インバウンド方向に IPv4 ACL を適用すると、IPsec トンネルから出てローカル Cisco IOS XE Catalyst SD-WAN デバイスで受信されるデータパケットに影響を及ぼします。IPv6 の場合は、アウトバウンド ACL がルータによって送信されるトラフィックに適用され、インバウンド ACL は受信トラフィックに適用されます。

明示的なアクセスリストと暗黙的なアクセスリスト

ローカライズ型データポリシーを使用して設定するアクセスリストは、明示的な ACL と呼ばれます。明示的な ACL は、ルータ上の任意の VPN に適用できます。

ルータ トンネルインターフェイスには、サービスとも呼ばれる暗黙的な ACL もあります。これらの一部はデフォルトでトンネルインターフェイスに存在し、無効にしない限り有効です。設定によって、その他の暗黙的な ACL を有効にすることもできます。Cisco IOS XE Catalyst SD-WAN デバイスでは、DHCP (DHCPv4 および DHCPv6 の場合)、DNS、および ICMP の各サービスがデフォルトで有効になっています。BGP、Netconf、NTP、OSPF、SSHD、および STUN のサービスを有効にすることもできます。

QoS アクションの実行

アクセスリストを使用すると、Quality of Service (QoS) をプロビジョニングできます。これにより、データトラフィックを重要度で分類して、複数のインターフェイスキューに分散させ、さまざまなクラスのトラフィックの送信レートを制御できるようになります。「転送と QoS の概要」を参照してください。

データパケットのミラーリング

パケットが分類されたら、アクセスリストを設定して、Cisco vEdge デバイスで検出されたデータパケットの複製を別のネットワークデバイス上の指定された宛先に送信できます。Cisco IOS XE Catalyst SD-WAN デバイスでサポートしているミラーリングは 1 対 1 です。つまり、すべてのパケットの複製は代わりの宛先に送信されます。

Cisco SD-WAN Manager を使用したローカライズ型ポリシーの設定

ローカライズ型ポリシーを設定するには、Cisco SD-WAN Manager のポリシー構成ウィザードを使用します。ウィザードは、次のローカライズ型ポリシーコンポーネントを構成および変更するための5つのウィンドウで構成される UI ポリシービルダーです。

- 対象グループ（リストとも呼ばれます）
- QoS に使用する転送クラス
- アクセス制御リスト（ACL）
- ルートポリシー
- ポリシー設定

作成する特定のポリシーに応じて、これらのコンポーネントの一部またはすべてを構成します。コンポーネントをスキップするには、ウィンドウの下部にある[次へ (Next)]をクリックします。コンポーネントに戻るには、ウィンドウの下部の[戻る (Back)]をクリックします。

Cisco SD-WAN Manager を使用してローカライズ型ポリシーを設定するには、このセクションに続く手順で示すステップを実行します。

ポリシー構成ウィザードの開始

ポリシー構成ウィザードを開始するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Policies]** を選択します。
2. [ローカライズ側ポリシー (Localized Policy)] を選択します。
3. [Add Policy] をクリックします。

[対象グループの作成 (Create Groups of Interest)] ページが表示されます。

ローカライズ型ポリシーの対象グループの構成

[対象グループの作成 (Create Groups of Interest)] で、ローカライズ型ポリシーで使用するグループのリストを作成します。

[対象グループの作成 (Create Groups of Interest)] で、次のセクションの説明に従って、リストタイプの新しいグループを作成し、ローカライズ型ポリシーで使用します。

AS パスの構成

1. [対象グループ (Group of Interest)] リストで、[AS パス (AS Path)] をクリックします。

2. [新しい AS パスリスト (New AS Path List)] をクリックします。
3. リストの名前を入力します。
4. AS パスは、AS 番号をコンマで区切って入力します。
5. [Add] をクリックします。

[AS パス (AS Path)] リストには、1 つ以上の BGP AS パスを指定します。各 AS は、単一の数値または正規表現として記述できます。1 つのパスに複数の AS を指定するには、コンマで区切ってリストに含めます。1 つのリストに複数の AS パスを構成するには、複数の **as-path** オプションを含め、各オプションに 1 つの AS パスを指定します。

コミュニティの設定

コミュニティリストは、ルートマップの **match** 句で使用するコミュニティのグループ作成に使用されるリストです。コミュニティリストは、ルートの受け入れ、優先、配布、またはアドバタイズの制御に使用できます。また、コミュニティリストは、ルートのコミュニティの設定、追加または変更にも使用できます。

1. [対象グループ (Group of Interest)] リストで、[コミュニティ (Community)] をクリックします。
2. [新しいコミュニティリスト (New Community List)] をクリックします。
3. コミュニティリストの名前を入力します。
4. [コミュニティの追加 (Add Community)] フィールドに、次のいずれかの形式で、1 つ以上のデータプレフィックスをコンマで区切って入力します。
 - **aa:nn** : 自律システム (AS) 番号とネットワーク番号。各番号は、1 ~ 65535 の範囲の 2 バイト値です。
 - **internet** : このコミュニティのルートはインターネットコミュニティにアドバタイズされます。このコミュニティは、すべての BGP 対応ネットワークングデバイスで構成されます。
 - **local-as** : このコミュニティのルートはローカル AS 番号の外にはアドバタイズされません。
 - **no-advertise** : NO_ADVERTISE コミュニティをルートにアタッチします。このコミュニティのルートは他の BGP ピアにはアドバタイズされません。
 - **no-export** : NO_EXPORT コミュニティをルートにアタッチします。このコミュニティのルートは、ローカル AS や BGP コンフェデレーション境界の外にアドバタイズされません。1 つのリストに複数の BGP コミュニティを設定するには、複数の **community** オプションを含め、各オプションに 1 つのコミュニティを指定します。
5. [Add] をクリックします。

データプレフィックスの設定

1. [対象グループ (Group of Interest)] リストで、[データプレフィックス (Data Prefix)] をクリックします。
2. [新しいデータプレフィックスリスト (New Data Prefix List)] をクリックします。
3. リストの名前を入力します。
4. 1つ以上の IP プレフィックスを入力します。
5. [Add] をクリックします。

データプレフィックスリストには、1つ以上の IP プレフィックスを指定します。ユニキャストアドレスとマルチキャストアドレスの両方を指定できます。1つのリストに複数のプレフィックスを構成するには、複数の **ip-prefix** オプションを含め、各オプションに1つのプレフィックスを指定します。

拡張コミュニティの構成

1. [対象グループ (Group of Interest)] リストで、[拡張コミュニティ (Extended Community)] をクリックします。
2. [新しい拡張コミュニティリスト (New Extended Community List)] をクリックします。
3. リストの名前を入力します。
4. 次の形式で BGP 拡張コミュニティを入力します。
 - [rt] (aa:nn | ip-address) : ルートターゲットコミュニティ。BGP によって運ばれる一連のルートを受信できる1つ以上のルータです。AS 番号とネットワーク番号を1～65535の2バイトの数値、またはIPアドレスで指定します。
 - [soo] (aa:nn | ip-address) : ルートオリジンコミュニティ。一連のルートをBGPに挿入できる1つ以上のルータです。AS 番号とネットワーク番号を1～65535の2バイトの数値、またはIPアドレスで指定します。1つのリストに複数の拡張 BGP コミュニティを設定するには、複数の [community] オプションを含め、各オプションに1つのコミュニティを指定します。
5. [Add] をクリックします。

クラスマップの設定

1. [対象グループ (Group of Interest)] リストで、[クラスマップ (Class Map)] をクリックします。
2. [新しいクラスリスト (New Class List)] をクリックします。
3. クラスの名前を入力します。
4. [キュー (Queue)] ドロップダウンリストから必要なキューを選択します。

5. [Save] をクリックします。

ミラーの設定

1. [対象グループ (Group of Interest)] リストで、[ミラー (Mirror)] をクリックします。
2. [新しいミラーリスト (New Mirror List)] をクリックします。[ミラーリスト (Mirror List)] ポップアップが表示されます。
3. リストの名前を入力します。
4. [Remote Destination IP] フィールドには、パケットをミラーリングする宛先の IP アドレスを入力します。
5. [Source IP] フィールドには、ミラーリングするパケットの送信元 IP アドレスを入力します。
6. [Add] をクリックします。

ミラーリングパラメータを設定するには、パケットのミラーリング先のリモート接続先を定義し、パケットの送信元を定義します。ミラーリングはユニキャストトラフィックにのみ適用されます。マルチキャストトラフィックには適用されません。

ポリサーの構成

1. [対象グループ (Group of Interest)] リストで、[ポリサー (Policer)] をクリックします。
2. [新しいポリサーリスト (New Policer List)] をクリックします。
3. リストの名前を入力します。
4. [バースト(bps) (Burst(bps))] フィールドに、最大トラフィックバーストサイズを入力します。15,000 ~ 10,000,000 バイトの値を指定できます。
5. [超過 (Exceed)] フィールドで、バーストサイズまたはトラフィックレートを超えたときに実行するアクションを選択します。[ドロップ (Drop)] (デフォルト) を選択して、[パケット損失の優先順位 (PLP) (Packet Loss Priority (PLP))] を [低 (Low)] に設定します。[注釈 (Remark)] を選択して、PLP を [高 (High)] に設定します。
6. [レート(bps) (Rate(bps))] フィールドに、最大トラフィックレートを入力します。8 ~ 2⁶⁴ bps (8 ~ 100,000,000,000) の値にすることができます。
7. [Add] をクリックします。

プレフィックスの構成

1. [対象グループ (group of interest)] リストで、[プレフィックス (Prefix)] をクリックします。
2. [新しいプレフィックスリスト (New Prefix List)] をクリックします。
3. リストの名前を入力します。

4. [インターネットプロトコル (Internet Protocol)] フィールドで、[IPv4] または [IPv6] をクリックします。
5. [Add Prefix] で、リストのプレフィックスを入力します。(例を表示します。) 必要に応じて、右側にある緑色の [インポート (Import)] リンクをクリックして、プレフィックスリストをインポートします。
6. [Add] をクリックします。

[次へ (Next)] をクリックして、ウィザードの [転送クラス/QoSの設定 (Configure Forwarding Classes/QoS)] に移動します。

転送クラス/QoSの設定

[転送クラス/QoS (Forwarding Classes/QoS)] ページを初めて開くと、デフォルトで [QoSマップ (QoS Map)] が選択されています。

QoS マップ (QoS Map)

新しい QoS マッピングを作成するには、次の手順を実行します。

1. [QoS] で、[QoSマップの追加 (Add QoS Map)] ドロップダウンリストをクリックします。
2. [新規作成 (Create New)] を選択します。
3. QoS マッピングの名前と説明を入力します。
4. [キューの追加 (Add Queue)] をクリックします。[キューの追加 (Add Queue)] ポップアップが表示されます。
5. [キュー (Queue)] ドロップダウンリストからキュー番号を選択します。
6. 最大帯域幅とバッファの割合、およびスケジューリングとドロップタイプを選択します。
7. [転送クラス (Forwarding Class)] を入力します。
8. [キューを保存 (Save Queue)] をクリックします。

既存の QoS マッピングをインポートするには、次の手順を実行します。

1. [QoS] で、[QoSマップの追加 (Add QoS Map)] ドロップダウンリストをクリックします。
2. [既存をインポート (Import Existing)] を選択します。[既存のアプリケーションQoSマップポリシーのインポート (Import Existing Application QoS Map Policy)] ポップアップが表示されます。
3. [QoSマップ (QoS Map)] ポリシーを選択します。
4. [Import] をクリックします。

QoS マッピングを表示またはコピーするか、ローカライズ型ポリシーからマッピングを削除するには、[...] をクリックして、目的のアクションを選択します。

ハードウェアの場合、各インターフェイスには0～7の番号が付けられた8つのキューがあります。キュー0は低遅延キューイング（LLQ）用に予約されているため、キュー0にマップされるクラスはすべてLLQを使用するように構成する必要があります。すべてのデフォルトのスケジューリング方式は、加重ラウンドロビン（WRR）です。

Cisco IOS XE Catalyst SD-WAN デバイス の場合、各インターフェイスには0～7の番号が付けられた8つのキューがあります。キュー0は制御トラフィック用に予約されており、キュー1、2、3、4、5、6、7はデータトラフィック用に使用できます。8つのキューすべてのスケジューリング方式はWRRです。LLQはサポートされていません。

Cisco IOS XE Catalyst SD-WAN デバイス で QoS パラメータを設定するには、QoS スケジューリングとシェーピングを有効にする必要があります。Cisco IOS XE Catalyst SD-WAN デバイスがトランスポート側インターフェイスから受信するトラフィックの QoS パラメータを有効にするには、次の手順を実行します。

Cisco IOS XE Catalyst SD-WAN デバイス がサービス側インターフェイスから受信するトラフィックの QoS パラメータを有効にするには、次の手順を実行します。

ポリシーの書き換え

QoS マッピングのポリシー書き換えルールを構成するには、次の手順を実行します。

1. [ポリシーの書き換え（Policy Rewrite）]で、[書き換えポリシーの追加（Add Rewrite Policy）] ドロップダウンリストをクリックします。
2. [新規作成（Create New）]を選択します。
3. 書き換えルールの名前と説明を入力します。
4. [書き換えルールの追加（Add Rewrite Rule）]をクリックします。[ルールの追加（Add Rule）]ポップアップが表示されます。
5. [クラス（Class）]ドロップダウンからクラスを選択します。
6. [優先順位（Priority）]ドロップダウンから優先順位（[低（Low）]または[高（High）]）を選択します。
[低（Low）]の優先順位はCisco IOS XE Catalyst SD-WAN デバイス でのみサポートされません。
7. [DSCP]フィールドにDSCP値（0～63）を入力します。
8. [レイヤ2サービスクラス（Layer 2 Class of Service）]フィールドに、サービスクラス（CoS）の値（0～7）を入力します。
9. [Save Rule]をクリックします。

既存の書き換えルールをインポートするには、次の手順を実行します。

1. [QoS]で、[書き換えポリシーの追加（Add Rewrite Policy）]ドロップダウンをクリックします。

2. [既存をインポート (Import Existing)] を選択します。[既存のポリシー書き換えのインポート (Import Existing Policy Rewrite)] ポップアップが表示されます。
3. 書き換えルールポリシーを選択します。
4. [Import] をクリックします。

[次へ (Next)] をクリックして、[アクセスリストの設定 (Configure Access Lists)] ページに移動します。

ACL の設定

1. [アクセス制御リストの設定 (Configure Access Control Lists)] ページで、ACL を設定します。
2. 新しいアクセス制御リスト (ACL) を作成するには、[アクセス制御リストポリシーの追加 (Add Access Control List Policy)] ドロップダウンリストをクリックします。次のオプションのいずれかを選択します。
 - **IPv4 ACL ポリシーの追加 (Add IPv4 ACL Policy)** : IPv4 ACL ポリシーを設定します。
 - **IPv6 ACL ポリシーの追加 (Add IPv6 ACL Policy)** : IPv6 ACL ポリシーを設定します。
 - **既存のインポート (Import Existing)** : 既存の ACL ポリシーをインポートします。
3. [IPv4 ACL ポリシーの追加 (Add IPv4 ACL Policy)] をクリックすると、[IPv4 ACL ポリシーの追加 (Add IPv4 ACL Policy)] ページが表示されます。
または
[IPv6 ACL ポリシーの追加 (Add IPv6 ACL Policy)] をクリックすると、[IPv6 ACL ポリシーの追加 (Add IPv6 ACL Policy)] ページが表示されます。
4. [ACL ポリシー (ACL Policy)] ページで、ACL の名前と説明を入力します。
5. 左側のペインで、[ACL シーケンスの追加 (Add ACL Sequence)] をクリックします。左側のペインに [アクセス制御リスト (Access Control List)] ボックスが表示されます。
6. [アクセス制御リスト (Access Control List)] ボックスをダブルクリックし、ACL の名前を入力します。
7. 右側のペインで、[シーケンスルールの追加 (Add Sequence Rule)] をクリックして、ACL に単一のシーケンスを作成します。デフォルトでは [マッチ (Match)] が選択されています。
8. マッチ条件をクリックします。
9. 左側に、マッチ条件の値を入力します。
 1. 右側に、ポリシーが一致した場合に実行するアクションを入力します。

10. ステップ 6～8 を繰り返して、ACL にマッチ/アクションペアを追加します。
11. ACL のマッチ/アクションペアを並び替えるには、右側のペインでそれらを目的の位置にドラッグします。
12. ACL からマッチ/アクションペアを削除するには、条件の右上にある **[X]** をクリックします。
13. [マッチとアクションの保存 (Save Match and Actions)] をクリックして、シーケンスルールを保存します。
14. ACL のシーケンスルールを並び替えるには、左側のペインでルールを目的の位置にドラッグします。
15. ACL のシーケンスルールをコピー、削除、または名前変更するには、左側のペインで、ルール名の横にある **[...]** をクリックし、目的のオプションを選択します。

Default Action

評価されるパケットがアクセスリストのマッチ条件のいずれにも一致しない場合、デフォルトアクションがこのパケットに適用されます。デフォルトでは、パケットはドロップされます。デフォルトのアクションを変更するには、次の手順を実行します。

1. 左側のペインで [Default Action] をクリックします。
2. [鉛筆 (Pencil)] アイコンをクリックします。
3. デフォルトのアクションを [Accept] に変更します。
4. [Save Match and Actions] をクリックします。
5. [アクセス制御リストポリシーの保存 (Save Access Control List Policy)] をクリックします。

デバイスアクセスポリシーを設定するには、[デバイスアクセスポリシー](#)を参照してください。

[次へ (Next)] をクリックして、[ルートポリシーの設定 (Route Policy page)] ページに移動します。

明示的なアクセスリストと暗黙的なアクセスリスト

ローカライズ型データポリシーを介して **policy access-list** コマンドを使用して設定するアクセスリストは、明示的な ACL と呼ばれます。明示的な ACL は、デバイス上の任意の VPN の、どのインターフェイスにも適用できます。

VPN 0 のデバイスのトンネルインターフェイスには、サービスとも呼ばれる暗黙的な ACL もあります。一部のサービスはトンネルインターフェイスでデフォルトで有効化されており、無効にしない限り有効のままです。設定で、他のサービスを有効にすることもできます。

allow-service コマンドで、暗黙的な ACL を設定および変更します。

```
Device(config)# vpn 0
Device(config-vpn)# interface interface-name
Device(config-interface)# tunnel-interface
```

```
Device(config-tunnel-interface)# allow-service service-name
Device(config-tunnel-interface)# no allow-service service-name
```

Cisco IOS XE Catalyst SD-WAN デバイスでは、DHCP（DHCPv4 および DHCPv6 の場合）、DNS、および ICMP の各サービスがデフォルトで有効になっています。これら 3 つのサービスにより、トンネルインターフェイスは DHCP、DNS、および ICMP パケットを受け入れることができます。BGP、Netconf、NTP、OSPF、SSHD、および STUN のサービスを有効にすることもできます。



(注) 接続がデバイスから開始され、デバイスで NAT が有効になっている場合（たとえば、ダイレクトインターネットアクセス（DIA）が設定されている場合）、暗黙的な ACL が **no allow-service** として設定されていても、リターントラフィックは NAT エントリによって許可されます。この場合も、明示的な ACL でこのトラフィックをブロックできます。

明示的な ACL と Cisco IOS XE ACL を混同しないようにしてください。Cisco IOS XE ACL は、Cisco Catalyst SD-WAN の明示的および暗黙的 ACL と双方向でやり取りせず、暗黙的 ACL または明示的 ACL を上書きできません。Cisco IOS XE ACL は、トラフィック処理操作の順序において、後で実行されます。

データトラフィックが明示的 ACL と暗黙的 ACL の両方に一致する場合、パケットの処理方法は ACL の設定によって異なります。具体的には、以下に応じて決定されます。

- 暗黙的 ACL が許可 (**allow-service service-name**) または拒否 (**no allow-service service-name**) として設定されているかどうか。暗黙的 ACL でサービスを許可することは、明示的 ACL で許可アクションを指定することと同じであり、暗黙的 ACL でサービスを許可しないことは、明示的 ACL でドロップアクションを指定することと同じです。
- 明示的 ACL で、許可アクションまたは拒否アクションがポリシーシーケンスで設定されているか、デフォルトアクションで設定されているか。

次の表に、暗黙的 ACL と明示的 ACL の両方に一致するトラフィックの処理方法を示します。

表 16:

暗黙的 ACL	明示的 ACL : シーケンス	明示的 ACL : デフォルト	結果
許可 (承認)	拒否 (ドロップ)	—	拒否 (ドロップ)
許可 (承認)	—	拒否 (ドロップ)	許可 (承認)
拒否 (ドロップ)	許可 (承認)	—	許可 (承認)
拒否 (ドロップ)	—	許可 (承認)	拒否 (ドロップ)

ルートポリシーの設定

[ルートポリシーの設定 (Configure Route Policies)] で、ルーティングポリシーを設定します。

1. [ルートポリシーの追加 (Add Route Policy)] で、[新規作成 (Create New)] を選択します。
2. ルートポリシーの名前と説明を入力します。
3. 左側のペインで、[シーケンスタイプの追加 (Add Sequence Type)] をクリックします。左側のペインに [ルート (Route)] ボックスが表示されます。
4. [ルート (Route)] ボックスをダブルクリックし、ルートポリシーの名前を入力します。
5. 右側のペインで、[シーケンスルールの追加 (Add Sequence Rule)] をクリックして、ポリシーに単一のシーケンスを作成します。デフォルトでは [マッチ (Match)] が選択されています。
6. [Protocol] ドロップダウンリストから目的のプロトコルを選択します。オプションは、[IPv4]、[IPv6]、またはその両方です。
7. マッチ条件をクリックします。
8. 左側に、マッチ条件の値を入力します。
9. 右側に、ポリシーが一致した場合に実行するアクションを入力します。
10. ステップ 6 ~ 8 を繰り返して、ルートポリシーにマッチ/アクションのペアを追加します。
11. ルートポリシーのマッチ/アクションのペアを並び替えるには、右側のペインでペアを目的の位置にドラッグします。
12. ルートポリシーからマッチ/アクションのペアを削除するには、条件の右上にある [X] をクリックします。
13. [マッチとアクションの保存 (Save Match and Actions)] をクリックして、シーケンスルールを保存します。
14. ルートポリシーのシーケンスルールを並び替えるには、左側のペインでルールを目的の位置にドラッグします。
15. ルートポリシーシーケンスルールをコピー、削除、または名前変更するには、左側のペインでルール名の横にある [...] をクリックし、目的のオプションを選択します。
16. どのルートポリシーシーケンスルールにも一致するパッケージがない場合、デフォルトのアクションはパッケージをドロップすることです。デフォルトのアクションを変更するには、次の手順を実行します。
 1. 左側のペインで [Default Action] をクリックします。
 2. 鉛筆アイコンをクリックします。
 3. デフォルトのアクションを [Accept] に変更します。

4. [Save Match and Actions] をクリックします。
17. [Save Route Policy] をクリックします。
18. [次へ (Next)] をクリックして、[ポリシーの概要 (Policy Overview)] ページに移動します。

match パラメータ

アクセスリストパラメータ

アクセスリストがあれば、IPヘッダーのIPプレフィックスおよびフィールドを照合できます。CLI では、**policy access-list sequence match** コマンドを使用してマッチパラメータを設定します。

access-list の各シーケンスには、マッチ条件が1つ含まれている必要があります。

ACLのマッチクラスはサポートされません。書き換えポリシーを使用すればDSCP値を設定できます。

アクセスリストの場合、次のパラメータを照合できます。

一致条件	説明
Class	policy class-map コマンドで定義されたクラスの名前。
Destination Data Prefix	data-prefix-list リストの名前。
宛先ポート	単一のポート番号、ポート番号のリスト（スペースで区切られた番号）、またはポート番号の範囲（ハイフン[-]で区切られた2つの番号）を指定します。範囲は0～65535です。
[DSCP]	DSCP 値を指定します。範囲は 0 ～ 63 です。
Protocol	インターネットプロトコル番号を指定します。範囲は 0 ～ 255 です。
ICMP Message	<p>[プロトコル (Protocol)] 値を 1 にすると、[ICMP メッセージ (ICMP Message)] フィールドが表示され、データポリシーに適用する ICMP メッセージを選択できます。</p> <p>[次ヘッダー (Next Header)] の値を 58 にすると、[ICMP メッセージ (ICMP Message)] フィールドが表示され、データポリシーに適用する ICMP メッセージを選択できます。</p> <p>(注) このフィールドは、Cisco IOS XE リリース 17.4.1、Cisco vManage リリース 20.4.1 以降で使用できます。</p> <p>icmp-msg および icmp6-msg メッセージタイプについては、一元管理型の章にある「ICMP メッセージタイプ/コードと対応する列挙値」の表を参照してください。</p>

一致条件	説明
パケット長 (Packet Length)	パケットの長さを指定します。指定できる範囲は 0 ~ 65535 です。単一の長さ、長さのリスト (スペースで区切られた番号)、または長さの範囲 (ハイフン[-]で区切られた2つの番号) を指定します。
Source Data Prefix	data-prefix-list リストの名前を指定します。
PLP	パケット損失プライオリティ (PLP) ([高 (high)] [低 (low)]) を指定します。デフォルトでは、パケットの PLP 値は [低 (low)] です。PLP 値を [高 (high)] に設定するには、 注釈超過 オプションのあるポリサーを適用します。
送信元ポート	単一のポート番号、ポート番号のリスト (スペースで区切られた番号)、またはポート番号の範囲 (ハイフン[-]で区切られた2つの番号) を指定します。範囲は 0~65535 です。
[TCP]	syn

ルートポリシーパラメータ

ルートポリシーの場合、次のパラメータを照合できます。

一致条件	説明
アドレス	Prefix-List リストの名前を指定します。
AS パスリスト	1つ以上の BGP AS パスリストを指定します。各 AS は、単一の数値または正規表現として記述できます。1つのパスに複数の AS 番号を指定するには、引用符 (" ") でくくってリストに含めます。1つのリストに複数の AS パスを設定するには、複数の AS パス オプションを含め、オプションごとに1つの AS パスを指定します。

一致条件	説明
コミュニティ リスト	<p>1つ以上の BGP コミュニティのリスト。[コミュニティリスト (CommunityList)]では、次の項目を指定できます。</p> <ul style="list-style-type: none"> • aa:nn : AS 番号とネットワーク番号。各番号は、1 ~ 65535 の範囲の 2 バイト値です。 • internet : このコミュニティのルートはインターネットコミュニティにアドバタイズされます。このコミュニティは、すべての BGP 対応ネットワークデバイスで構成されます。 • local-as : このコミュニティのルートは、ローカル AS 番号以外ではアドバタイズされません。 • no-advertise : NO_ADVERTISE コミュニティをルートにアタッチします。このコミュニティのルートは他の BGP ピアにはアドバタイズされません。 • no-export : NO_EXPORT コミュニティをルートにアタッチします。このコミュニティのルートは、ローカル AS や BGP コンフェデレーション境界の外にアドバタイズされません。1つのリストに複数の BGP コミュニティを設定するには、複数の community オプションを含め、各オプションに1つのコミュニティを指定します。
拡張コミュニティリスト	<p>1つ以上の BGP 拡張コミュニティのリストを指定します。[コミュニティ (community)]では、次の項目を指定できます。</p> <ul style="list-style-type: none"> • [rt] (aa:nn ip-address) : ルートターゲット コミュニティ。BGP によって運ばれる一連のルートを受信できる 1つ以上のルータです。AS 番号とネットワーク番号を 1 ~ 65535 の 2 バイトの数値、または IP アドレスで指定します。 • [soo] (aa:nn ip-address) : ルートオリジンコミュニティ。一連のルートを BGP に挿入できる 1つ以上のルータです。AS 番号とネットワーク番号を 1 ~ 65535 の 2 バイトの数値、または IP アドレスで指定します。1つのリストに複数の拡張 BGP コミュニティを設定するには、複数の [community] オプションを含め、各オプションに1つのコミュニティを指定します。
BGP ローカル プリファレンス	BGP ローカルプリファレンス番号を指定します。範囲は 0 ~ 4294967295 です。
[メトリック (Metric)]	ルートメトリック値を指定します。範囲は 0 ~ 4294967295 です。
Next Hop	IP プレフィックスリストの名前を指定します。
OMP タグ	OMP タグ番号を指定します。範囲は 0 ~ 4294967295 です。
Origin	BGP 送信元コードを指定します。オプションは、EGP (デフォルト) 、IGP、Incomplete です。
OSPF タグ	OSPF タグ番号を指定します。範囲は 0 ~ 4294967295 です。
Peer	ピア IP アドレスを指定します。

アクションパラメータ

アクセスリストパラメータ

パケットがアクセスリストの一致部分の条件に一致すると、そのパケットを受け入れ、ドロップ、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を分類、ミラーリング、またはポリシングできます。

CLI では、**policy access-list sequence action** コマンドによってアクションパラメータを設定します。

アクセスリスト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。

アクション条件	説明
承認	パケットを受け入れます。受け入れられたパケットは、アクセスリストの アクション 部分に設定された追加パラメータによって変更できます。
カウンタ	カウンタの名前。カウンタ情報を表示するには、Cisco IOS XE Catalyst SD-WAN デバイスで show policy access-lists counters コマンドを使用します。
削除 (Drop)	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。

受け入れられたパケットに対して、次のアクションを設定できます。

説明	値または範囲
Class	QoS クラスの名前を指定します。 policy class-map コマンドを使用して定義することもできます。
Mirror List	ミラーの名前を指定します。これは policy mirror コマンドで定義されます。
Policer	policy policer コマンドで定義されたポリサーの名前を指定します。
[DSCP]	パケットの DSCP 値を指定します。範囲は 0 ~ 63 です。
Next Hop	IPv4 アドレスを指定します。パケットの転送先となるネクストホップ IP アドレスを設定します。 (注) Cisco vManage リリース 20.5.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降では、[ネクストホップが使用できない場合にデフォルトルートを使用 (Use Default Route when Next Hop is not available)] フィールドが [ネクストホップアクション (Next Hop action)] パラメータの横に表示されません。

ルートポリシーパラメータ

ローカライズ型制御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。

ルートがルートポリシーの一致部分の条件に一致する場合、そのルートは許可または拒否されます。

受け入れられたパケットに対して、次のアクションを設定できます。

説明	値または範囲
アグリゲータ	BGP ルートアグリゲータが配置されている AS 番号とルートアグリゲータの IP アドレスを設定します。指定できる範囲は 1 ～ 65535 です。
AS パス	AS パスから除外する、または AS パスの先頭に付加する、AS 番号または一連の AS 番号を設定します。指定できる範囲は 1 ～ 65535 です。
アトミック集約	BGP アトミック集約属性を設定します。
Community	BGP コミュニティ値を設定します。 Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a以降では、[追加コミュニティ (Community Additive)] オプションフィールドを使用できます。追加オプションは、ルートの既存のコミュニティにコミュニティを追加します。
ローカルプリファレンス	BGP ローカルプリファレンスを設定します。範囲は 0 ～ 4294967295 です。
[メトリック (Metric)]	メトリック値を設定します。範囲は 0 ～ 4294967295 です。
Metric Type	メトリックタイプを設定します。オプションは、type1 または type2 です。
Next Hop	IPv4 アドレスを設定します。パケットの転送先となるネクストホップ IP アドレスを設定します。 (注) Cisco vManage リリース 20.5.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a以降では、[ネクストホップが使用できない場合にデフォルトルートを使用 (Use Default Route when Next Hop is not available)] フィールドが [ネクストホップアクション (Next Hop action)] パラメータの横に表示されます。
OMP タグ	使用する OSPF の OMP タグを設定します。範囲は 0 ～ 4294967295 です。
Origin	BGP 送信元コードを設定します。オプションは、EGP (デフォルト)、IGP、Incomplete です。
発信元 (Originator)	ルートが学習された IP アドレスを設定します。
OSPF タグ	OSPF タグ値を設定します。範囲は 0 ～ 4294967295 です。
重量	BGP の重量を設定します。範囲は 0 ～ 4294967295 です。

ポリシー設定の構成

[ポリシーの概要 (Policy Overview)] で、ポリシーを設定します。

1. [ローカライズ型マスターポリシーの名前と説明の入力 (Enter name and description for your localized master policy)] ペインで、ポリシーの名前と説明を入力します。
2. [ポリシー設定 (Policy Settings)] ペインで、設定するポリシーの適用チェックボックスをオンにします。次のオプションがあります。
 - [Netflow] : IPv4 トラフィックのトラフィック フロー モニリングを実行します。
 - [Netflow IPv6] : IPv6 トラフィックのトラフィック フロー モニタリングを実行します。
 - [アプリケーション (Application)] : IPv4 アプリケーションを追跡して監視します。
 - [アプリケーション IPv6 (Application IPv6)] : IPv6 アプリケーションを追跡して監視します。
 - [クラウド QoS (Cloud QoS)] : QoS スケジューリングを有効にします。
 - [クラウド QoS サービス側 (Cloud QoS Service Side)] : サービス側で QoS スケジューリングを有効にします。
 - [暗黙的な ACL ロギング (Implicit ACL Logging)] : トラフィック フロー モニタリングを実行するサービスとマッチしないためにドロップされたすべてのパケットのヘッダーをログに記録します。
3. パケットフローのログ記録の頻度を設定するには、[ログ頻度 (Log Frequency)] をクリックします。

パケットフローとは、アクセスリスト (ACL)、cflowd フロー、またはアプリケーション認識型ルーティングフローにマッチするもののことです。
4. [プレビュー (Preview)] をクリックして、CLI 形式でポリシー全体を表示します。
5. [Save Policy] をクリックします。

デバイステンプレートへのローカライズ型データポリシーの適用

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Templates] の順に選択します。
2. 新しいデバイステンプレートを作成する場合、次の手順を実行します。
 1. [Device Template] をクリックします。



(注) Cisco vManage リリース 20.7.1 以前のリリースでは、[デバイステンプレート (Device Templates)] は [デバイス (Device)] と呼ばれています。

2. [テンプレートの作成 (Create Template)] ドロップダウンから、[機能テンプレートから (From Feature Template)] を選択します。
 3. [デバイスモデル (Device Model)] ドロップダウンから、Cisco IOS XE Catalyst SD-WAN デバイスの 1 つを選択します。
 4. [TemplateName] フィールドに、デバイステンプレートの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0～9 の数字、ハイフン (-)、下線 (_) のみです。スペースやその他の文字を含めることはできません。
 5. [Description] フィールドにデバイステンプレートの説明を入力します。このフィールドは必須であり、任意の文字とスペースを含めることができます。
 6. ステップ 4 に進みます。
3. 既存のデバイステンプレートを編集する場合は、次の手順を実行します。
 1. [デバイステンプレート (Device Templates)] をクリックし、目的のテンプレートを見つけたら、[...] をクリックして [編集 (Edit)] を選択します。



(注) Cisco vManage リリース 20.7.1 以前のリリースでは、[デバイステンプレート (Device Templates)] は [デバイス (Device)] と呼ばれています。

2. [Additional Templates] をクリックします。画面をスクロールして、[追加のテンプレート (Additional Templates)] セクションまで行きます。
3. [ポリシー (Policy)] ドロップダウンから、設定したポリシーの名前を選択します。
4. [説明 (Description)] フィールドのすぐ下にある [追加テンプレート (Additional Templates)] をクリックします。画面をスクロールして、[追加のテンプレート (Additional Templates)] セクションまで行きます。
5. [ポリシー (Policy)] ドロップダウンから、設定したポリシーの名前を選択します。
6. [作成 (Create)] (新しいテンプレートの場合) または [更新 (Update)] (既存のテンプレートの場合) をクリックします。

ローカライズ型ポリシーのアクティブ化

1. [ローカライズ型ポリシー (Localized Policy)] をクリックして、ポリシーを選択します。
2. 目的のポリシーについて、[...] をクリックし、[アクティブ化 (Activate)] を選択します。
3. [ポリシーのアクティブ化 (Activate Policy)] ポップアップで、[アクティブ化 (Activate)] をクリックして、ネットワーク内の到達可能なすべての Cisco SD-WAN コントローラにポリシーをプッシュします。

4. **[OK]** をクリックして、すべての Cisco SD-WAN コントローラ でポリシーのアクティブ化を確認します。
5. ローカライズ型ポリシーを非アクティブにするには、**[=]** を選択し、ポリシーを選択します。
6. 目的のポリシーについて、**[...]** をクリックし、**[非アクティブ化 (Deactivate)]** を選択します。
7. **[ポリシーの非アクティブ化 (Deactivate Policy)]** ポップアップで、**[非アクティブ化 (Deactivate)]** をクリックして、到達可能なすべての Cisco SD-WAN コントローラ からポリシーを削除することを確認します。

ローカライズ型ポリシーの表示

ローカライズ型ポリシーを表示するには、次の手順を実行します。

1. **[ローカライズ型ポリシー (Localized Policy)]** をクリックして、ポリシーを選択します。
2. UI ポリシービルダーまたは CLI を使用して作成されたポリシーの場合は、**[...]** をクリックし、**[表示 (View)]** を選択します。UI ポリシービルダーを使用して作成されたポリシーはグラフィカル形式で表示され、CLI メソッドを使用して作成されたポリシーはテキスト形式で表示されます。
3. Cisco SD-WAN Manager ポリシー構成ウィザードを使用して作成されたポリシーの場合は、**[...]** をクリックし、**[プレビュー (Preview)]** を選択します。このポリシーはテキスト形式で表示されます。

ポリシーのコピー、編集、削除

ポリシーをコピーするには、次の手順を実行します。

1. **[ローカライズ型ポリシー (Localized Policy)]** をクリックして、ポリシーを選択します。
2. 目的のポリシーについて、**[...]** をクリックし、**[コピー (Copy)]** を選択します。
3. **[ポリシーのコピー (Policy Copy)]** ポップアップウィンドウで、ポリシー名とポリシーの説明を入力します。



(注) Cisco IOS XE リリース 17.2 以降では、次のポリシータイプのポリシー名に 127 文字がサポートされています。

- 中央ルートポリシー
- ローカルルートポリシー
- ローカルアクセス制御リスト (ACL)
- ローカル IPv6 ACL
- 中央データポリシー
- 中央アプリケーション ルート ポリシー
- QoS マップ
- 書き換えルール

他のすべてのポリシー名は 32 文字をサポートします。

4. [コピー (Copy)] をクリックします。

Cisco SD-WAN Manager ポリシー構成ウィザードで作成したポリシーを編集するには、次の手順を実行します。

1. 目的のポリシーについて、[...] をクリックし、[編集 (Edit)] を選択します。
2. 必要に応じて、ポリシーを編集します。
3. [ポリシーの変更の保存 (Save Policy Changes)] をクリックします。

CLI 方式で作成されたポリシーを編集するには、次の手順を実行します。

1. [カスタムオプション (Custom Options)] ドロップダウンの [ローカライズ型ポリシー (Localized Policy)] で [CLI ポリシー (CLI Policy)] を選択します。
2. 目的のポリシーについて、[...] をクリックし、[編集 (Edit)] を選択します。
3. 必要に応じて、ポリシーを編集します。
4. [Update] をクリックします。

ポリシーを削除するには、次の手順を実行します。

1. [ローカライズ型ポリシー (Localized Policy)] をクリックして、ポリシーを選択します。
2. 目的のポリシーについて、[...] をクリックし、[削除 (Delete)] を選択します。
3. [OK] をクリックして、ポリシーの削除を確認します。

CLI を使用した、IPv4 に対するローカライズ型ポリシーの設定

Cisco IOS XE Catalyst SD-WAN デバイス で CLI を使用してアクセスリストを設定する手順の概要を次に示します。

1. 必要に応じて、IP プレフィックスのリストを作成します。

```
デバイス(config)# policy lists data-prefix-list ipv4_prefix_list
デバイス(config-data-prefix-list-ipv4_prefix_list)
# ip-prefix 192.168.0.3/24
```

2. QoS の場合は、**class-map ios** を設定します。

```
デバイス(config)# class-map match-any class1
デバイス(config)# match qos-group 1
class-map match-any class6
match qos-group 6
class-map match-any class7
match qos-group 7
class-map match-any class4
match qos-group 4
class-map match-any class5
match qos-group 5
class-map match-any class2
match qos-group 2
class-map match-any class3
match qos-group 3
class-map match-any class1
match qos-group 1
end
```



(注) ここでは **class-default** を使用しているため、**queue2** はオプションです。

3. QoS の場合は、必要に応じて、パケットの外部 IP ヘッダーの DSCP フィールドを上書きする書き換えルールを定義します。

```
デバイス(config)# policy rewrite-rule rule1
デバイス(config-rewrite-rule-rule1)# class class1 low dscp 3
デバイス(config-rewrite-rule-rule1)# class class2 high dscp 4
Will be a table to map class-id → QoS-Group, QID, DSCP, Discard-Class
```

4. QoS の場合、各転送クラスを出力キューにマッピングし、各転送クラスの QoS スケジューラを設定して、QoS スケジューラを QoS マップにグループ化します。

```
デバイス(config)# policy class-map class class1 queue 1
<0..7>[1]
```

5. QoS マップ設定の場合、シェーピングが設定されている場合は、インターフェイスシェーピング設定とマージします。

シェーピングが設定されていない場合は、**qos-map** に対して生成された **policy-map** を適用できます。

```
デバイス(config)# policy-map qos_map_for_data_policy
<name:string
デバイス(config-pmap)# class class1 name:string
デバイス(config-pmap-c)# bandwidth percentage
デバイス(config-pmap-c)# random-detect
```

6. シェーピング設定なしで WAN インターフェイスを設定します。

```
デバイス(config)# policy-map qos_map_for_data_policy name:string
デバイス(config-pmap)# class class1 name:string
デバイス(config-pmap-c)# bandwidth percentage
デバイス(config-pmap-c)# random-detect
```

7. シェーピング設定を使用して WAN インターフェイスを設定します。

```
デバイス(config)# policy-map shaping_interface
デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# shape average 100000000(rate-in-bps)
デバイス(config-pmap-c)# service-policy qos_map_for_data_policy
```

8. **service-policy** を Cisco IOS XE Catalyst SD-WAN デバイスに関連付けます。

```
デバイス(config)# sdwan interface GigabitEthernet 1
デバイス(config-if)# rewrite-rule rule1
デバイス(config-if)# service-policy output qos_map_for_data_policy
```

9. ポリシングパラメータを次のように定義します。

```
デバイス(config)# policy policer policer_On_gige
デバイス(config-policer-policer_On_gige)# rate ?
Description: Bandwidth for 1g interfaces: <8..1000000000>bps; for 10g interfaces:
<8..10000000000>bps
Possible completions:<0..2^64-1>
デバイス(config-policer-policer_On_gige)# burst
Description: Burst rate, in bytes
Possible completions:<15000..100000000>
デバイス(config-policer-policer_On_gige)# exceed drop
```

10. アクセスリストセットをポリサーに関連付けます。

```
デバイス(config)# policy access-list ipv4_acl
デバイス(config-access-list-ipv4_acl)# sequence 100
デバイス(config-sequence-100)# match dscp 10
デバイス(config-match)# exit
デバイス(config-sequence-100)# action accept
デバイス(config-sequence-100)# action count dscp_10_count
デバイス(config-sequence-100)# policer policer_On_gige
デバイス(config-sequence-100)# action drop
vm5(config-action)#
```

11. アクセスリストを LAN または WAN インターフェイスに関連付けます。

```
デバイス(config)# sdwan interface GigabitEthernet5  
デバイス(config-interface-GigabitEthernet5)# access-list ipv4_acl  
デバイス(config-interface-GigabitEthernet5)# commit
```

CLIを使用した、IPv6に対するローカライズ型ポリシーの設定

以下は、CLIを使用した、アクセスリストを設定する手順の概略です。

1. ポリシングパラメータを次のように定義します。

```
デバイス(config)# policy policer policer_On_gige  
デバイス (config-policer-policer_On_gige)# rate ?  
Description: Bandwidth for lg interfaces: <8..1000000000>bps;for 10g interfaces:  
<8..10000000000>bps Possible completions: <0..2^64-1>  
デバイス(config-policer-policer_On_gige)# burst  
Description: Burst rate, in bytes Possible completions:<15000..100000000>  
デバイス(config-policer-policer_On_gige)# exceed drop
```

2. アクセスリストインスタンスを次のように作成します。

```
デバイス (config)# policy ipv6 access-list ipv6_access_list
```

3. 一連のマッチ/アクションペアのシーケンスを次のように作成します。

```
デバイス(config-access-list-ipv6_access_list)# sequence 100
```

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。

4. 次のように、パケットのマッチパラメータを定義します。

```
デバイス(config-sequence-100)# match traffic-class 10  
デバイス(config-match)# exit
```

5. 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。

```
デバイス(config-sequence-100)# action accept count traffic_class10_count  
デバイス(config-sequence-100)# action drop  
デバイス(config-sequence-100)# action accept class class1  
デバイス(config-sequence-100)# action accept policer policer_On_gige
```

6. 必要に応じて、アクセスリスト内にマッチ/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。
7. パケットがいずれかのシーケンスの条件のどれにもマッチしない場合、そのパケットはデフォルトで拒否されています。マッチしないパケットを受け入れる場合は、アクセスリストのデフォルトアクションを設定します。
8. アクセスリストをインターフェイスに適用します。

```

デバイス(config)# sdwan interface GigabitEthernet5
デバイス(config-interface-GigabitEthernet5)
# ipv6 access-list ipv6_access_list in
デバイス(config-interface-GigabitEthernet5)
# commit

```

インバウンド方向 (**in**) にアクセスリストを適用すると、インターフェイスで受信されるパケットに影響が出ます。アウトバウンド方向 (**out**) に適用すると、インターフェイスで送信されるパケットに影響が出ます。

ローカライズ型データポリシーの設定例

このトピックでは、ローカライズ型データポリシーを設定する簡単な例をいくつか紹介します。これはポリシーを使用して Cisco Catalyst SD-WAN ドメイン全体のトラフィックフローに影響を与える方法を理解するのに役立ちます。ローカライズされたデータポリシー（アクセスリストとも呼ばれる）は、ローカルの Cisco vEdge デバイスで直接設定されます。

QoS

Quality of Service (QoS) を設定して、データパケットを分類し、トラフィックが Cisco vEdge デバイスのインターフェイスやインターフェイスキューでどのように出入りするかを制御できます。QoS ポリシーの設定方法の例については、「転送および QoS の設定例」を参照してください。

ICMP Message の例

この例では、ICMP メッセージのローカライズ型データポリシーの設定を表示します。

```

policy
access-list acl_1
sequence 100
match
  protocol 1
  icmp-msg administratively-prohibited
!
action accept
count administratively-prohibited
!
!

```


ルータ生成 Cisco SD-WAN Manager トラフィックの QoS

表 17: 機能の履歴

機能名	リリース情報	説明
ルータ生成 Cisco SD-WAN Manager トラフィックの QoS	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a	これは、特定の要件に基づいてルータ生成 Cisco SD-WAN Manager トラフィックに優先順位を付けたり、キューイングしたりするのに役立つ機能です。QoS ポリシーとクラスマップを使用して、選択したキューを介して Cisco SD-WAN Manager トラフィックをルーティングします。

ルータ生成 Cisco SD-WAN Manager トラフィックの QoS について

Quality of Service (QoS) は、特定のタイプのトラフィックが他のトラフィックよりも優先されるように、ネットワークトラフィックを管理および優先順位付けするために使用される技術です。QoS は、ネットワークデバイスの管理とモニタリングに使用されるルータ生成 Cisco SD-WAN Manager トラフィックにとって特に重要です。詳細については、「[転送と QoS](#)」を参照してください。

ルータ生成トラフィックは、特定の要件に基づいて優先順位を付けたり、キューイングしたりできます。優先順位付けは、QoS ポリシーとクラスマップを使用して実現できます。

ルータ生成トラフィックを選択したキューに入れるには、次の手順を用いてください。

1. CLI テンプレートを使用してクラスマップを定義する：優先するトラフィックのタイプを指定します。この場合、クラスマップを作成して、キューに入れるルータ生成トラフィックを識別します。
2. CLI テンプレートを使用してポリシーマップを定義する：クラスマップで識別されたトラフィックに対して実行するアクションを定義します。優先順位を割り当てる、またはルータ生成トラフィックを特定のキューに配置するポリシーマップを作成します。

ルータ生成 Cisco SD-WAN Manager トラフィックにとっての QoS 上の利点

- ネットワークパフォーマンスの向上：ルータ生成された重要なトラフィックを重要度の低いトラフィックよりも優先することで、ネットワーク管理機能をスムーズに動作させ、ネットワークデバイスを効果的にモニターして制御します。
- ユーザーエクスペリエンスの向上：ルータ生成されたトラフィックをキューイングすることで、ネットワークの輻輳が防止されるので、ユーザー生成されたトラフィックによりネットワーク管理機能に悪い影響が出ません。キューイングにより、ユーザーエクスペリエンスが向上することになります。
- ネットワークの可用性の向上：ネットワーク管理の問題によって引き起こされるネットワークのダウンタイムのリスクを軽減します。これにより、ネットワークの可用性を向上させ、ネットワークの問題による事業運営への影響を軽減します。
- ネットワーク管理の簡素化：ネットワーク管理を簡素化し、手動による介入の必要性を軽減します。簡素化することで、時間の節約になるほか、人的エラーによるリスクの軽減もできるようになります。
- ネットワークリソースの効率的な使用：QoS ポリシーとクラスマップを使用すると、ネットワークリソースの効率的な割り当てができます。これにより、ルータで生成された重要なトラフィックが効率的にフローでき、他のネットワークトラフィックへの影響も最小限に抑えることができます。

ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の制約事項

- ルータ生成 Cisco SD-WAN Manager トラフィックに対して QoS 機能サポートしているのは、Cisco IOS XE Catalyst SD-WAN デバイスのみです。
- ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の設定は、CLI テンプレートを使用する場合にのみ可能です。
- この機能を使用すると、Cisco SD-WAN Manager 用にデバイスが生成するトラフィックに対してのみ、キューを使用して優先順位を付けることができます。他のデータおよび管理プレーントラフィックでは、引き続きデフォルトでキュー 0 を使用します。

CLI テンプレートを使用した、ルータで生成された Cisco SD-WAN Manager トラフィックの QoS の設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および[CLI テンプレート](#)を参照してください。



- (注) デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

クラスマップの定義とキュー番号へのマッピング

1. ローカライズ型ポリシーを使用してクラスマップを定義し、キュー番号にマッピングします。

```
policy class-map class Queue_1 queue 2
```

2. 変更を確定します。

クラス マップを定義し、キュー番号にマッピングするための設定例の全容を次に示します。

```
config-t
policy class-map class Queue_1 queue 2
!
```

ルータで生成された Cisco SD-WAN Manager トラフィックの QoS の有効化

ここでは、ルータで生成された Cisco SD-WAN Manager トラフィックの QoS を有効にする CLI 設定例を示します。

1. config-policy モードを開始します。

```
policy
```

2. 転送クラスを使用し、優先順位を付けるキューにマッピングしたクラスマップを使用します。

```
vmanage-forwarding-class queue_name
```

3. 変更を確定します。

ルータで生成された Cisco SD-WAN Manager トラフィックの QoS が有効になっています。

ルータで生成された Cisco SD-WAN Manager トラフィックの QoS を有効にする設定例の全容を次に示します。

```
config-t
policy
vmanage-forwarding-class Queue_1
!
```

CLI を使用した、ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS の確認

以下は、`show policy-map interface` コマンドで `GigabitEthernet 1` キーワードを指定した場合のサンプル出力例です。

```
Device# show policy-map interface GigabitEthernet 1
```

```

Service-policy output: shape_GigabitEthernet1

Class-map: class-default (match-any)
  8619 packets, 5056404 bytes
  5 minute offered rate 113000 bps, drop rate 0000 bps
  Match: any
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 8619/5056404
  shape (average) cir 4200000, bc 16800, be 16800
  target shape rate 4200000

Service-policy : qosmap

queue stats for all priority classes:
  Queueing
  priority level 1
  queue limit 512 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 565/95064

Class-map: Queue0 (match-any)
  565 packets, 95064 bytes
  5 minute offered rate 4000 bps, drop rate 0000 bps
  Match: qos-group 0
  police:
    rate 30 %
    rate 1260000 bps, burst 39375 bytes
    conformed 565 packets, 95064 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 4000 bps, exceeded 0000 bps
  Priority: Strict, b/w exceed drops: 0

Priority Level: 1

Class-map: Queue_1 (match-any)
  8050 packets, 4961100 bytes ----->
  5 minute offered rate 111000 bps, drop rate 0000 bps
  Match: qos-group 1
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 8050/4961100
  bandwidth remaining ratio 10

Class-map: Queue_2 (match-any)
  4 packets, 240 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 2
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 4/240
  bandwidth remaining ratio 10

```

この例では、それぞれのキューの **Class-map** に、ルータから宛先へのパケット転送の数、サイズ、およびレートが表示されています。Queue_1 に変更があるのを確認でき、パケット転送の追跡ができます。

ルータ生成 Cisco SD-WAN Manager トラフィックに対する QoS のトラブルシューティング

問題

CLI を使用して変更をコミットできない

Possible Causes

変更のコミット中に、入力されたキュー名に入力ミスや誤りがあった可能性があります。たとえば、queue 2 ではなく queuee 2 と入力すると、次のエラーが表示されます。「中止：「policy vmanage-traffic-forwarding-class」の不正な参照 (Aborted: illegal reference 'policy vmanage-traffic-forwarding-class')」

ソリューション

ルータからの Cisco SD-WAN Manager トラフィックが通過する正しいキュー名を入力します。



第 6 章

サービス側 VPN での DNS リダイレクト



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 18: 機能の履歴

機能名	リリース情報	説明
サービス側 VPN での DNS リダイレクト	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	プロキシサーバーを使用してドメインネームシステム (DNS) クエリに応答するよう、Cisco IOS XE Catalyst SD-WAN デバイスを設定できます。この機能により、サービス側 VPN ホストの DNS プロキシとサービス VPN 内の DNS リダイレクトのサポートが追加されます。

- [サービス側 VPN での DNS リダイレクトについて \(130 ページ\)](#)
- [サービス側 VPN での DNS リダイレクトに関する制約事項 \(130 ページ\)](#)
- [サービス側 VPN での DNS リダイレクトの使用例 \(131 ページ\)](#)
- [サービス側 VPN での DNS リダイレクトの設定 \(132 ページ\)](#)
- [CLI を使用したサービス側 VPN での DNS リダイレクトの設定 \(136 ページ\)](#)
- [サービス側 VPN での DNS リダイレクトの確認 \(137 ページ\)](#)
- [DNS リダイレクトの設定例 \(137 ページ\)](#)

サービス側 VPN での DNS リダイレクトについて

DNS リダイレクト機能を使用することで、Cisco IOS XE Catalyst SD-WAN デバイスが、クエリに関する一定の特性に基づいて選択された、ある具体的な設定と関連するホストテーブルキャッシュを使用して、DNS のクエリに対応できるようになります。DNS リダイレクト環境では、デバイスで複数の DNS データベースを設定できます。Cisco Catalyst SD-WAN ソフトウェアを設定しておくことで、デバイスが DNS クエリに応答するたびに、そのクエリを転送または解決することによって、DNS ネームサーバー設定の 1 つを選択できます。Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a がリリースされる前は、DNS リダイレクトのサポートは NAT ダイレクトインターネットアクセス (DIA) パスを介してのみでした。

アプリケーション認識型ルーティングポリシーにより、Cisco IOS XE Catalyst SD-WAN デバイスがアプリケーショントラフィックをサービス VPN に送信し、サービス VPN からアプリケーショントラフィックを受信することが許可されている場合、そのデバイスによって DNS ルックアップが実行され、アプリケーションサーバーに到達するためのパスが決まります。ルータがインターネットに接続されていない場合、そのような接続があるエッジデバイスに DNS クエリを送信し、そのデバイスがそのアプリケーションのサーバーに到達する方法を決定します。



- (注) インターネット接続されたデバイスが地理的に離れたデータセンターにあるネットワークでは、解決された DNS アドレスが、サービス VPN が配置されているサイトから地理的に離れたサーバーを指します。

Cisco IOS XE Catalyst SD-WAN デバイスはインターネット出口ポイントとして設定できるため、任意のルータがインターネットに直接到達して DNS ルックアップを実行することもできます。

DNS リダイレクトの設定は、一元管理型データポリシーを使用して設定するか、またはデータトラフィックに SLA 基準を適用する場合はアプリケーション認識型ルーティングポリシーを使用して行うことができます。

サービス側 VPN での DNS リダイレクトに関する制約事項

- DNS リダイレクト要求が同じポートと同じ VPN の別のホストからのものである場合、NAT が設定されていなければ、DNS リダイレクト要求は受け入れられません。
- NAT を使用して DNS サーバーの IP アドレスを設定する場合、データポリシーを使用して変更することはできません。
- フラグメント化された DNS パケットと自己生成された DNS はサポートされません。
- オーバーレイトンネルからの DNS 要求はサポートされていません。
- DNS リダイレクトは IPv4 トラフィックでのみサポートされ、IPv6 トラフィックではサポートされません。

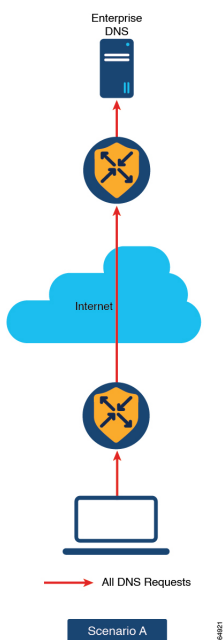
- User Datagram Protocol (UDP) を介した DNS 要求がサポートされています。ただし、Transmission Control Protocol (TCP) からの要求はサポートされていません。

サービス側 VPN での DNS リダイレクトの使用例

無条件の DNS リダイレクト

無条件の DNS リダイレクト (シナリオ A) では、ホストがすべての DNS 要求をローカルエッジルータに送信し、ローカルエッジルータは DNS 要求をデータセンターのエンタープライズ DNS サーバーにリダイレクト (これは、サービス側 VPN を使用している場合にのみ利用可能) し、DNS フォワーダとして機能します。この機能の使用例としては、プリンタに静的に設定された IP アドレスをデータセンターのエンタープライズ DNS サーバーにリダイレクトするのがあります。このような使用例では、すべてのレガシープリンタに DNS サーバーとなるローカルルータの IP アドレスが静的に設定されているため、プリンタからのすべての DNS 要求を転送する DNS フォワーダとして機能します。

図 12: 無条件の DNS リダイレクト



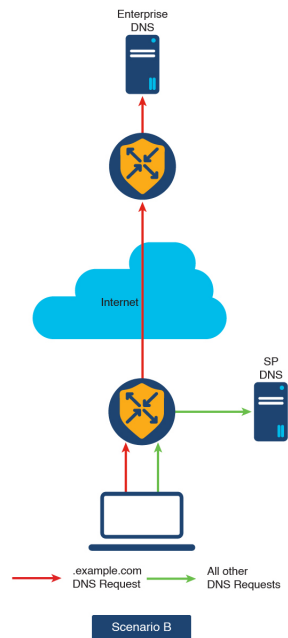
条件付き DNS リダイレクト

条件付き DNS リダイレクト (シナリオ B) では、ホストがデフォルトでサービスプロバイダー (SP) またはマネージドサービス プロバイダー (MSP) の DNS を使用します。Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン (SAIE) またはカスタムアプリケーション (*.google.com など) を使用する有名なアプリケーションの場合、DNS 要求は Cisco Catalyst SD-WAN オーバーレイ ネットワークを使用してエンタープライズ DNS サーバーに転送されます。他のすべての DNS 要求は、SP または MSP DNS サーバーに送信されます。



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

図 13: 条件付き DNS リダイレクト



サービス側 VPN での DNS リダイレクトの設定

1. Cisco SD-WAN Manager メニューから、[**Configuration**] > [**Policies**] の順に選択します。
2. [カスタムオプション (Custom Options)] ドロップダウンリストの [一元管理型ポリシー (Centralized Policy)] メニューから [トラフィックポリシー (Traffic Policy)] を選択します。
3. [トラフィックデータ (Traffic Data)] をクリックして、トラフィックデータポリシーを作成します。
4. [ポリシーの追加 (Add Policy)] ドロップダウンリストから、[新規作成 (Create New)] を選択します。
5. [名前 (Name)] と [説明 (Description)] に、データポリシーの名前と説明を入力します。
6. [シーケンスタイプ (Sequence Type)] をクリックします。
[データポリシーの追加 (Add Data Policy)] ダイアログボックスが表示されます。

7. 作成するデータポリシーのタイプを [アプリケーションファイアウォール (Application Firewall)]、[QoS]、[サービスチェーン (Service Chaining)]、[トラフィックエンジニアリング (Traffic Engineering)]、[カスタム (Custom)] から選択します。
 選択したタイプのデータポリシーを含むポリシーシーケンスが左側のペインに追加されます。
8. 該当するテキスト文字列をダブルクリックして、ポリシーシーケンスの名前を入力します。
 入力した名前は、左側のペインと右側のペインの両方にある [シーケンスタイプ (Sequence Type)] リストに表示されます。
9. [Sequence Rule] をクリックします。[マッチ/アクション (Match/Action)] ダイアログボックスが開くと、デフォルトで [マッチ (Match)] が選択されています。使用可能なポリシーマッチ条件は、メニューに一覧表示されます。
10. [プロトコル (Protocol)] ドロップダウンリストから [IPv4] を選択し、IPv4 アドレスファミリーにのみポリシーを適用します。
11. 1 つ以上の **マッチ** 条件を選択するには、フィールドをクリックし、説明に従って値を設定します。



(注) すべてのポリシーシーケンスタイプですべてのマッチ条件を使用できるわけではありません。

12. マッチするデータトラフィックに対して実行するアクションを選択するには、[アクション (Actions)] メニューをクリックします。
13. マッチするトラフィックをドロップするには、[ドロップ (Drop)] をクリックします。
 使用可能なポリシーアクションが右側に表示されます。
14. マッチするトラフィックを受け入れるには、[受け入れ (Accept)] をクリックします。
 使用可能なポリシーアクションが右側に表示されます。
15. [アクション (Actions)] メニューで、[DNS リダイレクト (Redirect DNS)] を選択して DNS リダイレクトを設定します。
16. [DNS のリダイレクト (Redirect DNS)] 条件フィールドに **IP アドレス** を入力し、[マッチとアクションの保存 (Save Match and Actions)] をクリックします。
17. [データポリシーの保存 (Save Data Policy)] をクリックします。

一致条件	手順
なし (すべてのパケットにマッチ)	マッチ条件を指定しないでください。

一致条件	手順
アプリケーション/アプリケーションファミリリスト/カスタムアプリケーション	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[アプリケーション/アプリケーションファミリリスト (Applications/Application Family List)] をクリックします。 2. ドロップダウンリストから、アプリケーションファミリを選択します。 3. アプリケーションリストを作成するには、次の手順を実行します。 <ol style="list-style-type: none"> 1. [新しいアプリケーションリスト (New Application List)] をクリックします。 2. リストの名前を入力します。 3. [アプリケーション (Application)] をクリックして、個々のアプリケーションのリストを作成します。[アプリケーションファミリ (Application Family)] をクリックして、関連するアプリケーションのリストを作成します。 4. [アプリケーションの選択 (Select Application)] ドロップダウンリストから、対応するアプリケーションまたはアプリケーションファミリを選択します。 5. [Save] をクリックします。
DNS アプリケーションリスト (DNS Application List)	<p>スプリット DNS を有効にするには、次のようにアプリケーションリストを追加します。</p> <ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[DNS アプリケーションリスト (DNS Application List)] をクリックします。 2. ドロップダウンリストから、アプリケーションファミリを選択します。
DNS	<p>アプリケーションリストを追加して、次のようにスプリット DNS 要求を処理します。</p> <ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[DNS] をクリックします。 2. ドロップダウンリストから、[リクエスト (Request)] を選択して、DNS アプリケーションの DNS 要求を処理します。
Destination Data Prefix	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[宛先データプレフィックス (Destination Data Prefix)] をクリックします。 2. 宛先プレフィックスのリストと照合するには、[データプレフィックス (Data Prefix)] ドロップダウンリストからリストを選択します。 3. 個々の宛先プレフィックスと照合するには、[宛先 : IPプレフィックス (Destination: IP Prefix)] フィールドにプレフィックスを入力します。

一致条件	手順
宛先ポート	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[宛先ポート (Destination Port)] をクリックします。 2. [宛先ポート (Destination Port)] フィールドにポート番号を入力します。単一のポート番号、ポート番号のリスト (番号がスペースで区切られたもの)、またはポート番号の範囲 (2つの番号がハイフン[-]で区切られたもの) を指定します。
[DSCP]	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[DSCP] をクリックします。 2. [DSCP] フィールドに、DSCP 値を 0 ~ 63 の数値で入力します。
パケット長 (Packet Length)	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[パケット長 (Packet Length)] をクリックします。 2. [パケット長 (Packet Length)] フィールドに、パケット長を 0 ~ 65535 の値で入力します。
PLP	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[PLP] をクリックして、[パケット損失の優先順位 (Packet Loss Priority)] を設定します。 2. [PLP] ドロップダウンリストから、[低 (Low)] または [高 (High)] を選択します。
Protocol	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[プロトコル (Protocol)] をクリックします。 2. [プロトコル (Protocol)] フィールドに、インターネットプロトコル番号を 0 ~ 255 の数字で入力します。
Source Data Prefix	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[送信元データプレフィックス (Source Data Prefix)] をクリックします。 2. 送信元プレフィックスのリストと照合するには、[送信元データプレフィックスリスト (Source Data Prefix List)] ドロップダウンリストからデータプレフィックスリストを選択します。 3. 個々の送信元プレフィックスと照合するには、[送信元 (Source)] フィールドにプレフィックスを入力します。
送信元ポート	<ol style="list-style-type: none"> 1. [マッチ (Match)] 条件メニューで、[送信元ポート (Source Port)] をクリックします。 2. [送信元 (Source)] フィールドに、ポート番号を入力します。単一のポート番号、ポート番号のリスト (スペースで区切られた番号)、またはポート番号の範囲 (ハイフン[-]で区切られた2つの番号) を指定します。

CLI を使用したサービス側 VPN での DNS リダイレクトの設定

次の手順は、一元管理型データポリシーを使用してリダイレクト DNS を有効にするために必要な最小限のポリシーコンポーネントを示しています。

1. 一元管理型制御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、番号を半角ダッシュ (-) 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. リダイレクト DNS を有効にするアプリケーションまたはアプリケーションファミリのリストを作成します。データポリシーの [マッチ (match)] セクションでこれらのリストを参照します。

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

3. リダイレクト DNS ポリシーを適用する VPN リストを作成します。

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

4. 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)# vpn-list list-name
```

5. 一連のマッチ/アクションペアのシーケンスを次のように作成します。

```
vSmart(config-vpn-list)# 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。

6. アプリケーションリストに含まれるアプリケーションまたはアプリケーションファミリの DNS サーバー解決を処理します。list-name の引数には、リスト名を指定します。

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

7. 次のように、DNS 要求（アウトバウンドデータトラフィックの場合）または応答（インバウンドデータトラフィックの場合）を処理するマッチ/アクションペアのシーケンスを設定します。

```
vSmart(config-sequence)# match dns (request | response)
```

8. デフォルトでは、ポリシーが適用される VPN で設定された DNS サーバーが、アプリケーションの DNS ルックアップの処理に使用されます。DNS 要求は、特定の DNS サーバーに送信できます。（サービスネットワークからの）アウトバウンドトラフィックに適用されるデータポリシー条件の場合は、DNS サーバーの IP アドレスを設定します。

```
vSmart(config-sequence)# action accept redirect-dns ip-address
```

（トンネルからの）インバウンドトラフィックに適用されるデータポリシー条件の場合は、DNS 応答がサービス VPN に正しく転送されるように、次のアクションを含めます。

```
vSmart(config-sequence)# action accept redirect-dns host
```

9. Cisco Catalyst SD-WAN 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)
```

サービス側 VPN での DNS リダイレクトの確認

以下は、DNS リダイレクト設定の確認方法を示す `show sdwan policy from-vsmart` コマンドからの出力例です。

```
vSmart# show sdwan policy from-vsmart
from-vsmart data-policy vpn1_dns-redirect-prefer-lte
direction from-service
vpn-list vpn1
sequence 1
match
source-ip 10.0.0.0/0
dns request
action accept
count gdns2 -396115821
redirect-dns 10.255.255.254
default-action accept
from-vsmart lists vpn-list vpn1
vpn 1
```

DNS リダイレクトの設定例

無条件 DNS リダイレクト

以下は、無条件 DNS リダイレクトの設定例であり、この場合すべての DNS 要求がマッチします。

```
policy
data-policy rdns
vpn-list vpn10
sequence 10
match
source-ip 0.0.0.0/0
```

```

        dns      request
        !
        action
        redirect-dns 209.165.200.225
        !
        default-action accept
        !
        !
!
apply-policy
site-list siteA
data-policy rdns from-service

```

条件付き DNS リダイレクト

以下は、条件付き DNS リダイレクトの設定例であり、この場合、アプリケーションリストを使用して次のように選択的 DNS 要求が定義されます。

```

policy
data-policy rdns
vpn-list vpn10
sequence 10
match
source-ip 10.0.0.0/8
dns      request
dns-app-list YouTube
!
action
redirect-dns 209.165.200.225
!
default-action accept
!
!
!
!
apply-policy
site-list siteA
data-policy rdns from-service

```




第 7 章

デフォルトの AAR ポリシーと QoS ポリシー



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 19: 機能の履歴

機能名	リリース情報	説明
デフォルトの AAR ポリシーと QoS ポリシーの設定	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、Cisco IOS XE Catalyst SD-WAN デバイスのデフォルトのアプリケーション認識型ルーティング (AAR)、データ、および Quality of Service (QoS) ポリシーを効率的に設定できます。この機能は、ネットワークアプリケーションのビジネス関連性、パス設定、およびその他のパラメータを分類し、それらの設定をトラフィックポリシーとして適用するための詳細なワークフローを提供します。

- [デフォルトの AAR ポリシーと QoS ポリシーについて \(140 ページ\)](#)
- [デフォルトの AAR ポリシーと QoS ポリシーの前提条件 \(141 ページ\)](#)
- [デフォルトの AAR ポリシーと QoS ポリシーに対する制約事項 \(141 ページ\)](#)
- [デフォルトの AAR ポリシーと QoS ポリシーに対応したデバイス \(142 ページ\)](#)
- [デフォルトの AAR ポリシーと QoS ポリシーの使用例 \(142 ページ\)](#)

- [Cisco SD-WAN Manager を使用したデフォルトの AAR および QoS ポリシーの設定 \(142 ページ\)](#)
- [デフォルトの AAR ポリシーと QoS ポリシーのモニター \(147 ページ\)](#)

デフォルトの AAR ポリシーと QoS ポリシーについて

ネットワーク内のデバイスに対し、AAR ポリシー、データポリシー、および QoS ポリシーを作成しておく、役立つことがよくあります。これらのポリシーは、トラフィックのルーティングと優先順位付けを行い、最善のパフォーマンスを実現します。これらのポリシーを作成する場合は、アプリケーションのビジネス関連性に基づいてネットワークトラフィックを生成するアプリケーション同士を区別し、ビジネス関連アプリケーションに高い優先順位を与えるとうまくいきます。

Cisco SD-WAN Manager は、ネットワーク内のデバイスに適用する AAR ポリシー、データポリシー、および QoS ポリシーのデフォルトセットを作成する際のワークフローを効率化します。このワークフローでは、1000 を超えるアプリケーションのセットが表示され、それらは Cisco IOS XE Catalyst SD-WAN デバイ스에組み込まれたアプリケーション認識テクノロジーである Network-Based Application Recognition (NBAR) によって識別されるようになっています。アプリケーションは、ワークフローを通じて、次の 3 つのビジネス関連カテゴリのいずれかにグループ化されます。

- [ビジネス関連 (Business-relevant)] : Webex ソフトウェアなど、事業運営にとって重要になりそうなもの。
- [ビジネス無関連 (Business-irrelevant)] : ゲームソフトウェアなど、事業運営にとって重要ではなさそうなもの。
- [デフォルト (Default)] : 事業運営との関連性についての判断はなし。

アプリケーションは、ワークフローを通じて、各ビジネス関連カテゴリ内のアプリケーションリスト (ブロードキャストビデオ、マルチメディア会議、VoIP テレフォニーなど) にグループ化されます。

この分類に関しては、ワークフローを使用して、各アプリケーションのビジネス関連性について事前定義したものを受け入れることも、特定のアプリケーションの場合はビジネス関連性のカテゴリから別のカテゴリに移動してカスタマイズすることもできます。たとえば、デフォルトでは、ワークフローによって特定のアプリケーションがビジネスに無関連と事前定義されたとしても、そのアプリケーションが自社の事業運営にとって重要な場合は、ビジネス関連として再分類できます。

ビジネスとの関連性、パス設定、およびサービスレベル契約 (SLA) カテゴリを設定するための手順は、このワークフローの中で順を追って説明します。

ワークフローを完了すると、Cisco SD-WAN Manager によって次のデフォルトセットが生成されます。

- AAR ポリシー
- QoS ポリシー

- データポリシー

これらのポリシーは一元管理型ポリシーにアタッチすると、デフォルトポリシーとして、ネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイスに適用できます。

NBAR に関する基本情報

NBAR は、Cisco IOS XE Catalyst SD-WAN デバイスに含まれるアプリケーションを認識するテクノロジーです。NBAR は、プロトコルと呼ばれるアプリケーションの定義一式を使用して、トラフィックを識別および分類します。トラフィックに割り当てるカテゴリの1つは、ビジネス関連属性です。この属性の値には、[ビジネス関連 (Business-relevant)]、[ビジネス無関連 (Business-irrelevant)]、および[デフォルト (Default)]があります。アプリケーションを識別するためのプロトコルを開発する際、シスコは、アプリケーションが一般的な事業運営にとって重要となりそうかどうかを推定し、ビジネス関連の値をアプリケーションに割り当てます。デフォルトの AAR および QoS ポリシー機能は、NBAR によって提供されるビジネス関連の分類を使用します。

デフォルトの AAR ポリシーと QoS ポリシーの利点

- 帯域幅の割り当てを管理およびカスタマイズします。
- ビジネスとの関連性に基づいてアプリケーションの優先順位付けを行います。

デフォルトの AAR ポリシーと QoS ポリシーの前提条件

- 関連するアプリケーションにまつわる知識。
- トラフィックに優先順位を付ける SLA マーキングと QoS マーキングに関する知識。

デフォルトの AAR ポリシーと QoS ポリシーに対する制約事項

- ビジネス関連のアプリケーショングループをカスタマイズする場合、そのグループから別のセクションにすべてのアプリケーションを移動することはできません。ビジネス関連セクションのアプリケーショングループには、少なくとも1つのアプリケーションが必要です。
- デフォルトの AAR ポリシーおよび QoS ポリシーは、IPv6 アドレッシングをサポートしていません。

デフォルトの AAR ポリシーと QoS ポリシーに対応したデバイス

- Cisco 1000 シリーズサービス統合型ルータ (ISR1100-4G および ISR1100-6G)
- Cisco 4000 シリーズサービス統合型ルータ (ISR44xx)
- Cisco Catalyst 8000V Edge ソフトウェア
- Cisco Catalyst 8300 シリーズ エッジプラットフォーム
- Cisco Catalyst 8500 シリーズ エッジプラットフォーム
- Cisco C1100 シリーズ サービス統合型ルータ

デフォルトの AAR ポリシーと QoS ポリシーの使用例

Cisco Catalyst SD-WAN ネットワークを設定し、ネットワーク内のすべてのデバイスに AAR および QoS ポリシーを適用する場合は、この機能を使用することで、これらのポリシーを迅速に作成して展開できます。

Cisco SD-WAN Manager を使用したデフォルトの AAR および QoS ポリシーの設定

Cisco SD-WAN Manager を使用してデフォルトの AAR、データ、および QoS ポリシーを設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. **[デフォルトの AAR と QoS を追加 (Add Default AAR & QoS)]** をクリックします。
[プロセスの概要 (Process Overview)] ページが表示されます。
3. **[Next]** をクリックします。
[選択内容に基づく推奨設定 (Recommended Settings based on your selection)] ページが表示されます。
4. ネットワークの要件に基づいて、**[ビジネス関連 (Business Relevant)]**、**[デフォルト (Default)]**、**[ビジネス非関連 (Business Irrelevant)]** の各グループ間でアプリケーションを移動します。



(注) アプリケーションの分類をビジネス関連、ビジネス非関連、またはデフォルトとしてカスタマイズする場合は、個々のアプリケーションをあるカテゴリから別のカテゴリに移動することはできません。あるカテゴリから別のカテゴリにグループ全体を移動することはできません。

5. **[Next]** をクリックします。

[パスの設定 (オプション) (Path Preferences (optional))] ページで、各トラフィッククラスの優先および優先バックアップトランスポートを選択します。

6. **[Next]** をクリックします。

[アプリルートポリシーサービスレベルアグリーメント (SLA) クラス (App Route Policy Service Level Agreement (SLA) Class)] ページが表示されます。

このページには、各トラフィッククラスの [損失 (Loss)]、[遅延 (Latency)]、および [ジッター (Jitter)] 値のデフォルト設定が表示されます。必要に応じて、各トラフィッククラスの [損失 (Loss)]、[遅延 (Latency)]、および [ジッター (Jitter)] 値をカスタマイズします。

7. **[Next]** をクリックします。

[エンタープライズクラスからサービスプロバイダークラスへのマッピング (Enterprise to Service Provider Class Mapping)] ページが表示されます。

1. さまざまなキューの帯域幅をカスタマイズする方法に基づいて、サービスプロバイダークラスのオプションを選択します。QoS キューの詳細については、「アプリケーションリストからキューへのマッピング」の項を参照してください。
2. 必要に応じて、各キューの帯域幅のパーセンテージの値をカスタマイズします。

8. **[Next]** をクリックします。

[デフォルトポリシーとアプリケーションリストのプレフィックスの定義 (Define prefixes for the default policies and applications lists)] ページが表示されます。

各ポリシーについて、プレフィックス名と説明を入力します。

9. **[Next]** をクリックします。

[Summary] ページが表示されます。このページでは、各設定の詳細を表示できます。

[編集 (Edit)] をクリックして、ワークフローの前に表示されたオプションを編集できます。[編集 (Edit)] をクリックすると、関連ページに戻ります。

10. **[構成]** をクリックします。

Cisco SD-WAN Manager は、AAR、データ、および QoS ポリシーを作成し、プロセスが完了したことを示します。

次の表では、ワークフローのステップまたはアクションと、それぞれの効果について説明します。

表 20: ワークフローのステップと効果

ワークフローステップ	影響を受けるものは次のとおりです
選択内容に基づく推奨設定	AAR とデータポリシー
パスの設定 (オプション)	AAR ポリシー
アプリ ルート ポリシー サービス レベル アグリーメント (SLA) クラス : <ul style="list-style-type: none"> • 損失 • 遅延 • Jitter 	AAR ポリシー
エンタープライズからサービスプロバイダークラスへのマッピング	データおよび QoS ポリシー
デフォルトポリシーとアプリケーションのプレフィックスの定義	AAR、データ、QoS ポリシー、転送クラス、アプリケーションリスト、SLA クラスリスト

11. ポリシーを表示するには、[作成したポリシーの表示 (View Your Created Policy)] をクリックします。



- (注) ネットワーク内のデバイスにデフォルトの AAR および QoS ポリシーを適用するには、AAR およびデータポリシーを必要なサイトリストにアタッチする一元管理型ポリシーを作成します。QoS ポリシーを Cisco IOS XE Catalyst SD-WAN デバイスに適用するには、デバイステンプレートを使用してローカライズ型ポリシーに適用します。

アプリケーションリストのキューへのマッピング

次のリストに、各サービス プロバイダークラス オプション、各オプションのキュー、および各キューに含まれるアプリケーションリストを示します。アプリケーションリストには、このワークフローの [パスの設定 (Path Preferences)] ページに表示される名前が付けられます。

4 QoS クラス

- 音声
 - インターネットワーク制御
 - VoIP テレフォニー
- ミッションクリティカル
 - ブロードキャストビデオ

- マルチメディア会議
- リアルタイム インタラクティブ
- マルチメディア ストリーミング

- ビジネスデータ
 - シグナリング
 - トランザクション データ
 - ネットワーク管理
 - バルク データ

- デフォルト
 - ベストエフォート型
 - スカベンジャー

5 QoS クラス

- 音声
 - インターネットワーク制御
 - VoIP テレフォニー

- ミッションクリティカル
 - ブロードキャストビデオ
 - マルチメディア会議
 - リアルタイム インタラクティブ
 - マルチメディア ストリーミング

- ビジネスデータ
 - シグナリング
 - トランザクション データ
 - ネットワーク管理
 - バルク データ

- 一般データ
 - スカベンジャー

- デフォルト

- ベストエフォート型

6 QoS クラス

- 音声
 - インターネットワーク制御
 - VoIP テレフォニー
- ビデオ
 - ブロードキャストビデオ
 - マルチメディア会議
 - リアルタイム インタラクティブ
- [Mission Critical]
 - マルチメディア ストリーミング
- ビジネスデータ
 - シグナリング
 - トランザクション データ
 - ネットワーク管理
 - バルク データ
- 一般データ
 - スカベンジャー
- デフォルト
 - ベストエフォート型

8 QoS クラス

- 音声
 - VoIP テレフォニー
- Net-ctrl-mgmt
 - インターネットワーク制御
- インタラクティブ ビデオ
 - マルチメディア会議

- リアルタイム インタラクティブ
- ストリーミング ビデオ
 - ブロードキャストビデオ
 - マルチメディア ストリーミング
- コール シグナリング
 - シグナリング
- 重要なデータ
 - トランザクション データ
 - ネットワーク管理
 - バルク データ
- スカベンジャー
 - スカベンジャー
- デフォルト
 - ベストエフォート型

デフォルトの AAR ポリシーと QoS ポリシーのモニター

デフォルト AAR ポリシーのモニタリング

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. **[カスタムオプション (Custom Options)]** をクリックします。
3. **[一元管理型ポリシー (Centralized Policy)]** から **[トラフィックポリシー (Traffic Policy)]** を選択します。
4. **[アプリケーション認識型ルーティング (Application Aware Routing)]** をクリックします。
AAR ポリシーのリストが表示されます。
5. **[トラフィックデータ (Traffic Data)]** をクリックします。
トラフィックデータポリシーのリストが表示されます。

QoS ポリシーのモニタリング

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

2. [カスタムオプション (Custom Options)] をクリックします。
3. [ローカライズ型ポリシー (Localized Policy)] から [転送クラス/QoS (Forwarding Class/QoS from Localized Policy)] を選択します。
4. [QoSマップ (QoS Map)] をクリックします。
QoS ポリシーのリストが表示されます。



(注) QoS ポリシーを確認するには、[「QoS ポリシーの確認」](#) を参照してください。



第 8 章

デバイスアクセスポリシー



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 21: 機能の履歴

機能名	リリース情報	説明
SNMP および SSH のデバイスアクセスポリシー	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	これは、トラフィックがインターフェイスを通過するために満たす必要のあるルールを定義する機能です。着信トラフィックのルールを定義した場合、そのルールが他のどのポリシーよりも先にトラフィックに適用されます。Cisco IOS XE Catalyst SD-WAN デバイスのコントロールプレーンは、一連の送信元からのローカルサービス (SSH や SNMP など) のデータトラフィックを処理します。オーバーレイを形成するには、ルーティングパケットが必要です。

- [デバイスアクセスポリシーの概要 \(150 ページ\)](#)
- [Cisco SD-WAN Manager を使用したデバイスアクセスポリシーの設定 \(150 ページ\)](#)
- [CLI を使用したデバイスアクセスポリシーの設定 \(153 ページ\)](#)
- [ACL 統計とカウンタの例 \(153 ページ\)](#)
- [SNMP サーバーに対する ACL ポリシーの確認 \(154 ページ\)](#)

- SSH に対する ACL ポリシーの確認 (156 ページ)

デバイスアクセスポリシーの概要

Cisco IOS XE SD-WAN リリース 17.2.1r 以降では、すべての Cisco IOS XE Catalyst SD-WAN デバイスでデバイスアクセスポリシーを設定するように Cisco SD-WAN Manager ユーザーインターフェイスが拡張されています。

Cisco IOS XE Catalyst SD-WAN デバイスのコントロールプレーンは、一連の送信元からのローカルサービス (SSH や SNMP など) のデータトラフィックを処理します。悪意のあるトラフィックを回避するため、フィルタを適用してデバイスアクセストラフィックから CPU を保護することが重要です。

アクセスポリシーでは、トラフィックがインターフェイスを通過するために満たす必要のあるルールを定義します。着信トラフィックのルールを定義した場合、そのルールが他のどのポリシーよりも先にトラフィックに適用されます。ルーテッドファイアウォールモードおよびトランスペアレントファイアウォールモードで、アクセスポリシーを使用して IP トラフィックを制御できます。アクセスルールでは、使用されるプロトコル、送信元および宛先の IP アドレスまたはネットワーク、および任意でユーザーおよびユーザーグループに基づいてトラフィックが許可または拒否されます。インターフェイスでの各着信パケットは、指定した基準に基づいて転送またはドロップする必要があるかどうかを判断するために分析されます。発信トラフィックのアクセスルールを定義した場合、パケットはインターフェイスから出る前に分析されます。アクセスポリシーは順序で適用されます。つまり、デバイスは、ルールとパケットを比較するとき、アクセスポリシーリストの上から下に検索を行い、最初に一致したルールに対するポリシーを適用します。それ以降のルールは、(最初のルールより一致率が高くて) すべて無視されます。したがって、特定のルールがスキップされないようにするには、そのルールを汎用性の高いルールよりも上に配置する必要があります。

Cisco SD-WAN Manager を使用したデバイスアクセスポリシーの設定

Cisco IOS XE Catalyst SD-WAN デバイスは、コントロールプレーンに向けられた SNMP および SSH トラフィックを処理するためのデバイスアクセスポリシー設定をサポートしています。Cisco SD-WAN Manager を使用して、デバイスアクセスポリシーに基づいて宛先ポートを設定します。



- (注) Cisco SD-WAN Manager の [ツール (Tools)] > [SSH ターミナル (SSH Terminal)] からデバイスへの接続を許可するには、**デバイスアクセスプロトコル**を SSH として、**送信元データプレフィックス**を 192.168.1.5/32 として受け入れるルールを作成します。

ローカライズされたデバイスアクセス制御ポリシーを設定するには、Cisco SD-WAN Manager のポリシー構成ウィザードを使用します。

作成する特定のポリシーに応じて、特定のコンポーネントまたはすべてのコンポーネントを構成します。コンポーネントをスキップするには、[次へ (Next)] ボタンをクリックします。コンポーネントに戻るには、画面下部にある [戻る (Back)] ボタンをクリックします。

デバイスアクセスポリシーの設定

1. Cisco SD-WAN Manager メニューから、[Configuration] > [Policies] の順に選択します。
2. [ローカライズ型ポリシー (Localized Policy)] をクリックし、[カスタムオプション (Custom Options)] ドロップダウンの [ローカライズ型ポリシー (Localized Policy)] で [アクセス制御リスト (Access Control Lists)] を選択します。
3. [デバイスアクセスポリシーの追加 (Add Device Access Policy)] ドロップダウンリストから、[IPv4 デバイスアクセスポリシーの追加 (Add IPv4 Device Access Policy)] または [IPv6 デバイスアクセスポリシーの追加 (Add IPv6 Device Access Policy)] オプションを選択してデバイスを追加します。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降でポリシーシーケンスを使用せず、デフォルトアクションの [受け入れ (Accept)] または [ドロップ (Drop)] のみで IPv4 または IPv6 のデバイスアクセスポリシーを設定する場合、デバイスアクセスポリシーは SSH と SNMP 構成を作成します。デフォルトアクションのみを使用し、ポリシーシーケンスを使用せずにデバイスアクセスポリシーを作成して、SSH と SNMP の両方のデバイス設定または Cisco SD-WAN Manager 設定を作成できるようになりました。

SNMP サーバー構成を作成しない場合、デバイスアクセスポリシーによって作成された SNMP 構成は使用されません。

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 より前では、デフォルトアクションの [受け入れ (Accept)] または [ドロップ (Drop)] のみを使用し、ポリシーシーケンスを使用せずにデバイスアクセスポリシーを設定する場合、デバイスアクセスポリシーはデバイス設定または Cisco SD-WAN Manager 設定を作成しませんでした。

4. ドロップダウンリストから [IPv4 デバイスアクセスポリシーの追加 (Add IPv4 Device Access Policy)] を選択して、[IPv4 ACL ポリシー (IPv4 ACL Policy)] を追加します。[デバイス IPv4 ACL ポリシーの編集 (Edit Device IPv4 ACL Policy)] ページが表示されます。
5. 新しいポリシーの名前と説明を入力します。
6. [ACL シーケンスの追加 (Add ACL Sequence)] をクリックして、シーケンスを追加します。[デバイスアクセス制御リスト (Device Access Control List)] ページが表示されます。
7. [Sequence Rule] をクリックします。[マッチ (Match)] と [アクション (Actions)] オプションが表示されます。
8. [マッチ (Match)] をクリックし、ACL ポリシーの次の条件を選択して設定します。

一致条件	説明
デバイスアクセスプロトコル (Device Access Protocol) (必須)	ドロップダウンリストからキャリアを選択します。たとえば、SNMP、SSH などです。
送信元データプレフィックス (Source Data Prefix)	送信元 IP アドレスを入力します。たとえば、10.0.0.0/12 です。
送信元ポート	送信元ポートのリストを入力します。値の範囲は 0 ~ 65535 です。
Destination Data Prefix	宛先 IP アドレスを入力します。たとえば、10.0.0.0/12 です。
VPN	VPN ID を入力します。範囲は 0 ~ 65536 です。

9. [アクション (Actions)] をクリックし、ACL ポリシーの次の条件を設定します。

アクション条件	説明
承認	
カウンタ名	受け付けるカウンタ名を入力します。最大で 20 文字です。
削除 (Drop)	
カウンタ名	ドロップするカウンタ名を入力します。最大で 20 文字です。

10. [マッチとアクションの保存 (Save Match And Actions)] をクリックして、ACL ポリシーのすべての条件を保存します。
11. [デバイスアクセス制御リストポリシーの保存 (Save Device Access Control List Policy)] をクリックして、選択したマッチ条件をアクションに適用します。
12. 一致するパケットがない場合、いずれかのルート ポリシー シーケンス ルールになります。左側のペインの [デフォルトアクション (Default Action)] では、パケットをドロップします。



- (注) IPv6 プレフィックス一致は、Cisco IOS XE Catalyst SD-WAN デバイス ではサポートされていません。これらのデバイスで IPv6 プレフィックス一致を設定しようとすると、Cisco SD-WAN Manager はデバイス設定の生成に失敗します。

CLI を使用したデバイスアクセスポリシーの設定

Configuration:

```
ip access-list standard snmp-acl
 1 permit 10.0.1.12 255.255.255.0
 11 deny any
!

snmp-server community private view v2 ro snmp-acl

ip access-list extended ssh-acl
 1 permit tcp host 10.0.1.12 any eq 22
 11 deny tcp any any eq 22
!

line vty 0 4
 access-class ssh-acl in vrf-also
!
```



(注) IPv6 プレフィックス一致は、Cisco IOS XE Catalyst SD-WAN デバイス ではサポートされていません。

ACL 統計とカウンタの例

YANG を使用して ACL 統計とカウンタを設定するには、次の手順を実行します。

Yang file: Cisco-IOS-XE-acl-oper.yang

```
grouping ace-oper-data {
  description
    "ACE operational data";
  leaf match-counter {
    type yang:counter64;
    description
      "Number of matches for an access list entry";
  }
}
```

YANG モデルを使用した設定の例：

```
Router# show access-lists access-list ACL-1
```

```
ACCESS
CONTROL
LIST      RULE  MATCH
NAME      NAME  COUNTER
-----
ACL-1    1     0
         2     0
```

```
Router# show access-lists access-list ACL-1 | display xml
```

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <access-lists xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acl-oper">
    <access-list>
      <access-control-list-name>ACL-1</access-control-list-name>
      <access-list-entries>
```

```

<access-list-entry>
  <rule-name>1</rule-name>
  <access-list-entries-oper-data>
    <match-counter>0</match-counter>
  </access-list-entries-oper-data>
</access-list-entry>
<access-list-entry>
  <rule-name>2</rule-name>
  <access-list-entries-oper-data>
    <match-counter>0</match-counter>
  </access-list-entries-oper-data>
</access-list-entry>
</access-list-entries>
</access-list>
</access-lists>
</config>
Router#

```

CLI を使用して ACL 統計とカウンタを表示するには、次のように コマンドを使用します。

```
show ip access-list [access-list-number | access-list-name]
```

CLI を使用した統計の出力例：

```
show ip access-list [access-list-number | access-list-name]
```

```

Router# show ip access-list ACL-1
Extended IP access list ACL-1
10 permit ip host 10.1.1.1 any (3 matches) 30
30 permit ip host 10.2.2.2 any (27 matches)

```

To clear counters in ACL stats:

```
clear ip access-list counters {access-list-number | access-list-name}
```

SNMP サーバーに対する ACL ポリシーの確認

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r リリース以降、Cisco IOS XE Catalyst SD-WAN デバイスでは SNMP サーバーに対するデバイスアクセスポリシー機能をサポートしています。SNMP の場合、SNMP 機能テンプレートが設定されていないときに、Cisco SD-WAN Manager が確認をして、デバイスでテンプレートがプッシュされるのをブロックします。



- (注) SNMP の場合、宛先データプレフィックスリストは Cisco IOS XE Catalyst SD-WAN デバイスに適用されません。デバイスの SNMP 設定を使用してこのローカライズ型ポリシーを適用しても、宛先データプレフィックスは無視されます。

Configuration:

```
snmp-server community private view v2 ro snmp-acl
```

snmp-server community コマンドの YANG モデル。以下は、YANG モデルの ACL 設定例を示したものです。


```
container community {
  description
    "Configure a SNMP v2c Community string and access privs";
  tailf:cli-compact-syntax;
  tailf:cli-sequence-commands;
  leaf community-string {
    tailf:cli-drop-node-name;
    type string;
  }
  container access {
    tailf:cli-drop-node-name;
    tailf:cli-flatten-container;
    leaf standard-acl {
      tailf:cli-drop-node-name;
      tailf:cli-full-command;
      type uint32 {
        range "1..99";
      }
    }
    leaf expanded-acl {
      tailf:cli-drop-node-name;
      tailf:cli-full-command;
      type uint32 {
        range "1300..1999";
      }
    }
  }
  leaf acl-name {
    tailf:cli-drop-node-name;
    tailf:cli-full-command;
    type string;
  }
  leaf ipv6 {
    description
      "Specify IPv6 Named Access-List";
    tailf:cli-full-command;
    type string;
  }
  leaf ro {
    description
      "Read-only access with this community string";
    type empty;
  }
  leaf rw {
    description
      "Read-write access with this community string";
    type empty;
  }
}
}
```

以下は、snmp-server ACL 設定のサンプルテストログを示したものです。

```
Device# sh sdwan ver
16.12.1

Device# config-t

admin connected from 127.0.0.1 using console on the device
Device(config)# snmp-server community TEST_1 RO 80
Device(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.

Device#
*Mar 13 21:17:19.377: %SYS-5-CONFIG_P: Configured programmatically by process
```

```

session_id_for_dmi_vty_100001 from console as NETCONF on vty31266
*Mar 13 21:17:19.377: %DMI-5-CONFIG_I: R0/0: nesc: Configured from NETCONF/RESTCONF by
admin, transaction-id 518

Device#
Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80

Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80
Device#

admin connected from 127.0.0.1 using console on the device
Device(config)# snmp-server community TEST_V6 ipv6 acl-name-1
Device(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
Device#

*Mar 13 21:18:10.040: %SYS-5-CONFIG_P: Configured programmatically by process
session_id_for_dmi_vty_100001 from console as NETCONF on vty31266
*Mar 13 21:18:10.041: %DMI-5-CONFIG_I: R0/0: nesc: Configured from NETCONF/RESTCONF by
admin, transaction-id 535

Device#
Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80
snmp-server community TEST_V6 ipv6 acl-name-1
Device#
Device# sh run | i snmp
snmp-server community TEST_1 RO 80
snmp-server community TEST_V6 RO ipv6 acl-name-1
Device#

```

SSH に対する ACL ポリシーの確認

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r リリース以降、Cisco IOS XE Catalyst SD-WAN デバイスでは仮想テレタイプ (VTY) 回線を使用する SSH サーバー上で `device-access-policy` 機能をサポートしています。Cisco SD-WAN Manager は、バックエンドで使用可能なすべての VTY 回線を使用し、それに応じてポリシーをプッシュします。

Configuration:

```

line vty 0 4
  access-class ssh-acl in vrf-also
!
```

以下は、YANG モデルの ACL 設定例を示したものです。

```

// line * / access-class
  container access-class {
    description
      "Filter connections based on an IP access list";
    tailf:cli-compact-syntax;
    tailf:cli-sequence-commands;
    tailf:cli-reset-container;
    tailf:cli-flatten-container;
    list access-list {
      tailf:cli-drop-node-name;
    }
  }

```

```
tailf:cli-compact-syntax;
tailf:cli-reset-container;
tailf:cli-suppress-mode;
tailf:cli-delete-when-empty;
key "direction";
leaf direction {
  type enumeration {
    enum "in";
    enum "out";
  }
}
leaf access-list {
  tailf:cli-drop-node-name;
  tailf:cli-prefix-key;
  type ios-types:exp-acl-type;
  mandatory true;
}
leaf vrf-also {
  description
    "Same access list is applied for all VRFs";
  type empty;
}
}
```

次に、line-server ACL 設定のサンプルテストログを示します。

```
Device# config-transaction

admin connected from 127.0.0.1 using console on Device
Device(config)# line vty 0 4
Device(config-line)# access-class acl_1 in vrf-also
Device(config-line)# transport input ssh
Device(config-line)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
Device#
*May 24 20:51:02.994: %SYS-5-CONFIG_P: Configured programmatically by process
iosp_vty_100001_dmi_nesd from console as NETCONF on vty31266
*May 24 20:51:02.995: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by
admin, transaction-id 227
Device#
Device#
Device# sh sdwan run | sec vty
Error: Licensing infrastructure is NOT initialized.
Error: Licensing infrastructure is NOT initialized.
line vty 0 4
  access-class acl_1 in vrf-also
  login local
  transport input ssh
line vty 5 80
  login local
  transport input ssh
Device#
Device# sh run | sec vty
Error: Licensing infrastructure is NOT initialized.
Error: Licensing infrastructure is NOT initialized.
line vty 0 4
  access-class acl_1 in vrf-also
  exec-timeout 0 0
  password 7 11051807
  login local
  transport preferred none
  transport input ssh
line vty 5 80
```

```
login local
transport input ssh
```



第 9 章

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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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 \(159 ページ\)](#)
- [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 \(160 ページ\)](#)
- [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 \(166 ページ\)](#)

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 22:

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 <i>counter-name</i>	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 23:

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 <i>color [encap encapsulation]</i>	<i>color</i> 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、privatel ~ private6、public-internet、red、silver。 デフォルトでは、 <i>encapsulation</i> 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ダプ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 <i>service-name</i> [tloc <i>ip-address</i> tloc-list <i>list-name</i>] [vpn <i>vpn-id</i>]	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 <i>color</i> [encap <i>encapsulation</i>]	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 <i>list-name</i>	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 <i>vpn-id</i>	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



第 10 章

アプリケーション認識型ルーティング



(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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

- [アプリケーション認識型ルーティングについて \(169 ページ\)](#)
- [アプリケーション認識型ルーティングの設定 \(180 ページ\)](#)
- [CLI を使用したアプリケーション認識型ルーティングの設定 \(202 ページ\)](#)
- [CLI を使用したアプリケーションプロブクラスの設定 \(204 ページ\)](#)
- [アプリケーション認識型ルーティングポリシーの設定例 \(205 ページ\)](#)

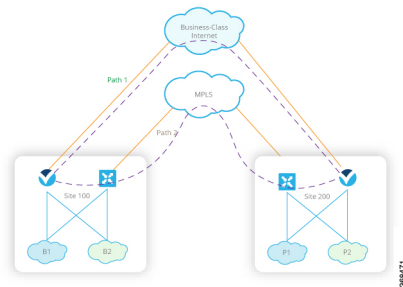
アプリケーション認識型ルーティングについて

アプリケーション認識型ルーティングは、Cisco IOS XE Catalyst SD-WAN デバイス間のデータプレーントンネルのネットワークとパスの特性を追跡し、収集した情報を使用してデータトラフィックの最適なパスを計算します。対象となる特性には、パケット損失、遅延、ジッターなどがあります。ルートプレフィックス、メトリック、リンクステート情報、Cisco IOS XE Catalyst SD-WAN デバイスでのルート削除など、標準のルーティングプロトコルで 사용되는パス選択の要因以外を考慮する機能があるため、企業に次のような多くの利点をもたらします。

- 通常のネットワーク運用の場合は、ネットワークを経由するアプリケーションデータトラフィックのパスを最適化できます。アプリケーションの SLA で定義されたパケット損

失、遅延、ジッターに対し、必要なレベルを満たせるようにする WAN リンクにパスを誘導することにより、これを実現します。

- ネットワークの停止またはソフト障害が発生した場合は、パフォーマンスの低下を最小限に抑えることができます。ネットワークとパスの状況をリアルタイムなアプリケーション認識型ルーティングで追跡するので、パフォーマンスの問題をすぐに明らかにし、利用できる最善なパスにデータトラフィックをリダイレクトする戦略を自動的にアクティブ化させます。ネットワークがソフト障害の状態から回復すると、アプリケーション認識型ルーティングはデータトラフィックパスを自動的に再調整します。
- データトラフィックをより効率的にロードバランシングできるため、ネットワークコストを削減できます。
- WAN をアップグレードせずに、アプリケーションのパフォーマンスを向上させることができます。



各 Cisco IOS XE Catalyst SD-WAN デバイスは最大 8 つの TLOC をサポートするので、1 つの Cisco IOS XE Catalyst SD-WAN デバイスを最大 8 つの異なる WAN ネットワークに接続できます。この機能により、アプリケーショントラフィックにパケット損失と遅延に関するさまざまなニーズがあっても、パスのカスタマイズができるのです。

マルチキャストプロトコルに対応したアプリケーション認識型ルーティング

表 24: 機能の履歴

機能	リリース情報	説明
マルチキャストに対応したアプリケーション認識型ルーティング	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	これは、送信元と宛先、プロトコル照合、および SLA 要件に基づいて、Cisco IOS XE Catalyst SD-WAN デバイスのマルチキャストトラフィックに、アプリケーション認識型ルーティングポリシーを設定できるようにする機能です。

Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降、アプリケーション認識型ルーティングは、Cisco IOS XE Catalyst SD-WAN デバイス上のオーバーレイ マルチキャストトラフィックをサポートしています。これ以前のリリースでは、アプリケーションルートポリシーはユニキャストトラフィックにしか対応していません。

Cisco IOS XE Catalyst SD-WAN デバイスは、グループアドレスに基づいてマルチキャストトラフィックを分類し、SLA クラスを設定します。グループアドレスには、送信元 IP、宛先 IP、送信元プレフィックス、および宛先プレフィックスを指定できます。フォワーディングプレーンでは、グループアドレスのトラフィックは、SLA 要件を満たす TLOC パスのみを使用する必要があります。グループのパス選択は、優先カラー、バックアップカラー、またはデフォルトアクションに基づいて実行できます。

マルチキャストプロトコルに関する制約事項

Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) フローを使用する Network-Based Application Recognition (NBAR) は、マルチキャストではサポートされていません。



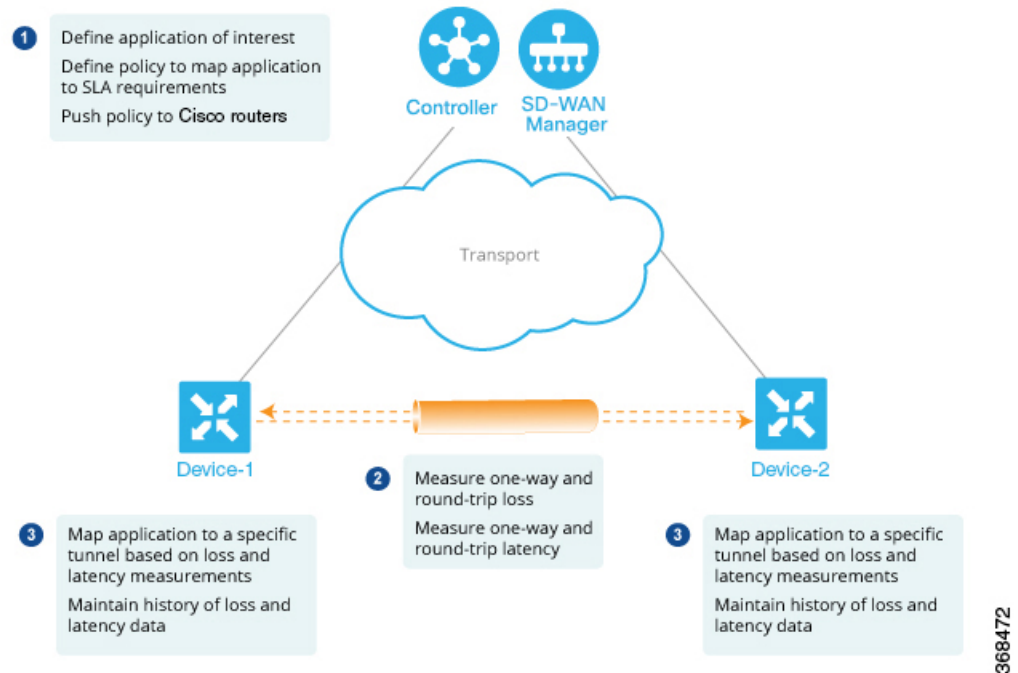
(注) Cisco vManage リリース 20.7.1 以前のリリースでは、SAIE フローはディープ パケット インスペクション (DPI) フローと呼ばれていました。

アプリケーション認識型ルーティングのコンポーネント

Cisco IOS XE Catalyst SD-WAN アプリケーション認識型ルーティングのソリューションは、次の 3 つの要素で構成されています。

- **識別**：目的のアプリケーションを定義してから、アプリケーションを特定の SLA 要件にマッピングする一元管理型データポリシーを作成します。パケットのレイヤ 3 ヘッダーとレイヤ 4 ヘッダー（送信元と宛先のプレフィックス、ポート、プロトコル、DSCP フィールドなど）を照合して、目的のデータトラフィックを選び出します。すべての一元管理型データポリシーと同様に、Cisco Catalyst SD-WAN コントローラ で設定すると、適切な Cisco IOS XE Catalyst SD-WAN デバイスに渡されます。
- **モニタリングと測定**：Cisco IOS XE Catalyst SD-WAN ソフトウェアでは BFD パケットを使用して、デバイス間のデータプレーントンネル上のデータトラフィックを継続的にモニターし、トンネルのパフォーマンス特性を定期的に測定します。パフォーマンスを測定するために、Cisco IOS XE Catalyst SD-WAN デバイスはトンネルでのトラフィック損失を探し、トンネルを通過するトラフィックの片道時間と往復時間を調べることで遅延を測定します。これらの測定値によって、最適ではないデータトラフィックの状態が示されることもあります。
- **特定のトランスポートトンネルへのアプリケーショントラフィックのマッピング**：最後の手順では、アプリケーションのデータトラフィックを、そのアプリケーションに必要なパフォーマンスを提供するデータプレーントンネルにマッピングします。マッピングの決定は、WAN 接続で実行された測定値から計算されたベストパス基準と、アプリケーション

認識型ルーティングに固有のポリシーで指定された制約という2つの基準に基づいて行われます。



レイヤ7アプリケーション自体に基づいてデータポリシーを作成するには、一元管理型データポリシーを使用して 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) フローを設定します。SAIE フローを使用すると、リモート TLOC、リモート TLOC、あるいはその両方に基づいて、トラフィックを特定のトンネルに転送できます。トンネルへのトラフィック転送は、SLA クラスに基づいて行うことはできません。



(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。

SLA クラス

表 25: 機能の履歴

機能	リリース情報	説明
SLA クラスのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	Cisco SD-WAN コントローラ で最大 8 つの SLA クラスを設 定できます。この機能を使用 すると、アプリケーション認 識型ルーティングポリシーに 追加のオプションを設定でき ます。
各ポリシーで 6 つの SLA クラ スのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	Cisco IOS XE Catalyst SD-WAN デバイスのポリシーごとに、 最大 6 つの SLA クラスを設定 できます。この機能拡張によ り、アプリケーション認識型 ルーティングポリシーに追加 のオプションを設定できま す。
SLA クラスのサポートの拡張 機能	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	Cisco IOS XE Catalyst SD-WAN デバイスで最大 16 の SLA ク ラスをサポートするための拡 張機能です。
アプリケーション認識型ルー ティングおよびデータポリ シーの SLA 優先色	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	アプリケーション認識型ルー ティングポリシーとデータポリ シーの両方が設定されてい る場合、SLA 要件を基に優先 色を選択するためのさまざま な動作を提供します。

サービスレベル契約 (SLA) は、アプリケーション認識型ルーティングで実行されるアクションを決定します。SLA クラスは、Cisco IOS XE Catalyst SD-WAN デバイスのデータプレーントンネルの最大ジッター、最大遅延、最大パケット損失、またはこれらの値の組み合わせを定義します。各データプレーントンネルは、ローカルトランスポートロケータ (TLOC) とリモート TLOC のペアで構成されます。Cisco SD-WAN コントローラの **policy sla-class** コマンド階層で SLA クラスを設定できます。Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r から、最大 8 つの SLA クラスを Cisco SD-WAN Validator で設定できます。ただし、アプリケーション認識ルートポリシーで定義できる一意の SLA クラスは 4 つだけです。Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r より前のリリースでは、最大 4 つの SLA クラスを設定できます。

Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降、Cisco IOS XE Catalyst SD-WAN デバイスのポリシーごとに最大 6 つの SLA クラスを設定できます。

SLA クラスでは、次のパラメータを設定できます。

表 26: SLA コンポーネント

説明	コマンド	値または範囲
データプレーントンネルの最大許容パケットジッター	ジッター (ミリ秒)	1 ~ 1000 ミリ秒
データプレーントンネルの最大許容パケット遅延。	遅延 (ミリ秒)	1 ~ 1000 ミリ秒
データプレーントンネルの最大許容パケット損失	損失率 (%)	1 ~ 100%

SLA サポートの機能拡張

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降、Cisco IOS XE Catalyst SD-WAN デバイスのポリシーごとに 6 つ以上の SLA クラスを設定できます。

Cisco IOS XE Catalyst SD-WAN デバイスが最大 16 の SLA クラスをサポートするには、16 GB 以上の RAM が必要です。

この機能拡張により、Cisco SD-WAN コントローラ および SD-WAN エッジデバイスでサポートされる SLA クラスの数が増加します。SLA クラスのサポートの増加により、SLA クラスをマルチプロトコル ラベル スイッチング (MPLS) ネットワーク上の IP 仮想プライベートネットワーク (IP-VPN) に合わせて、グローバルネットワークにトラフィックを転送できます。

SLA の機能拡張はマルチテナントに役立ち、テナントごとに異なる SLA クラスをプッシュできます。マルチテナント機能を使用するには、Cisco SD-WAN コントローラ が 8 つ以上の SLA クラスをサポートする必要があります。SLA クラスを異なるテナントに割り当てるには、ポリシーのグローバル制限を 64 にする必要があります。



(注) デフォルトの SLA は設定できません。デフォルトの SLA は、ユーザー定義の SLA が満たされない場合にトラフィックを転送するよう、すべてのデバイスに設定されます。

表 27: Cisco IOS XE Catalyst SD-WAN デバイスでサポートされる最大 SLA クラス数

サポートするプラットフォームとモデル	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a より前のユーザー設定可能な SLA クラス (+1 デフォルト SLA クラス)	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降のユーザー設定可能な SLA クラス (+1 デフォルト SLA クラス)
ASR 1001 HX -16GB • vedge-ASR-1001-HX	6	15

サポートするプラットフォームとモデル	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a より前の ユーザー設定可能な SLA クラス (+1 デフォルト SLA クラス)	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降のユーザー 設定可能な SLA クラス (+1 デフォルト SLA クラス)
ASR 1002 X -16GB • vedge-ASR-1002-X	6	15
ASR 1002 HX -16GB • vedge-ASR-1002-HX	6	15
ASR 1001 X -16GB • vedge-ASR-1001-X	6	15
ISR 4451 X • vedge-ISR-4451-X	6	7
ISR 4431 • vedge-ISR-4431	6	7
Catalyst 8300 エッジプラットフォーム • vedge-C8300-2N2S-6G • vedge-C8300-2N2S-4G2X • vedge-C8300-1N1S-6G • vedge-C8300-1N1S-4G2X • vedge-C8300-1N1S-6T • vedge-C8300-1N1S-4T2X • vedge-C8300-2N2S-6T • vedge-C8300-2N2S-4T2X	該当なし	7
Catalyst 8500 エッジプラットフォーム -16GB • vedge-C8500L-8S4X • vedge-C8500-12X4QC • vedge-C8500-12X	該当なし	15

サポートするプラットフォームとモデル	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a より前の ユーザー設定可能な SLA クラス (+1 デフォルト SLA クラス)	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降のユーザー設定可能な SLA クラス (+1 デフォルト SLA クラス)
その他の Cisco IOS XE Catalyst SD-WAN デバイス (C11xx、ISR1100、CSR1000v)	6	6

SLA 優先色

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降、アプリケーション認識型ルーティングポリシーとデータポリシーの両方を設定し、データフローがアプリケーションルートとデータポリシーのシーケンスに一致する場合、想定される次の動作が発生します。

- アプリケーション認識型ルーティングで設定した優先色が SLA 要件を満たし、これらの優先色にデータポリシーと共通した色が含まれる場合、他の色よりも共通の優先色が転送用に選択されます。(Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以前は、データポリシーの優先色が転送され、アプリケーション認識型ルーティングポリシーの推奨は無視されていました)。
- アプリケーション認識型ルーティングの優先色が SLA を満たしていないが、データポリシーと共通する色があり、それらの色がアプリケーション認識型ルーティングの SLA を満たしている場合、これらの色が推奨され、転送用に選択されます。
- アプリケーション認識型ルーティングで SLA を満たすトンネルまたは色がない場合は、データポリシーが推奨され、転送用に選択されます。データポリシーに優先色がある場合は、それらの色が選択されます。それ以外の場合は、データポリシーのすべての色でロードバランスが発生します。

トンネルの SLA クラスへの分類

アプリケーション認識型ルーティングのためにトンネルを 1 つ以上の SLA クラスに分類するプロセスは、次の 3 つの部分で構成されます。

- トンネルの損失、遅延、ジッター情報の測定。
- トンネルの平均損失、遅延、ジッターの計算。
- トンネルの SLA 分類の決定。

損失、遅延、ジッターの測定

オーバーレイネットワークでデータプレーントンネルが確立されると、トンネルで BFD セッションが自動的に開始されます。オーバーレイネットワークでは、各トンネルはローカル TLOC とリモート TLOC 間の特定のリンクを識別する色で識別されます。BFD セッションは、Hello

パケットを定期的に送信してリンクが動作しているかどうかを検出することで、トンネルの稼働状態をモニタリングします。アプリケーション認識型ルーティングでは、BFD Hello パケットを使用して、リンクの損失、遅延、およびジッターを測定します。

デフォルトでは、BFD Hello パケット間隔は 1 秒です。この間隔は、ユーザーが設定できます (**bfd color interval** コマンドを使用)。BFD Hello パケット間隔はトンネルごとに設定できることに注意してください。

平均損失、遅延、およびジッターの計算

BFD は、Cisco IOS XE Catalyst SD-WAN デバイス上のすべてのトンネルを定期的にポーリングして、アプリケーション認識型ルーティングで使用するパケット遅延、損失、ジッター、およびその他の統計情報を収集します。アプリケーション認識型ルーティングは、ポーリング間隔ごとに、各トンネルの平均損失、遅延、およびジッターを計算し、各トンネルの SLA を計算または再計算します。各ポーリング間隔は「パケット」とも呼ばれます。

デフォルトでは、ポーリング間隔は 10 分間です。デフォルトの BFD Hello パケット間隔が 1 秒の場合、トンネルの損失、遅延、ジッターを計算するために、1 回のポーリング間隔で約 600 個の BFD Hello パケット情報が使用されることを意味します。ポーリング間隔は、ユーザーが設定できます (**bfd app-route poll-interval** コマンドを使用)。アプリケーション認識型ルーティングのポーリング間隔は、Cisco IOS XE Catalyst SD-WAN デバイスごとに設定できることに注意してください。つまり、デバイスを起点とするすべてのトンネルに適用されるということです。

BFD Hello パケット間隔を短くせずにポーリング間隔を短くすると、損失、遅延、ジッターの計算品質に影響する可能性があります。たとえば、BFD Hello パケット間隔が 1 秒の場合にポーリング間隔を 10 秒に設定すると、トンネルの損失、遅延、ジッターの計算に 10 個の Hello パケットのみが使用されます。

各ポーリング間隔からの損失、遅延、ジッター情報は、6 回のポーリング間隔にわたって保持されます。7 回目のポーリング間隔では、最も早いポーリング間隔の情報が破棄され、最新の情報が優先されます。このように、アプリケーション認識型ルーティングでは、トンネル損失、遅延、ジッター情報のスライディングウィンドウが維持されます。

ポーリング間隔の数 (6) は、ユーザーでは設定できません。各ポーリング間隔は、**show app-route statistics** コマンドの出力のインデックス番号 (0 ~ 5) によって識別されます。

SLA 分類の決定

トンネルの SLA 分類を決定するために、アプリケーション認識型ルーティングでは、最新のポーリング間隔に応じて収集された損失、遅延、およびジッター情報を使用します。使用されるポーリング間隔の数は、乗数によって決まります。デフォルトでは、乗数は 6 であるため、すべてのポーリング間隔 (特に最後の 6 回のポーリング間隔) を通した情報を使用して分類が決定します。デフォルトのポーリング間隔が 10 分で、デフォルトの乗数が 6 の場合、各トンネルの SLA を分類するときに、直前の 1 時間に収集された損失、遅延、およびジッター情報が考慮されます。これらのデフォルト値は、トンネルの頻繁な再分類 (フラッピング) を防ぐ方法として、一種の減衰となるように選択する必要があります。

乗数はユーザーが設定できます (`bfd app-route multiplier` コマンドを使用)。アプリケーション認識型ルーティング乗数は Cisco IOS XE Catalyst SD-WAN デバイスごとに設定できることに注意してください。つまり、デバイスを起点とするすべてのトンネルに適用されるということです。

トンネル特性の変化に迅速に対応する必要がある場合は、乗数を 1 まで減らすことができます。乗数が 1 の場合、そのトンネルが 1 つ以上の SLA 基準を満たすことができるかどうかを判断するために、最新のポーリング間隔での損失と遅延の値のみが使用されます。

トンネル損失と遅延の測定と計算に基づく、各トンネルが 1 つ以上のユーザー設定の SLA クラスを満たすこともあります。たとえば、平均損失が 0 パケット、平均遅延が 10 ミリ秒のトンネルであれば、最大パケット損失が 5、最小遅延が 20 ミリ秒で定義されたクラスを満たすこととなりますが、その上、最大パケット損失 0、最小遅延が 15 ミリ秒で定義されたクラスも満たすこととなります。

トンネルが再分類される速度に関わらず、損失、遅延、およびジッター情報は継続的に測定および計算されます。アプリケーション認識型ルーティングによる変更への対応速度は、ポーリング間隔と乗数を変更することで設定できます。

クラスごとのアプリケーション認識型ルーティング

表 28: 機能の履歴

機能名	リリース情報	説明
クラスごとのアプリケーション認識型ルーティング	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能により、サービスレベル契約 (SLA) の定義に基づいてトラフィックをネクストホップアドレスに転送する機能が強化されます。この SLA 定義と、トラフィックタイプを照合および分類するポリシーを使用することで、特定の Cisco Catalyst SD-WAN トンネルを介してトラフィックを転送できます。SLA の定義は、損失、遅延、ジッターの値で構成されます。これらの値は、2 つのトランスポートローケータ (TLOC) 間に存在する Bidirectional Forwarding Detection (BFD) チャンネルを使用して測定されます。

クラスごとのアプリケーション認識型ルーティングの概要

SLA 定義は、2 つの TLOC 間に存在する BFD チャンネルを使用して測定される損失、遅延、およびジッターの値で構成されます。これらの値から、ネットワークと BFD リンクの状態がまとめて表されます。BFD 制御メッセージは、Differentiated Services Code Point (DSCP) が 48 という高プライオリティで送信されます。

高プライオリティパケットに基づく SLA メトリックには、エッジデバイスを通る実際のデータによって受信されるプライオリティが反映されません。データは、アプリケーションク

ラスに応じて、ネットワーク内で異なる DSCP 値を持つことができます。したがって、ネットワークがこのような測定を使用してトラフィックタイプを適切なトンネルに転送するには、トラフィックプロファイルの損失、遅延、およびジッターをより正確に表現する必要があります。

アプリケーション認識型ルーティングでは、アプリケーションの転送に使用できるパスを制約するポリシーを使用します。こうした制約は通常、SLA クラスに規定された、満たすべき損失、遅延、およびジッターの要件をもとに表現されます。これに沿うには、これらのメトリックを、トラフィックの宛先に向かうすべてのパスで、アクティブプローブまたはパッシブモニタリングを使用して測定する必要があります。

アクティブプローブの方法には、実際のトラフィックとともに注入される合成トラフィックの生成などがあります。この場合、プローブと実際のトラフィックが同じように転送されることが想定されます。BFD プロブ、ICMP、定期的な HTTP 要求、および IP SLA 測定は、アクティブプローブの仕組みを表す例です。Cisco Catalyst SD-WAN ソリューションでは、アクティブな測定に BFD ベースのプローブを使用します。パッシブモニタリング方式は、Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) フローを使用して、実際のトラフィックをモニタリングします。たとえば、RTP/TCP トラフィックは、損失、遅延、およびジッターを確認するためにモニタリングされます。



- (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。

アプリケーションプローブクラス

アプリケーションプローブクラス (app-probe-class) は、転送クラス、カラー、および DSCP で構成されます。これによって、転送されるアプリケーションのカラーごとのマーキングが定義されます。カラーまたは DSCP マッピングは、Cisco SD-WAN ネットワークサイトに対してローカルです。ただし、いくつかのカラーと、カラーの DSCP マッピングはサイトごとに変更されません。転送クラスによって、BFD エコー要求を出力トンネルポートでキューイングする場合の QoS キューが決まります。これは、BFD エコー要求パケットにのみ適用されます。BFD パケットの損失優先順位は低に固定されています。BFD パケットが SLA クラスで送信される場合、同じ DSCP 値が使用されます。BFD パケットが SLA クラスとともに app-probe-class を使用して送信される場合、BFD パケットは各 SLA app-probe-class に対してラウンドロビン方式で個別に送信されます。



- (注) アプリケーションルートポリシーがサイトに適用されると、そのサイトに関連するカラーのみが使用されます。Cisco IOS XE Catalyst SD-WAN デバイスは 6 つの SLA クラスをサポートしているため、app-probe-class も同様に最大 6 つまでサポートされます。

デフォルトの DSCP 値

DSCP 制御トラフィックで使用されるデフォルトの DSCP 値は 48 です。ただし、エッジデバイスで設定するオプションとともに、デフォルト値を変更するプロビジョニングがあります。すべてのネットワーク サービス プロバイダーが DSCP 48 を使用するとは限りません。

デフォルトの DSCP を持つ BFD パケットは、PMTU などの他の機能にも使用できます。デフォルト DSCP を変更すると、他の機能が変更後のデフォルト DSCP 値に影響を受けます。したがって、サービスプロバイダーが提供する、優先順位の最も高い DSCP マーキングを設定することを推奨します（通常は 48 ですが、サービスプロバイダーの SLA 契約によって異なる場合があります）。色のレベルは、グローバルレベルのデフォルト DSCP マーキングを上書きしません。

アプリケーション認識型ルーティングの設定

表 29: 機能の履歴

機能名	リリース情報	説明
IPv6 向けアプリケーション認識型ルーティング	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	これは、アプリケーション認識型ルーティング (AAR) ポリシーを設定して、IPv6 アプリケーショントラフィックで動作できるようにする機能です。

このトピックでは、アプリケーション認識型ルーティングを設定するための一般的な手順について説明します。アプリケーション認識型ルーティングポリシーによって影響を受けるトラフィックは、サービス側（ローカル/WAN 側）から Cisco IOS XE Catalyst SD-WAN デバイスのトンネル（WAN）側に流れるトラフィックのみです。

アプリケーション認識型ルーティングポリシーでは、アプリケーションを SLA と照合します。つまり、アプリケーションのデータトラフィックを送信するために必要なデータプレントネルのパフォーマンス特性と照合するということです。アプリケーション認識型ルーティングポリシーの主な目的は、Cisco IOS XE Catalyst SD-WAN デバイスによって送信されるデータトラフィックのパスを最適化することにあります。

アプリケーション認識型ルーティングポリシーは、一元管理型データポリシーの一種です。Cisco SD-WAN コントローラでポリシーを設定すると、コントローラから影響を受ける Cisco IOS XE Catalyst SD-WAN デバイスに自動的にプッシュされます。他のポリシーと同様に、アプリケーション認識型ルーティングポリシーも、一連の番号（順序）が付いたマッチ/アクションペアのシーケンスで構成されています。こうしたペアは、順番に、シーケンス番号の昇順で評価されます。データパケットがいずれかのマッチ条件にマッチすると、SLA アクションがパケットに適用され、そのパケットの送信に使用するデータプレントネルが決まります。パケットがどのポリシーシーケンスのパラメータにもマッチせず、default-action に SLA クラスが設定されていない場合、そのパケットは SLA を考慮せずに受け入れられ、転送されます。アプリケーション認識型ルーティングポリシーは、デフォルトでマッチしないトラフィックを受

け入れるようになっているため、ポジティブポリシーと見なされています。Cisco IOS XE Catalyst SD-WAN ソフトウェアの他のポリシータイプはネガティブポリシーですが、それは、デフォルトでマッチしないトラフィックをドロップするからです。

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降では、AAR ポリシーとデータポリシーを設定して、マッチアプリケーション、つまり app-list 基準に基づいて IPv6 トラフィックを制御できます。

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a 以前は、IPv6 トラフィックには、アプリケーション名またはアプリケーションリストに基づいて IPv6 トラフィックを照合し、目的のインテントに基づいて IPv6 トラフィックを誘導する機能がありませんでした。

Cisco SD-WAN Manager を使用したアプリケーション認識型ルーティングポリシーの設定

アプリケーション認識型ルーティングポリシーを設定するには、Cisco SD-WAN Manager ポリシー構成ウィザードを使用します。一元管理型ポリシーの設定に関する詳細は、「[一元管理型ポリシーの設定](#)」を参照してください。このウィザードは、次のような4つのウィンドウが順次開いて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ようになっています。

- [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、ポリシーのマッチ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。
- [トポロジの設定 (Configure Topology)] : ポリシーが適用されるネットワーク構造を作成します。トポロジ設定の詳細については、「[トポロジと VPN メンバーシップの設定](#)」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。
- [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。

ポリシー構成ウィザードの最初の3ウィンドウで、ポリシーコンポーネント、つまりブロックを作成します。最後のウィンドウで、オーバーレイネットワークのサイトと VPN にポリシーブロックを適用します。

アプリケーション認識型ルーティングポリシーを有効にするには、ポリシーをアクティブ化する必要があります。

最善のトンネルパスの設定

表 30: 機能の履歴

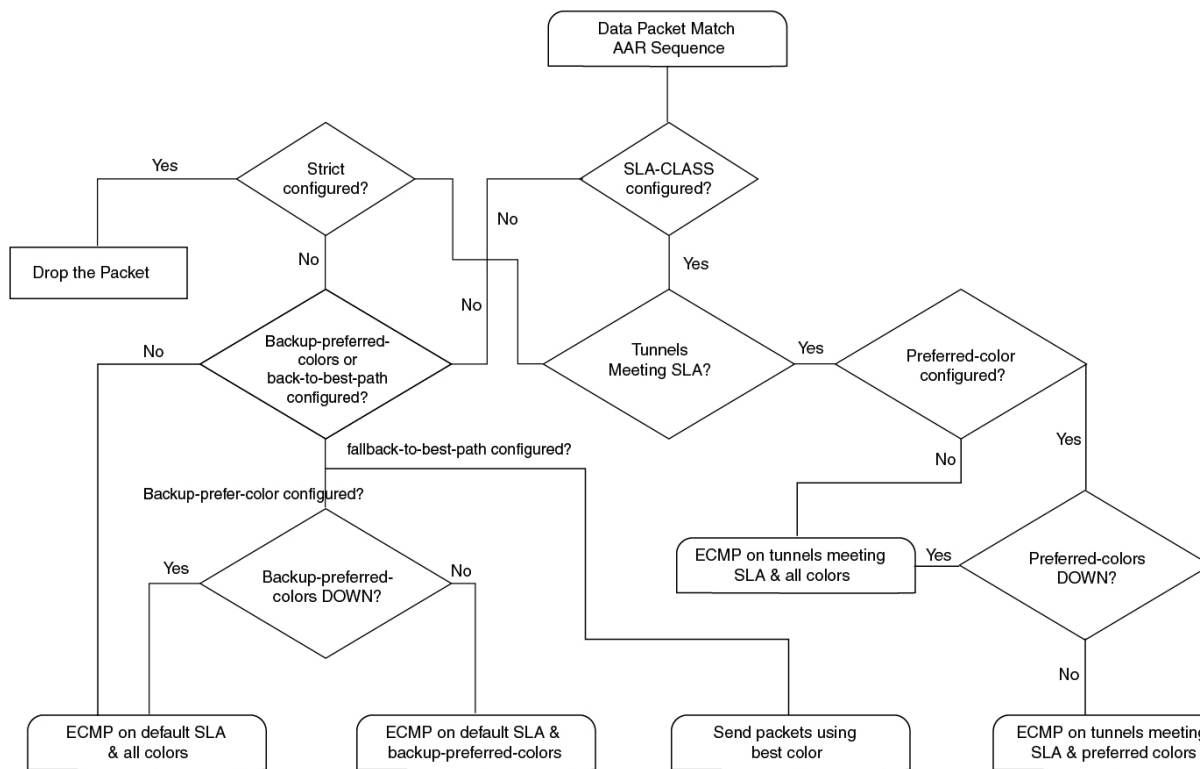
機能名	リリース情報	説明
ベストオブザワースト (最悪の中の最善、 BOW) トンネルの選 択	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリー ス 20.5.1	この機能では、使用可能な色からベストパス や色を選択する新しいポリシーアクション fallback-to-best-path を導入しています。 データトラフィックが SLA クラスの要件のい ずれも満たしていない場合、この機能により、 各 SLA クラスの [フォールバックベストトン ネル (Fallback Best Tunnel)] オプションを使用 して最適なトンネルパスの基準の順序を選 択し、パケット損失を回避できます。

最善のトンネルパスの概要

SLA が満たされていない場合にデータパケット損失を回避し、最適なアプリケーション認識型ルーティングトンネルの選択を設定するために、次のポリシーアクションを設定できます。

- **backup-preferred-color**
- **backup-preferred-color**

図 14: アプリケーション認識型ルーティングトンネル選択のフローチャート



最善のトンネルパスに向けた推奨事項

- SLA クラスを設定するときに、Cisco SD-WAN Manager で **fallback-to-best-path policy action** ポリシーアクションを設定します。
- トラフィックルールを設定するときに、Cisco SD-WAN Manager で **backup-preferred-color** ポリシーアクションを設定します。

最善のトンネルパスに向けたバリエーション設定

Cisco SD-WAN Manager では、SLA クラス要件のいずれも満たすトンネルがない場合に、ベストオブワースト（最悪の中の最善、BOW）機能を使用して最善のトンネルを検索します。

仮にSLA クラスの要件を満たすために規定されている遅延が 100 ミリ秒で、トンネル T1 の遅延が 110 ミリ秒だったとします。トンネル T2 は 111 ミリ秒、トンネル T3 は 112 ミリ秒です。

BOW ロジックによると、最善のトンネルは T1 です。T2 と T3 は、差が数ミリ秒しかないので、同じくらい良いトンネルと言えます。

SLA クラスを設定するときは、Cisco SD-WAN Manager でバリエーションを設定します。バリエーションがあると、最善のトンネル選択の一環として小さな偏差に対応できます。

詳細については、「[SLA クラスの設定 \(Configure SLA Class\)](#)」を参照してください。

例：バリエーションが設定されていない場合

時刻 t1：T1 は 100 ミリ秒、T2 は 101 ミリ秒、T3 は 102 ミリ秒

時刻 t2：T1 は 101 ミリ秒、T2 は 100 ミリ秒、T3 は 102 ミリ秒

時刻 t3：T1 は 101 ミリ秒、T2 に 112 ミリ秒、T3 に 100 ミリ秒

時刻 t1 で、最善のトンネルが T1 から T2 に変更され、時刻 t2 で、最善のトンネルが T2 から T3 に変更されます。バリエーションが設定されていないと、データベースの再プログラミングとデータトラフィックパスの変更が発生することになります。

代わりに、ミリ秒単位の小さな偏差を減衰するようにバリエーションを設定すると仮定します。

たとえば、バリエーションを 5 ミリ秒に設定すると、最善のトンネル SLA は 100 ミリ秒ということになります。範囲は 100 ~ 105 ミリ秒です。

例：バリエーションが設定されている場合

BOW(t1) = {T1, T2, T3}

BOW(t2) = {T1, T2, T3}

BOW(t3) = {T1, T2, T3}

バリエーションが設定されている場合、データベースの再プログラミングやデータトラフィックパスの変更は必要ありません。

最善のトンネルパスに向けたバリエーション設定の確認**遅延バリエーションの例**

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class video
latency 100
jitter 150
  fallback-best-tunnel latency
```

Tunnel T1: Latency: 110 msec, Loss: 0%, Jitter: 200 msec

Tunnel T2: Latency: 115 msec, Loss: 0%, Jitter: 200 msec

Tunnel T3: Latency: 120 msec, Loss: 0%, Jitter: 200 msec

遅延バリエーションがない場合、最適なトンネルは T1 です。

遅延バリエーションが 10 ミリ秒に設定されている場合、T1、T2、T3 が最適なトンネルです。

範囲は 110 ~ 120 ミリ秒です。

最適な遅延 + バリエーションは 110 ミリ秒 + 10 ミリ秒です。

次の式を使用して、遅延バリエーションに最適なトンネルを選択します。

(best_latency、best_latency + Latency_variance)

ジッターバリエーションの例

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class video
latency 100
```

```
jitter 150
  fallback-best-tunnel jitter

Tunnel T1: Latency: 90 msec, Loss: 0%, Jitter: 160 msec
Tunnel T2: Latency: 80 msec, Loss: 0%, Jitter: 200 msec
Tunnel T3: Latency: 70 msec, Loss: 0%, Jitter: 152 msec
```

ジッターバリエーションがない場合、最適なトンネルは T3 です。

ジッターバリエーションが 10 ミリ秒に設定されている場合、T1、T3 が最適なトンネルです。

範囲は 152 ~ 162 ミリ秒です。

最適なジッター + バリエーションは 152 ミリ秒 + 10 ミリ秒です。

次の式を使用して、ジッターバリエーションに最適なトンネルを選択します。

(best_jitter、best_jitter + Jitter_variance)

損失バリエーションの例

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class video
latency 100
jitter 1
  fallback-best-tunnel loss

Tunnel T1: Latency: 110 msec, Loss: 2%, Jitter: 200 msec
Tunnel T2: Latency: 115 msec, Loss: 3%, Jitter: 200 msec
Tunnel T3: Latency: 120 msec, Loss: 4%, Jitter: 200 msec
```

損失バリエーションがない場合、最適なトンネルは T1 です。

損失バリエーションが 1% に設定されている場合、T1 と T2 が最適なトンネルです。

範囲は 2% ~ 3% です。

最適な損失 + バリエーションは 2% です。

次の式を使用して、損失バリエーションに最適なトンネルを選択します。

(best_loss、best_loss + loss_variance)

SLA クラスの構成

1. Cisco SD-WAN Manager メニューから、[設定 (Configuration)] >> [ポリシー (Policies)] の順に選択します。[一元管理型ポリシー (Centralized Policy)] がデフォルトで選択され、表示されます。
2. [Add Policy] をクリックします。
3. 対象グループの作成ページの左側のペインで、[SLA クラス (SLA Class)] をクリックし、[新規 SLA クラスリスト (New SLA Class List)] をクリックします。
4. [SLA クラスリスト名 (SLA Class List Name)] フィールドに、SLA クラスリストの名前を入力します。
5. SLA クラスのパラメータを定義します。

1. [損失 (Loss)]フィールドに、接続の最大パケット損失を 0 ～ 100% の値で入力します。
2. [遅延 ([Latency)]フィールドに、接続での最大パケット遅延を 1 ～ 1,000 ミリ秒の値で入力します。
3. [ジッター (Jitter)]フィールドに、接続の最大ジッターを 1 ～ 1,000 ミリ秒の値で入力します。
4. [アプリケーションプローブクラス (App Probe Class)]ドロップダウンリストから必要なアプリケーションプローブクラスを選択します。
6. (オプション) [フォールバックのベストトンネル (Fallback Best Tunnel)]チェックボックスをオンにして、ベストトンネルの基準を有効にします。

このオプションフィールドは、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a から利用できるため、SLA が満たされていない場合に、使用可能なカラーからベストパスまたはカラーを選択できます。このオプションを選択すると、ドロップダウンから必要な基準を選択できます。基準には、損失、遅延、およびジッターの値を 1 つ以上組み合わせます。
7. ドロップダウンリストから[基準 (Criteria)]を選択します。使用可能な基準は次のとおりです。
 - なし
 - 遅延
 - 損失
 - Jitter
 - 遅延、損失
 - 遅延、ジッター
 - 損失、遅延
 - 損失、ジッター
 - ジッター、遅延
 - ジッター、損失
 - 遅延、損失、ジッター
 - 遅延、ジッター、損失
 - 損失、遅延、ジッター
 - 損失、ジッター、遅延
 - ジッター、遅延、損失
 - ジッター、損失、遅延

8. (オプション) 選択した基準の損失バリエーション (%)、遅延バリエーション (ミリ秒)、およびジッターバリエーション (ミリ秒) を入力します。
詳細については、「[最善のトンネルパスに向けたバリエーション設定](#)」を参照してください。
9. [Add] をクリックします。

トラフィックルールの設定

アプリケーション認識型ルーティングポリシーを設定するには、次の手順を実行します。

1. [アプリケーション認識型ルーティング (Application Aware Routing)] をクリックします。
2. [ポリシーの追加 (Add Policy)] ドロップダウンリストから、[新規作成 (Create New)] を選択します。
3. [シーケンスタイプ (Sequence Type)] をクリックします。アプリケーションルートテキスト文字列を含むポリシーシーケンスが左側のペインに追加されます。
4. アプリケーションルートのテキスト文字列をダブルクリックし、ポリシーシーケンスの名前を入力します。ポリシーシーケンスは、コピー、削除、名前の変更ができます。入力した名前は、左側のペインと右側のペインの両方の [シーケンスタイプ (Sequence Type)] リストに表示されます。
5. 右側のペインで、[シーケンスルール (Sequence Rule)] をクリックします。[マッチ/アクション (Match/Actions)] ダイアログボックスを開くと、デフォルトで [マッチ (Match)] が選択されます。使用可能なポリシーマッチ条件は、ダイアログボックスの下に一覧表示されます。
6. [プロトコル (Protocol)] ドロップダウンリストで、次のいずれかのオプションを選択します。
 - IPv4
 - IPv6
 - Both



(注) 選択したプロトコルに応じて、[マッチ (Match)] または [アクション (Match)] の条件が異なる場合があります。

7. 1つ以上の [マッチ (Match)] 条件をクリックして選択します。次の表の説明に従って値を設定します。

表 31 : Match Conditions

一致条件	手順

なし (すべてのパケットに一致)	マッチ条件を指定しないでください。
アプリケーション/アプリケーションファミリリスト (Application/Application Family List)	<p>[アプリケーション/アプリケーションファミリリスト (Application/Application Family List)] をクリックし、アプリケーションリストを選択します。</p> <p>このマッチ条件は、Cisco IOS XE リリース17.9.1a および Cisco vManage リリース20.9.1 以降の IPv6 トラフィックで使用できます。</p>
クラウド SaaS アプリケーションリスト (Cloud SaaS Application List)	<p>Cisco SD-WAN Manager では、Cisco Catalyst SD-WAN Cloud OnRamp for SaaS が各 Software as a Service (SaaS) アプリケーションのベストパスの選択を決定するために使用できるクラウドアプリケーションのリストが提供されます。</p> <p>Cisco Catalyst SD-WAN Cloud OnRamp for SaaS の詳細については、『Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.x』を参照してください。</p> <p>(注) [プロトコル (Protocol)] オプションとして [IPv4] を指定すると、[クラウドSaaSアプリケーションリスト (Cloud SaaS Application List)] がマッチ条件として表示されます。</p> <p>ドロップダウンリストで、[SaaS アプリケーション (SaaS application)] を選択します。</p>
DNS アプリケーションリスト (DNS Application List)	<p>ドロップダウンリストで、[アプリケーションファミリ (application family)] を選択します。</p> <p>このマッチ条件は、Cisco IOS XE リリース17.9.1a および Cisco vManage リリース20.9.1 以降の IPv6 トラフィックで使用できます。</p>
Destination Data Prefix	<p>宛先プレフィックスのリストと照合するには、ドロップダウンリストから該当するリストを選択します。</p> <p>個々の宛先プレフィックスと照合するには、[宛先 (Destination)] ダイアログボックスにプレフィックスを入力します。</p>

Destination Region (宛先リージョン)	<p>Cisco Catalyst SD-WAN マルチリージョンファブリックを使用して、Cisco Catalyst SD-WAN ネットワークの [宛先リージョン (Destination Region)] を使用できます。</p> <p>ドロップダウンリストから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> • [プライマリ (Primary)] : 宛先サイトが送信元と同じプライマリリージョン (アクセスリージョン) 内にある場合にトラフィックを照合します。 • [セカンダリ (Secondary)] : 宛先サイトが送信元と同じプライマリリージョン内にはないが、送信元と同じセカンダリリージョン内にある場合にトラフィックを照合します。このトラフィックは、セカンダリリージョンで説明されているように、ダイレクトトンネルを使用して宛先に到達できます。 • [その他 (Other)] : 宛先サイトが送信元と同じプライマリリージョン内にもセカンダリリージョン内にもない場合にトラフィックを照合します。このトラフィックには、送信元から宛先へのマルチホップパスが必要です。 <p>マルチリージョンファブリックの設定方法の詳細については、『<i>Cisco Catalyst SD-WAN Multi-Region Fabric</i> (および <i>Hierarchical SD-WAN Configuration Guide</i>)] を参照してください。</p>
宛先ポート	<p>ポート番号を入力します。単一のポート番号、ポート番号のリスト (スペースで区切られた番号)、またはポート番号の範囲 (ハイフン [-] で区切られた2つの番号) を指定します。</p>
トラフィック転送先 (Traffic To)	<p>マルチリージョンファブリックの境界ルータ用のデータポリシーまたはアプリケーション認識型ポリシーを作成する場合、一致基準を使用して、アクセスリージョン、コアリージョン、またはサービスVPNに流れるトラフィックを照合できます。</p>
DNS (スプリット DNS を有効にする場合)	<p>DNS アプリケーションの DNS 要求を処理するには、ドロップダウンリストで [要求 (Request)] を選択し、アプリケーションの DNS 応答を処理するには [応答 (Response)] を選択します。</p>
[DSCP]	<p>DSCP 値を 0 ~ 63 の数値で入力します。</p>
PLP	<p>[低 (Low)] または [高 (High)] を選択します。PLP を [高 (High)] に設定するには、[注釈超過 (exceed remark)] オプションのあるポリシーを適用します。</p>

Protocol	インターネットプロトコル番号を 0 ～ 255 の数字で入力します。
ICMP Message	<p>プロトコル (IPv4) の場合、[マッチ条件 (Match Conditions)] セクションの[プロトコル (Protocol)] フィールドの値を 1 にすると、[ICMPメッセージ (ICMP Message)] フィールドが表示され、データポリシーに適用する ICMP メッセージを選択できます。</p> <p>プロトコル (IPv6) の場合、[マッチ条件 (Match Conditions)] セクションの[プロトコル (Protocol)] フィールドの値を 58 にすると、[ICMPメッセージ (ICMP Message)] フィールドが表示され、データポリシーに適用する ICMP メッセージを選択できます。</p> <p>(注) このフィールドは、Cisco IOS XE リリース 17.4.1 または Cisco SD-WAN リリース 20.4.1、および Cisco vManage リリース 20.4.1 以降で使用できます。</p> <p>[プロトコル (Protocol)] で [両方 (Both)] を選択すると場合、[ICMPメッセージ (ICMP Message)] または [ICMPv6メッセージ (ICMPv6 Message)] フィールドが表示されます。</p>
Source Data Prefix	<p>送信元プレフィックスのリストと照合するには、ドロップダウンリストから該当するリストを選択します。</p> <p>個々の送信元プレフィックスと照合するには、[送信元 (Source)] フィールドにプレフィックスを入力します。</p>
送信元ポート	ポート番号を入力します。単一のポート番号、ポート番号のリスト (スペースで区切られた番号)、またはポート番号の範囲 (ハイフン [-] で区切られた 2 つの番号) を指定します。

8. 条件が一致したデータトラフィックのアクションを選択するには、[アクション (Actions)] をクリックします。次の表の説明に従って値を設定します。

表 32: アクション

アクション	手順
バックアップ SLA の優先カラー	[バックアップ SLA の優先カラー (Backup SLA Preferred Color)] のマッチ条件のポリシーアクションを設定します。SLA に一致するトンネルがない場合は、データトラフィックを特定のトンネルに転送します。そのトンネルインターフェイスが使用できる場合、データトラフィックは設定されたトンネルから送信されます。そのトンネルインターフェイスが使用できない場合、トラフィックは別の使用可能なトンネルに送信されます。1 つ以上の色を指定できます。バックアップ SLA の優先カラーは、厳密なマッチ条件ではなく、緩いマッチ条件です。

アクション	手順
カウンタ	<p>[カウンタ (Counter)] のマッチ条件のポリシーアクションを設定します。</p> <p>[カウンタ (Counter)] をクリックします。</p> <p>[カウンタ名 (Counter Name)] フィールドに、パケットカウンタを保存するファイルの名前を入力します。</p>
Log	<p>SLA クラスルールに一致するパケットのサンプルセットをシステムログ (syslog) ファイルに配置できます。パケットヘッダーが最初にログに記録される際、パケットヘッダーのログの他に、syslog メッセージが生成されます。その後もフローがアクティブである限り、5分ごとに生成されます。</p> <p>ロギングを有効にするには、[ログ (Log)] をクリックします。</p>

アクション	手順
SLA クラスリスト	<p>[SLAクラスリスト (SLA Class List)] のマッチ条件のポリシーアクションを設定します。SLA クラスの場合、条件が一致するすべてのデータトラフィックは、クラスで定義された SLA パラメータとパフォーマンスが一致するトンネルに送信されます。デバイスは、最初に SLA に一致するトンネルを介してトラフィックを送信しようとしています。単一のトンネルが SLA に一致する場合、データトラフィックはそのトンネルを介して送信されます。2つ以上のトンネルが一致する場合、トラフィックはトンネル間で分散されます。SLA に一致するトンネルがない場合、データトラフィックは使用可能なトンネルの1つを介して送信されます。</p> <p>[SLA Class List] をクリックします。</p> <p>[SLAクラス (SLA Class)] ドロップダウンリストで、1つ以上の SLA クラスを選択します。</p> <p>[優先カラー (Preferred Color)] が選択されていない場合、必要に応じて、[優先カラーグループ (Preferred Color Group)] ドロップダウンリストから優先カラーグループを選択できます。優先するデータプレーントンネルの優先カラーグループを選択します。カラーまたはパスの設定に基づいて、最大3段階の優先順位を設定できます。このフィールドは、Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降で使用できます。</p> <p>必要に応じて、[優先カラー (Preferred Color)] ドロップダウンリストで、優先するデータプレーントンネルの色を選択します。トラフィックは、すべてのトンネル間でロードバランシングされます。SLA に一致するトンネルがない場合、データトラフィックは使用可能ないずれかのトンネルを介して送信されます。つまり、カラーの設定は厳密な一致ではなく緩い一致です。</p> <p>SLA クラスの厳密な照合を実行するには、[厳密/ドロップ (Strict/Drop)] をクリックします。SLA 基準を満たすデータプレーントンネルがない場合、トラフィックはドロップされます。</p> <p>パケットドロップを回避するには、[ベストパスへのフォールバック (Fallback to best path)] をクリックして利用可能で最適なトンネルを選択します。</p> <p>(注) [ベストパスへのフォールバック (Fallback to best path)] オプションは、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a および Cisco SD-WAN リリース 20.5.1 以降で使用できます。</p> <p>SLA クラスの定義中に、[フォールバックのベストトンネル (Fallback Best Tunnel)] オプションが有効になっている場合にのみ、[ベストパスへのフォールバック (Fallback to best path)] アクションを選択できます。[フォールバックのベストトンネル (Fallback Best Tunnel)] オプションが有効になっていない場合、次のエラーメッセージが Cisco SD-WAN Manager に表示されます。</p> <p>SLA Class selected, does not have Fallback Best Tunnel enabled. Please change the SLA class or change to Strict/Drop.</p> <p>すべてのトンネル間でトラフィックの負荷を分散するには、[ロードバランス (Load Balance)] をクリックします。</p>
クラウド SLA	<p>クラウド SLA により、トラフィックは Cisco Catalyst SD-WAN Cloud OnRamp for SaaS で最適なパス選択を使用できます。</p> <p>[クラウドSLA (Cloud SLA)] をクリックします。</p>

9. [Save Match and Actions] をクリックします。
10. 必要に応じて、追加のシーケンスルールを作成します。ルールをドラッグアンドドロップして再配置します。
11. [アプリケーション認識型ルーティングポリシーの保存 (Save Application Aware Routing Policy)] をクリックします。
12. [次へ (Next)] をクリックして、ウィザードの [サイトとVPNにポリシーを適用 (Apply Policies to Sites and VPNs)] に移動します。

アプリケーション認識型ルーティングポリシーのデフォルトアクション

マッチ条件のいずれにもマッチしないパケットをどう処理するかは、ポリシーのデフォルトアクションで定義します。アプリケーション認識型ルーティングポリシーの場合、デフォルトアクションを設定しないと、すべてのデータパケットは通常のルーティング決定に基づいて受け入れられ、送信されます。SLA は考慮されません。

この動作を変更するには、**default-action sla-class *sla-class-name*** コマンドをポリシーに含め、**policy sla-class** コマンドで定義した SLA クラスの名前を指定します。

ポリシーのデフォルトアクションで SLA クラスを適用する場合、**strict** オプションは指定できません。

デフォルトアクションで SLA クラスを満たすデータプレーントンネルがない場合、Cisco IOS XE Catalyst SD-WAN デバイスは、等しいパス間でロードバランシングを実行することによって、使用可能なトンネルの 1 つを選択します。

データフローが AAR ポリシーとデータポリシーの両方にマッチする場合の予想される動作は以下になります。

1. データポリシーのローカル TLOC アクションが設定されている場合、**App-route preferred-color** および **backup-preferred-color** アクションが無視されます。
2. **sla-class** および **sla-strict** アクションは、アプリケーションルーティング設定として維持されます。
3. データポリシーの TLOC が優先されます。

local-tloc-list アクションがあり、複数のオプションが含まれている場合は、SLA を満たすローカル TLOC を選択します。

- SLA を満たす **local-tloc** がない場合は、**local-tloc-list** を介したトラフィックに等コストマルチパス (ECMP) ルーティングを選択します。
- どの **local-tloc** も稼働していない場合は、稼働している TLOC を選択します。
- どの **local-tloc** も稼働しておらず、データポリシーが制限モードで設定されている場合は、トラフィックをドロップします。

Cisco Catalyst SD-WAN Manager を介したアプリケーション プロブ クラスの設定

1. Cisco SD-WAN Manager メニューから、[**Configuration**] > [**Policies**] の順に選択します。
2. [一元管理型ポリシー (Centralized Policy)] で、[ポリシーの追加 (Add Policy)] をクリックします。[対象グループの作成 (Create Groups of Interest)] ページが表示されます。
3. 左側のナビゲーションパネルからリストタイプ [アプリケーション プロブ クラス (App Probe Class)] を選択して、対象グループを作成します。
4. [新しいアプリケーション プロブ クラス (New App Probe Class)] をクリックします。
5. [プローブクラス名 (Prob Class Name)] フィールドにプローブクラス名を入力します。
6. [転送クラス (Forwarding Class)] ドロップダウンリストから必要な転送クラスを選択します。

転送クラスがない場合は、[カスタム オプション (Custom Options)] メニューの [ローカライズ型ポリシーリスト (Localized Policy Lists)] の下にある [クラスマップ (Class Map)] リストページからクラスを作成します。

転送クラスを作成するには、次の手順を実行します。

1. [カスタムオプション (Custom Options)] ドロップダウンで、[ローカライズ型ポリシー (Localized Policy)] オプションから [リスト (Lists)] を選択します。
2. [リストの定義 (Define Lists)] ウィンドウで、左側のナビゲーションパネルからリストタイプとして [クラスマップ (Class Map)] を選択します。
3. [新しいクラスリスト (New Class List)] をクリックして新しいリストを作成します。
4. クラスを入力して、ドロップダウンリストから [キュー (Queue)] を選択します。
5. [Save] をクリックします。
7. [エン트리 (Entries)] ペインで、[カラー (Color)] ドロップダウンリストから適切なカラーを選択し、**DSCP** 値を入力します。
[+] 記号をクリックして、必要に応じてエントリを追加します。
8. [Save] をクリックします。

SLA クラスへのアプリケーション プロブ クラスの追加

1. 左側のペインから、[SLAクラス (SLA Class)] を選択します。
2. [新しいSLAクラスのリスト (New SLA Class List)] をクリックします。
3. [SLA クラスリスト名 (SLA Class List Name)] フィールドに、SLA クラスリストの名前を入力します。

4. 必要な損失（%）、遅延（ミリ秒）、ジッター（ミリ秒）を入力します。
5. [アプリケーションプローブクラス（App Probe Class）] ドロップダウンリストから必要なアプリケーションプローブクラスを選択します。
6. [Add]をクリックします。
損失、遅延、ジッター、アプリケーションプローブクラスで作成された新しい SLA クラスがテーブルに追加されます。

Cisco BFD テンプレートでのデフォルト DSCP の設定

1. Cisco SD-WAN Manager メニューから、[Configuration]>[Templates]の順に選択します。
2. [Feature Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. 左側のペインのデバイスリストから、デバイスを選択します。
5. 右側のペインで、[基本情報（Basic Information）]の下にリストされている BFD テンプレートを選択します。
6. それぞれのフィールドに [テンプレート名（Template Name）] と [説明（Description）] を入力します。
7. [基本設定（Basic Configuration）] ペインで、[乗数（Multiplier）] と [ポーリング間隔（ミリ秒）（Poll Interval (milliseconds)）] を入力します。
8. [BFDパケットのデフォルトDSCP値（Default DSCP value for BFD Packets）] フィールドに、必要なデバイス固有の値を入力するか、DSCP のデフォルト値を選択します。
9. (オプション) [色（Color）] ペインで、ドロップダウンリストから必要な色を選択します。
10. 必要な [Hello間隔（ミリ秒）（Hello Interval (milliseconds)）] と [乗数（Multiplier）] を入力します。
11. [パスMTUディスカバリ（Path MTU Discovery）] 値を選択します。
12. [TLOCカラーのBFDデフォルトDSCP値（BFD Default DSCP value for tloc color）] を入力します。
13. [Add]をクリックします。
デフォルトの DSCP 値と色の値は、BFD テンプレートで設定されます。

サイトと VPN へのポリシーの適用

ポリシー構成ウィザードの最後のウィンドウで、前の3つのウィンドウで作成したポリシーブロックを VPN およびオーバーレイネットワーク内のサイトに関連付けます。

オーバーレイネットワークのサイトと VPN にポリシーブロックを適用するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Policies]** の順に選択します。
[一元管理型ポリシー (Centralized Policy)] がデフォルトで選択され、表示されます。
2. **[Add Policy]** をクリックします。[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)] ページが表示されます。
3. **[Next]** をクリックします。[ネットワークトポロジ (Network Topology)] ウィンドウが開きます。[トポロジ (Topology)] バーで、[トポロジ (Topology)] がデフォルトで選択されています。
4. **[Next]** をクリックします。[トラフィックルールの設定 (Configure Traffic Rules)] ウィンドウが開きます。[アプリケーション認識型ルーティング (Application-Aware Routing)] バーで、[アプリケーション認識型ルーティング (Application-Aware Routing)] がデフォルトで選択されています。
5. **[Next]** をクリックします。[サイトと VPN にポリシーを適用 (Apply Policies to Sites and VPNs)] ウィンドウが開きます。
6. [ポリシー名 (Policy Name)] フィールドに、ポリシーの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0～9の数字、ハイフン (-)、下線 (_) のみです。スペースやその他の文字を含めることはできません。
7. [ポリシーの説明 (Policy Description)] フィールドに、ポリシーの説明を入力します。最大2048文字を使用できます。このフィールドは必須であり、任意の文字とスペースを含めることができます。
8. [トポロジ (Topology)] バーから、ポリシーブロックのタイプを選択します。表には、そのタイプのポリシーブロック用に作成したポリシーが一覧表示されます。
9. [新しいサイトリストを追加 (Add New Site List)] と [VPN リスト (VPN list)] をクリックします。1つ以上のサイトリストを選択し、1つ以上の VPN リストを選択します。
[Add] をクリックします。
10. [プレビュー (Preview)] をクリックして、設定されたポリシーを表示します。ポリシーは CLI 形式で表示されます。
11. **[Save Policy]** をクリックします。**[設定 (Configuration)] > [ポリシー (Policies)]** を選択すると、ポリシーテーブルに新しく作成されたポリシーが表示されます。

アプリケーション認識型ルートポリシーを有効にするには、次のようにオーバーレイネットワーク内のサイトのリストに適用します。

```
vSmart(config)# apply-policy site-list list-name app-route-policy policy-name
```

ポリシーを適用する場合は、（インバウンドまたはアウトバウンドのいずれであれ）方向は指定しません。アプリケーション認識型ルーティングポリシーは、Cisco IOS XE Catalyst SD-WAN デバイスのアウトバウンドトラフィックにのみ影響します。

apply-policy コマンドで適用するすべての **app-route-policy** ポリシーについて、すべてのサイトリストのサイト ID は一意である必要があります。つまり、サイトリストに重複するサイト ID が含まれてはなりません。重複するサイト ID の例には、2つのサイトリスト **site-list 1**、**site-id 1-100**、および **site-list 2 site-id 70-130** のサイト ID があります。ここでは、サイト 70 ~ 100 が両方のリストに含まれています。これらの2つのサイトリストを2つの異なる **app-route-policy** ポリシーに適用すると、Cisco Catalyst SD-WAN コントローラで設定をコミットする試みが失敗します。

同じタイプの制限は、次のポリシーのタイプにも適用されます。

- 一元管理型制御ポリシー (**control-policy**)
- 一元管理型データポリシー (**data-policy**)
- cflowd フローモニタリングに使用される一元管理型データポリシー (**cflowd** アクションを含む **data-policy** および **cflowd-template** コマンドを含む **apply-policy**)

ただし、異なるタイプのポリシーに適用するサイトリストのサイト ID は重複させることができます。たとえば、**app-route-policy** ポリシーと **data-policy** ポリシーのサイトリストでは、サイト ID が重複している可能性があります。したがって、上記2つのサイトリストの例 (**site-list 1**、**site-id 1-100**、および **site-list 2 site-id 70-130**) では、1つを制御ポリシーに、もう1つをデータポリシーに適用できます。

Cisco Catalyst SD-WAN コントローラで **commit** コマンドを発行して設定を正常にアクティブ化すると、コントローラは指定されたサイトの Cisco IOS XE Catalyst SD-WAN デバイスにアプリケーション認識型ルーティングポリシーをプッシュします。

Cisco Catalyst SD-WAN コントローラで設定されたポリシーを表示するには、コントローラで **show running-config** コマンドを使用します。

Cisco Catalyst SD-WAN コントローラがデバイスにプッシュしたポリシーを表示するには、ルータで **show policy from-vsmart** コマンドを発行します。

デバイスで実行されているアプリケーション認識型アプリケーションのフロー情報を表示するには、ルータで **show app dpi flow** コマンドを発行します。

アプリケーション認識型ルーティングポリシーを他のデータポリシーと組み合わせて適用する方法

Cisco IOS XE Catalyst SD-WAN デバイスにアプリケーション認識型ルーティングポリシーと他のポリシーを設定すると、そうしたポリシーはデータトラフィックに順次適用されます。

Cisco IOS XE Catalyst SD-WAN デバイスでは、次のタイプのデータポリシーを設定できます。

- 一元管理型データポリシー。Cisco Catalyst SD-WAN コントローラでこのポリシーを設定すると、ポリシーはデバイスに渡されます。 **policy data-policy configuration** コマンドを使

用して設定を定義したら、**apply-policy site-list data-policy** または **apply-policy site-list vpn-membership** コマンドを使用して適用します。

- ローカライズ型データポリシー。一般にアクセスリストと呼ばれます。デバイスでアクセスリストを設定するには、**policy access-list** 構成コマンドを使用します。VPN 内で **vpn interface access-list in** 構成コマンドを使用してインバウンドインターフェイスに適用するか、**vpn interface access-list out** コマンドを使用してアウトバウンドインターフェイスに適用します。
- アプリケーション認識型ルーティングポリシー。アプリケーション認識型ルーティングポリシーによって影響を受けるトラフィックは、Cisco IOS XE Catalyst SD-WAN デバイスのサービス側（ローカル/LAN 側）からトンネル（WAN）側に流れるトラフィックのみです。アプリケーション認識型ルーティングポリシーを **policy app-route-policy** 構成コマンドを使用して Cisco Catalyst SD-WAN コントローラ で設定し、**apply-policy site-list app-route-policy** コマンドを使用して適用します。設定をコミットすると、ポリシーが該当するデバイスに渡されます。次に、デバイス上のマッチするデータトラフィックが、設定された SLA 条件に従って処理されます。このポリシーの結果としてドロップされないデータトラフィックは、データポリシーに渡されて評価を受けます。データトラフィックがマッチせず、デフォルトアクションが何も設定されていない場合は、SLA を考慮せずにそのデータトラフィックが送信されます。

オーバーレイネットワーク内の単一サイトに適用できるのは、データポリシー 1 つとアプリケーション認識型ルーティングポリシー 1 つのみです。設定で複数のサイトリストを定義して適用する場合は、単一のデータポリシーまたは単一のアプリケーション認識型ルーティングポリシーが複数のサイトに適用されないようにする必要があります。CLI はこうした状況になっていないかチェックせず、**validate** 構成コマンドは、同じタイプの複数のポリシーが単一のサイトに適用されているかどうかを検出しません。

ルータのサービス側からルータの WAN 側に流れるデータトラフィックの場合、ポリシーによるトラフィック評価は次の順序で行われます。

1. LAN インターフェイスで入力アクセスリストを適用。このアクセスリストの結果としてドロップされないデータトラフィックは、アプリケーション認識型ルーティングポリシーに渡されて評価されます。
2. アプリケーション認識型ルーティングポリシーを適用。このポリシーの結果としてドロップされないデータトラフィックは、データポリシーに渡されて評価を受けます。データトラフィックがマッチせず、デフォルトアクションが何も設定されていない場合は、SLA を考慮せずにそのデータトラフィックが送信されます。
3. 一元管理型データポリシーを適用。入力アクセスリストの結果としてドロップされなかったデータトラフィックは、出力アクセスリストに渡されて評価されます。
4. WAN インターフェイスで出力アクセスリストを適用。出力アクセスリストの結果としてドロップされなかったデータトラフィックは、WAN インターフェイスから送信されます。

WAN からルータを経由してサービス側 LAN に流入するデータトラフィックの場合、ポリシーによるトラフィック評価は次の順序で行われます。

1. WAN インターフェイスで入力アクセスリストを適用。入力アクセスリストの結果としてドロップされなかったデータトラフィックは、データポリシーに渡されて評価されます。
2. データポリシーを適用。入力アクセスリストの結果としてドロップされなかったデータトラフィックは、出力アクセスリストに渡されて評価されます。
3. LAN インターフェイスで出力アクセスリストを適用。出力アクセスリストの結果としてドロップされなかったデータトラフィックは、ローカルサイトの宛先に向けてLAN インターフェイスから送信されます。

前述のように、アプリケーション認識型ルーティングポリシーは、Cisco IOS XE Catalyst SD-WAN デバイスのサービス側（ローカル/LAN 側）からトンネル（WAN）側に流れるトラフィックにのみ影響するため、WAN から流入するデータトラフィックはアクセスリストとデータポリシーによってのみ処理されます。



- (注) アプリケーション認識型ルーティングとデータポリシーの両方が設定されている場合、データポリシールールに DNS リダイレクト、ネクストホップ、セキュアインターネットゲートウェイ、NAT VPN、またはサービスなどのアクションが含まれていると、それらのルールにマッチするトラフィックは AAR ポリシーをスキップします。たとえそのトラフィックが、AAR ポリシーで定義されたルールにマッチしていたとしてもです。データポリシーアクションは、AAR ルールをオーバーライドします。

アプリケーション認識型ルーティングポリシーのアクティブ化

ポリシーをアクティブ化するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Policies]** の順に選択します。[一元管理型ポリシー (Centralized Policy)] がデフォルトで選択され、表示されます。
2. 目的のポリシーについて、[...] をクリックし、[アクティブ化 (Activate)] を選択します。[ポリシーのアクティブ化 (Activate Policy)] ポップアップが開きます。ポリシーが適用される到達可能な Cisco SD-WAN コントローラの IP アドレスが一覧表示されます。
3. [Activate] をクリックします。

アプリケーション認識型ルーティングポリシーをアクティブ化すると、接続されているすべての Cisco SD-WAN コントローラにポリシーが送信されます。

データプレーントンネルのパフォーマンスのモニター

Bidirectional Forwarding Detection (BFD) プロトコルは、Cisco IOS XE Catalyst SD-WAN デバイス間のすべてのデータプレーントンネルで実行され、トンネルの稼働状態、ネットワークおよびパスの特性をモニタリングします。アプリケーション認識型ルーティングは、BFD によって収集された情報を使用して、トンネルの伝送パフォーマンスを決定します。パフォーマンスは、トンネル上のパケット遅延とパケット損失の観点から報告されます。

BFDは定期的にHelloパケットを送信し、データプレーントンネルの稼働状態をテストして、トンネルの障害をチェックします。これらのHelloパケットは、トンネル上のパケット損失とパケット遅延の測定値を提供します。Cisco IOS XE Catalyst SD-WAN デバイスは、時間のスライディングウィンドウにわたってパケット損失と遅延の統計情報を記録します。BFDは、直近の6つのスライディングウィンドウの統計を追跡し、各統計セットを別々のバケットに配置します。デバイスにアプリケーション認識型ルーティングポリシーを設定する場合、ルータはこれらの統計情報を使用して、データプレーントンネルのパフォーマンスがポリシーのSLAの要件に一致するかどうかを判断します。

スライディングウィンドウのサイズは次のパラメータで決定します。

パラメータ	デフォルト	コンフィギュレーション コマンド	範囲
BFD Hello パケット間隔	1 秒	bfd color color hello-interval seconds	1 ~ 65535 秒
アプリケーション認識型ルーティングのポーリング間隔	10 分 (600,000 ミリ秒)	bfd app-route poll-interval milliseconds	1 ~ 4,294,967 (2 ³² - 1) ミリ秒
アプリケーション認識型ルーティングの乗数	6	bfd app-route multiplier number	1 ~ 6

これらのパラメータのデフォルト値を使用して、アプリケーション認識型ルーティングの動作について説明します。

- スライディングウィンドウの期間ごとに、アプリケーション認識型ルーティングは600個のBFD Helloパケットを確認します (BFD Hello 間隔 x ポーリング間隔 : 1 秒 x 600 秒 = 600 Hello パケット)。これらのパケットは、データプレーントンネルでのパケット損失と遅延の測定値を提供します。
- アプリケーション認識型ルーティングでは、統計情報が1時間保持されます (ポーリング間隔 x 乗数 : 10 分 x 6 = 60 分)。
- 統計情報は、0 ~ 5 の番号でインデックスが付けられた6つのバケットにそれぞれ配置されます。バケット0には最新の統計情報が、バケット5には最も古い統計情報が配置されます。10分ごとに、最新の統計情報がバケット0に配置されます。またバケット5の統計情報が破棄され、残りの統計情報が次のバケットに移動します。
- 60分ごと (1時間ごと) に、アプリケーション認識型ルーティングが損失と遅延の統計情報に基づいて動作します。すべてのスライディングウィンドウのすべてのバケットの損失および遅延の平均を計算し、この値をトンネルの指定されたSLAと比較します。計算された値がSLAを満たす場合、アプリケーション認識型ルーティングは何も行いません。値がSLAを満たさない場合、アプリケーション認識型ルーティングは新しいトンネルを計算します。
- アプリケーション認識型ルーティングは、6つのバケットすべての値を使用して、データトンネルの平均損失と遅延を計算します。これは、乗数が6であるためです。アプリケーション認識は常に6つのデータバケットを保持しますが、損失と遅延を計算するために実

際に使用する数は、乗数によって決まります。たとえば、乗数が 3 の場合、バケット 0、1、2 が使用されます。

これらのデフォルト値は 1 時間ごとにしかアクションを実行しないため、安定したネットワークに適しています。ネットワーク障害をより迅速にキャプチャして、アプリケーション認識型ルーティングが新しいトンネルをより頻繁に計算できるようにするには、これら 3 つのパラメータの値を調整します。たとえば、ポーリング間隔だけを 1 分 (60,000 ミリ秒) に変更した場合、アプリケーション認識型ルーティングはトンネルのパフォーマンス特性を毎分確認しますが、損失と遅延の計算は 60 個の Hello パケットのみに基づいて実行されます。アプリケーション認識型ルーティングが新しいトンネルが必要であると計算した場合、トンネルをリセットするのに 1 分以上かかることがあります。

各データプレーントンネルの統計情報を表示するには、**show sdwan app-route stats** コマンドを使用します。

デバイス# **show sdwan app-route stats**

SRC IP	DST IP	PROTO	SRC PORT	DST PORT	MEAN LOSS	MEAN LATENCY	INDEX	TOTAL PACKETS	LOSS	AVERAGE LATENCY	AVERAGE JITTER	TX DATA PKTS	RX DATA PKTS	
192.0.2.1	192.0.2.254	ipsec	12346	12346	0	22	0	596	0	21	2	0	0	
								1	596	0	21	2	0	0
								2	596	0	21	2	0	0
								3	597	1	21	2	0	0
								4	596	0	21	2	0	0
192.0.2.1	192.0.2.254	ipsec	12346	12346	0	24	0	596	0	24	3	0	0	
								1	596	0	25	3	0	0
								2	596	0	25	3	0	0
								3	596	0	24	3	0	0
								4	596	0	24	3	0	0
192.0.2.1	192.0.2.254	ipsec	12346	34083	0	21	0	596	0	21	3	0	0	
								1	596	0	22	3	0	0
								2	596	0	22	3	0	0
								3	596	0	21	3	0	0
								4	596	0	21	3	0	0
192.0.2.1	192.0.2.254	ipsec	12346	36464	0	23	0	596	0	23	3	0	0	
								1	596	0	23	3	0	0
								2	596	0	24	3	0	0
								3	596	0	23	4	0	0
								4	596	0	23	4	0	0
								5	596	0	23	4	0	0

デバイスがサービス側インターフェイスに送信する IP パケットのネクストホップ情報を表示するには、**show policy service-path** コマンドを使用します。ルータが WAN トランスポートトンネルインターフェイスに送信するパケットの類似情報を表示するには、**show policy tunnel-path** コマンドを使用します。

Cisco IOS XE Catalyst SD-WAN デバイスでのアプリケーションの可視性の有効化

LAN 内のすべての VPN で実行されているすべてのアプリケーションをモニタリングできるように、アプリケーション認識型ルーティングポリシーを設定せずに、Cisco IOS XE Catalyst SD-WAN デバイスでアプリケーションの可視性を直接有効にすることができます。これを行うには、ルータでアプリケーションの可視性を設定します。

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

アプリケーションをモニターするには、デバイスで **show app dpi applications** および **show app dpi supported-applications** コマンドを使用します。

CLIを使用したアプリケーション認識型ルーティングの設定

次に、アプリケーション認識型ルーティングポリシーの設定手順の概要を示します。

1. アプリケーション認識型ルーティング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 (**apply-policy** コマンドを使用)。

```
vSmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-site-list)# 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. 次のように、マッチするアプリケーションのデータトラフィックに適用する SLA クラスとトラフィック特性を作成します。

```
vSmart(config)# policy sla-class sla-class-name
vSmart(config-sla-class)# jitter milliseconds
vSmart(config-sla-class)# latency milliseconds
vSmart(config-sla-class)# loss percentage
vSmart(config-sla-class)# app-probe-class app-probe-class
vSmart(config-sla-class)# fallback-best-tunnelcriterialatencylossjitter
```

3. (ポリシー定義の **match** セクションで) 対象のアプリケーションのトラフィックの特定に使用するアプリケーション、IP プレフィックス、および VPN のリストを作成します。

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

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

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

4. 次のように、アプリケーション認識型ルーティング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 app-route-policy policy-name
vSmart(config-app-route-policy)# vpn-list list-name
```

5. ポリシー内で、マッチ/アクションペアの番号付きシーケンスを1つ以上作成します。ここで、マッチパラメータは対象のデータトラフィックとアプリケーションを定義し、アクションパラメータは一致が発生した場合に適用する SLA クラスを指定します。

1. シーケンスを作成します。


```
vSmart(config-app-route-policy)# sequence number
```

2. データパケットのマッチパラメータを定義します。

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

3. 次のように、マッチが発生したときに実行するアクションを定義します。

```
vSmart(config-sequence)# action sla-class sla-class-name [strict]
vSmart(config-sequence)# action sla-class sla-class-name [strict] preferred-color
colors
vSmart(config-sequence)# <userinput>action backup-sla-preferred-color</userinput>
<varname>colors</varname>
```

最初の2つのアクションオプションは、一致するデータトラフィックを、指定されたSLAクラスのSLA特性を満たすトンネルインターフェイスに転送します。

- **sla-class sla-class-name** : 追加パラメータなしでSLAクラスを指定すると、1つのトンネルインターフェイスが使用可能である限り、SLAに一致するデータトラフィックが転送されます。ソフトウェアは、最初にSLAに一致するトンネルを介してトラフィックを送信しようとします。単一のトンネルがSLAに一致する場合、データトラフィックはそのトンネルを介して送信されます。2つ以上のトンネルが一致する場合、トラフィックはトンネル間で分散されます。SLAに一致するトンネルがない場合、データトラフィックは使用可能なトンネルの1つを介して送信されます。
- **sla-class sla-class-name preferred-color color** : データトラフィックがSLAクラスと一致する場合に使用する特定のトンネルを設定するには、**preferred-color** オプションを含めて、優先トンネルの色を指定します。複数のトンネルがSLAに一致する場合、トラフィックは優先トンネルに送信されます。優先カラーのトンネルが使用できない場合、トラフィックはSLAクラスに一致するトンネルを介して送信されます。SLAに一致するトンネルがない場合、データトラフィックは使用可能ないずれかのトンネルを介して送信されます。この意味で、色設定は厳密な一致ではなく、緩い一致であると見なされます。これは、データトラフィックは優先色のトンネルが使用可能かどうかに関係なく、常に転送されるためです。
- **sla-class sla-class-name preferred-color colors** : データトラフィックがSLAクラスと一致する場合に使用する複数のトンネルを設定するには、**preferred-color** オプションを含めて、2つ以上のトンネルの色を指定します。トラフィックは、すべてのトンネル間でロードバランシングされます。

SLAに一致するトンネルがない場合、データトラフィックは使用可能ないずれかのトンネルを介して送信されます。この意味で、色設定は厳密な一致ではなく、緩い一致であると見なされます。これは、データトラフィックは優先色のトンネルが使用可能かどうかに関係なく、常に転送されるためです。SLAに一致するトンネルがない場合は、データトラフィックの処理方法を選択できます。

- **strict** : データトラフィックをドロップします。
- **backup-sla-preferred-color colors** : データトラフィックを特定のトンネルに転送します。トンネルインターフェイスが使用可能な場合、データトラフィックは設定されたトンネルから送信されます。そのトンネルが使用できない場合、トラフィック

クは使用可能な別のトンネルに送信されます。1 つ以上の色を指定できます。**preferred-color** オプションと同様に、バックアップ SLA の優先色は緩い一致です。単一のアクション設定では、**strict** オプションと **backup-sla-preferred-color** オプションの両方を含めることはできません。

4. ポリシーに一致するパケットまたはバイトをカウントします。

```
vSmart(config-sequence)# action count counter-name
```

5. SLA クラスルールに一致するパケットのサンプルセットを syslog ファイルに配置します。

```
vSmart(config-sequence)# action log
```

6. ポリシー内のマッチ/アクションペアは、シーケンス番号に基づいて、番号の小さいものから順に評価されます。マッチした場合は、対応するアクションが実行され、ポリシーの評価が停止します。

6. パケットがいずれかのシーケンスの条件のどれにもマッチしない場合は、デフォルトのアクションが実行されます。アプリケーション認識型ルーティングポリシーの場合、デフォルトのアクションでは、マッチしないトラフィックが受け入れられ、SLA を考慮せずにそのトラフィックがそのまま転送されます。次のようにデフォルトのアクションを設定しておくことで、SLA パラメータをマッチしないパケットに適用することができます。

```
vSmart(config-policy-name)# default-action sla-class sla-class-name
```

7. ポリシーを site-list に適用します。

```
vSmart(config)# apply-policy site-list list-name app-route-policy policy-name
```

CLI を使用したアプリケーション プロブ クラスの設定

次の例に示すように、app-probe-class と real-time-video を設定したら、それらを SLA クラスにマッピングします。

```
Device(config)# app-probe-class real-time-video
Device(config)# forwarding-class videofc
Device(config)# color mpls dscp 34
Device(config)# color biz-internet dscp 40
Device(config)# color lte dscp 0
```

```
Device(config)# sla-class streamsla
Device(config)# latency 20
Device(config)# loss 10
Device(config)# app-probe-class real-time-video
```

次に示すように、BFD テンプレートを使用して DSCP のデフォルト値を設定します。

```
Device(config)# bfd default-dscp 50
Device(config)# bfd color mpls 15
```

アプリケーション認識型ルーティングポリシーの設定例

このトピックでは、アプリケーション認識型ルーティングポリシーを設定する簡単な例を示します。この例では、ICMP トラフィックに適用するポリシーを定義し、リンクが使用可能な場合は遅延が 50 ミリ秒以下のリンクにトラフィックを誘導します。

Cisco Catalyst SD-WAN コントローラ にアプリケーション認識型ルーティングポリシーを設定します。設定は以下のハイレベルコンポーネントで構成されます。

- アプリケーションの定義
- アプリケーションプローブクラスの定義 (オプション)
- SLA パラメータの定義
- サイト、プレフィックス、VPN の定義
- アプリケーション認識型ルーティングポリシー自体
- ポリシーが適用されるオーバーレイ ネットワーク サイトの指定

これらのコンポーネントを設定する順序は、CLI の観点からは重要ではありません。ただし、アーキテクチャ設計の観点から見た論理的な順序は、まずアプリケーション認識型ルーティングポリシー自体で呼び出される、またはオーバーレイネットワーク内のさまざまなサイトにポリシーを適用するために使用されるすべてのパラメータを定義することです。次に、アプリケーション認識型ルーティングポリシー自体と、ポリシーを適用するネットワークサイトを指定します。

Cisco Catalyst SD-WAN コントローラ で、このアプリケーション認識型ルーティングポリシーを設定する手順を次に示します。

1. 一致する ICMP トラフィックに適用する SLA パラメータを定義します。この例では、遅延が 50 ミリ秒以下のリンクに ICMP トラフィックを転送します。

```
vSmart# config
vSmart(config)# policy sla-class test_sla_class latency 50
vSmart(config-sla-class-test_sla_class)#
```

2. アプリケーション認識型ルーティングポリシーを適用するサイトと VPN リストを定義します。

```
vSmart(config-sla-class-test_sla_class)# exit
vSmart(config-sla-class-test_sla_class)# lists vpn-list vpn_1_list vpn 1
vSmart(config-vpn-list-vpn_1_list)# exit
vSmart(config-lists)# site-list site_500 site-id 500
vSmart(config-site-list-site_500)#
```

3. アプリケーション認識型ルーティングポリシーの設定この例では、2つの異なる方法でアプリケーションにポリシーを適用することに注意してください。シーケンス 1、2、3 では、プロトコル番号を指定しています (プロトコル 1 は ICMP、プロトコル 6 は TCP、プロトコル 17 は UDP)。

```
vSmart(config-site-list-site_500)# exit
vSmart(config-lists)# exit
```

```
vSmart(config-policy)# app-route-policy test_app_route_policy
vSmart(config-app-route-policy-test_app_route_policy)# vpn-list vpn_1_list
vSmart(config-vpn-list-vpn_1_list)# sequence 1 match protocol 6
vSmart(config-match)# exit
vSmart(config-sequence-1)# action sla-class test_sla_class strict
vSmart(config-sequence-1)# exit
vSmart(config-vpn-list-vpn_1_list)# sequence 2 match protocol 17
vSmart(config-match)# exit
vSmart(config-sequence-2)# action sla-class test_sla_class
vSmart(config-sequence-2)# exit
vSmart(config-vpn-list-vpn_1_list)# sequence 3 match protocol 1
vSmart(config-match)# exit
vSmart(config-sequence-3)# action sla-class test_sla_class strict
vSmart(config-sequence-3)# exit
vSmart(config-sequence-4)#
```

4. Cisco IOS XE Catalyst SD-WAN オーバーレイネットワーク内の目的のサイトにポリシーを適用します。

```
vSmart(config-sequence-4)# top
vSmart(config)# apply-policy site-list site_500 app-route-policy test_app_route_policy
```

5. 設定の変更を表示します。

```
vSmart(config-site-list-site_500)# top
vSmart(config)# show config
```

6. 設定にエラーがないことを確認します。

```
vSmart(config)# validate
Validation complete
```

7. 設定を有効にします。

```
vSmart(config)# commit
Commit complete.
```

8. 設定モードを終了します。

```
vSmart(config)# exit
vSmart#
```

設定をすべてまとめると、次のようになります。

```
vSmart# show running-config policy
policy
sla-class test_sla_class
  latency 50
!
app-route-policy test_app_route_policy
vpn-list vpn_1_list
  sequence 1
    match
      protocol 6
    !
    action sla-class test_sla_class strict
  !
  sequence 2
    match
      protocol 17
    !
    action sla-class test_sla_class
  !
  sequence 3
```

```
        match
        protocol 1
        !
        action sla-class test_sla_class strict
        !
        !
        !
    lists
    vpn-list vpn_1_list
        vpn 1
        !
    site-list site_500
        site-id 500
        !
    site-list site_600
        site-id 600
        !
        !
    !
    !
    apply-policy
    site-list site_500
    app-route-policy test_app_route_policy
    !
    !
```

マルチキャストプロトコルを定義する例を次に示します。

```
policy
!
sla-class SLA_BEST_EFFORT
    jitter 900
    !
sla-class SLA_BUSINESS_CRITICAL
    loss 1
    latency 250
    jitter 300
    !
sla-class SLA_BUSINESS_DATA
    loss 3
    latency 400
    jitter 500
    !
sla-class SLA_REALTIME
    loss 2
    latency 300
    jitter 60
    !
app-route-policy policy_multicast
vpn-list multicast-vpn-list
sequence 10
match
    source-ip 10.0.0.0/8
    destination-ip 10.255.255.254/8
    !
    action
    count mc-counter-10
    sla-class SLA_BUSINESS_CRITICAL
    !
    !
sequence 15
match
    source-ip 172.16.0.0/12
    destination-ip 172.31.255.254/12
    !
```

```

    action
      count mc-counter-15
      sla-class SLA_BEST_EFFORT
    !
  !
sequence 20
match
  destination-ip 192.168.0.1
  !
  action
    count mc-counter-20
    sla-class SLA_BUSINESS_CRITICAL
  !
  !
sequence 25
match
  protocol      17
  !
  action
    count mc-counter-25
    sla-class SLA_REALTIME
  !
  !
sequence 30
match
  source-ip      192.168.0.0/16
  destination-ip 192.168.255.254
  protocol      17
  !
  action
    count mc-counter-30
    sla-class SLA_BUSINESS_DATA preferred-color lte
  !
  !
default-action sla-class SLA_BEST_EFFORT
!
sequence 35
match
  source-ip      10.0.0.0/8
  destination-ip 10.255.255.254/8
  protocol      17
  !
  action
    count mc-counter-35
    sla-class SLA_BUSINESS_DATA preferred-color lte
    backup-sla-preferred-color 3g
  !
  !
lists
  vpn-list multicast-vpn-list
  vpn 1
  vpn 60
  vpn 4001-4010
  vpn 65501-65510
  !
  site-list multicast-site-list
  site-id 1100
  site-id 500
  site-id 600
  !
!
!
apply-policy
  site-list multicast-site-list
```

```
    app-route-policy policy_multicast
  !
!
```

ランク付けカラーの優先順位の例

```
app-route-policy SAMPLE _AAR
vpn-list ONE
sequence 10
  match
    dscp 46
  !
  action
    sla VOICE_SLA strict preferred-color-group GROUP2_COLORS
  !
!
sequence 20
  match
    dscp 34
  !
  action
    sla VOICE_SLA preferred-color-group GROUP1_COLORS
  !
!
sequence 30
  match
    dscp 28
  !
  action
    sla VOICE_SLA preferred-color-group GROUP3_COLORS
  !
!
!
policy lists
  preferred-color-group GROUP1_COLORS
  primary-preference
    color-preference biz-internet
    path-preference direct-tunnel
  !
  secondary-preference
    color-preference mpls
    path-preference multi-hop-path
  !
  tertiary-preference
    color-preference lte
  !
!
  preferred-color-group GROUP2_COLORS
  primary-preference
    color-preference mpls
  !
  secondary-preference
    color-preference biz-internet
  !
!
  preferred-color-group GROUP3_COLORS
  primary-preference
    color-preference mpls biz-internet lte
  !
!
```



(注) Cisco SD-WAN Manager で [マルチリージョンファブリック (Multi-Region Fabric)] オプションを有効にしている場合にのみ、path-preference オプションを設定できます。

IPv6 アプリケーションに対する AAR ポリシーの例

```

policy
  sla-class Default
    jitter 100
    latency 300
    loss 25
  !
  app-route-policy _VPN1_AAR-Policy-for-IPv6-Traffic
  vpn-list VPN1
    sequence 1
      match
        app-list Msft-0365
      !
      action
        sla-class Default preferred-color public-internet
      !
    !
  !
  lists
    app-list Msft-0365
      app ms-office-web-apps
    !
    site-list SITE-100
      site-id 100
    !
    vpn-list VPN1
      vpn 1
    !
  !
  !
  apply-policy
    site-list SITE-100
    app-route-policy _VPN1_AAR-Policy-for-IPv6-Traffic
  !
  !

```




第 11 章

拡張アプリケーション認識型ルーティング



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 33: 機能の履歴

機能名	リリース情報	説明
拡張アプリケーション認識型ルーティング	<p>Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降で使用できます。</p> <p>Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降で使用できます。</p>	<p>拡張アプリケーション認識型ルーティングが有効になっていない場合、損失、遅延、およびジッターが特定のしきい値を超えたときに、Cisco IOS XE Catalyst SD-WAN デバイスが、SLA 要件を満たすために、あるネットワークパスから別のネットワークパスにトラフィックを切り替えるのに数分かかります。</p> <p>拡張アプリケーション認識型ルーティングを有効にすることで、トンネルパフォーマンスの問題は検出が迅速化されます。これにより、Cisco IOS XE Catalyst SD-WAN デバイスが SLA 要件を満たさないトンネルからトラフィックをリダイレクトできるようにする仕組みになっています。</p>

- [拡張アプリケーション認識型ルーティングについて \(212 ページ\)](#)
- [拡張アプリケーション認識型ルーティングに対応したデバイス \(217 ページ\)](#)
- [拡張アプリケーション認識型ルーティングに関する制約事項 \(217 ページ\)](#)
- [拡張アプリケーション認識型ルーティングの前提条件 \(217 ページ\)](#)
- [拡張アプリケーション認識型ルーティングの設定 \(217 ページ\)](#)
- [拡張アプリケーション認識型ルーティングの設定確認 \(220 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager を使用した拡張アプリケーション認識型ルーティングのモニター \(221 ページ\)](#)
- [拡張アプリケーション認識型ルーティングのトラブルシューティング \(222 ページ\)](#)

拡張アプリケーション認識型ルーティングについて

拡張アプリケーション認識型ルーティングが有効になっていない場合、損失、遅延、およびジッターが特定のしきい値を超えたときに、Cisco IOS XE Catalyst SD-WAN デバイスが SLA 要件を満たすために、あるネットワークパスから別のネットワークパスにトラフィックを切り替えるのに数分かかります。拡張アプリケーション認識型ルーティングを有効にすることで、トンネルパフォーマンスの問題は検出が迅速化されます。これにより、Cisco IOS XE Catalyst

SD-WAN デバイスは、SLA 要件を満たさないトンネルからトラフィックをリダイレクトできるようにします。

拡張アプリケーション認識型ルーティングの概要

Bidirectional Forwarding Detection (BFD) は、リンク障害状態を検出し、Cisco Catalyst SD-WAN トンネル (IPsec と GRE の両方) の損失、遅延、ジッター情報などのパフォーマンスルーティング データ (PfR) を収集します。各 BFD hello パケットは、次の情報を収集します。

遅延：BFD エコーの要求から応答までの RTT (ラウンドトリップ時間)。

ジッター：ネットワーク内のパケット到着時間の遅延変動。これはデータパケットが送受信されるタイミングの不規則性を示す指標です。

損失：応答を受信できなかったエコー要求の数。

デフォルトでは、BFD hello タイマーが 1 秒の場合、PfR データの 1 サンプルが 1 秒ごとに収集されます。この PfR データは、ポーリング間隔 (デフォルトは 10 分) の期間にわたって収集されます。ポーリング間隔中に、各統計情報の平均が計算されます。アプリケーション認識型ルーティング SLA で指定されたしきい値に基づいてダイナミックパス決定を行うために、デフォルトの乗数 6 が使用され、ポーリング間隔の複数の平均を確認します。ポーリング間隔平均とは、ネットワークモニタリングまたはパフォーマンス測定システムにおいて、連続するポーリングまたは測定イベント間の平均時間を指します。ポーリング間隔の平均は、システムが特定の期間にデータを収集したり、ネットワークメトリックをサンプリングしたりする頻度を示します。

コンバージェンス時間とは、障害後または中断後にネットワークが回復し、通常の動作を再開するのにかかる時間を指します。ただし、徐々に劣化する WAN 回線を検出するためのデフォルトのコンバージェンス時間は 10 分～1 時間です。推奨されるポーリング間隔の最小値が 2 分と 6 間隔の場合でも、コンバージェンス時間は 2～12 分です。設定されたポーリング間隔が非常に低い場合、損失、遅延、およびジッター測定のサンプルデータが不十分なため、PfR の誤検出やトラフィックの不安定が発生する可能性があります。

PfR 測定

表 34: PfR 測定

Metric	ソース	説明
損失	BFD	<p>BFD パケット損失を 1 pps または <code>n_app_probe_class</code> (<code>n-apc</code>) 秒の 1 パケットとして測定</p> <p>アプリケーションプローブクラス (APC) 設定が設定されていない場合、BFD パケットの損失は 1 パケット/秒 (1pps) のレートで発生します。APC 設定があれば、損失は N 秒で 1 パケットに減少します。</p> <p>詳細については、「アプリケーションプローブクラス」を参照してください。</p>
遅延	BFD	<p>1 pps または <code>n-apc</code> 秒で 1 パケットを測定する RTT</p> <p>アプリケーションプローブクラス (APC) が設定されていない場合、RTT パケットの損失は、1 秒あたり 1 パケット (1pps) のレートで発生します。APC 設定があれば、損失は N 秒で 1 パケットに減少します。</p>
Jitter	BFD	RTT の変動

アプリケーション認識型ルーティングの設計と測定

- デフォルトの BFD hello 間隔は 1 秒で、`app-route/SLA` のポーリング間隔は 10 分です。

BFD hello 間隔とは、BFD (Bidirectional Forwarding Detection) プロトコルがネットワークパスの活性状態を検出するために hello パケットを送信する頻度を指します。デフォルトでは、hello 間隔は 1 秒に設定されています。一方、`app-route/SLA` ポーリング間隔は、ネットワーク モニタリング システムがアプリケーションルートまたはサービスレベル契約 (SLA) に関連するデータを収集したり、ネットワークメトリックを測定したりする頻度を決定します。`app-route/SLA` のデフォルトのポーリング間隔は 10 分に設定されています。

- デフォルトでは、1 pps x 600 秒 x 6 バケットで 60 分を計算します。

ポーリング間隔のデフォルト値の分単位の計算を参照します。1秒あたり1パケット (pps) に 600 秒 (10 分) を掛け、その結果に 6 バケットを掛けて間隔を計算します。結果の値は 60 分です。これはデフォルトのポーリング間隔です。

- 専門家は、ポーリング間隔に 120 秒 (2 分)、乗数に 5 を使用し、10 分間隔とすることを推奨しています。この推奨事項は、特定のモニタリング頻度を実現するためによく使用されます。
- ポーリング間隔/乗数を小さくすると検出時間が短縮されますが、PfR メトリックのサンプル数が少ないと誤検出が発生する可能性があります。

ポーリング間隔や乗数を小さくすると、ネットワークパフォーマンスの問題の検出速度が向上します。しかし、これらの値を小さくすると、誤検出の可能性も高まる可能性があります。データサンプル数が少ないため、システムが問題を誤って特定する可能性があるためです。PfR (パフォーマンスルーティング) メトリックの検出時間と精度のバランスを取る必要があります。

- 唯一のオプションは、BFD Hello 間隔を短くして、より高速なレートで測定精度を向上させることです。

ネットワークパフォーマンスをより高速かつ正確に測定するには、BFD hello 間隔を小さくすることが推奨されます。ネットワークパスの活性状態とは、ネットワークパスの接続性と可用性の状態を指します。hello パケットの交換間隔を短くすることで、ネットワークパスの活性状態をより頻繁に検出できるようになり、測定精度が向上します。

拡張アプリケーション認識型ルーティングの利点

1. PfR メトリック (損失/遅延/ジッター) の測定にインラインデータを導入することで、これらのメトリックをより正確かつ詳細に測定できるように改善しました。インラインデータとは、Cisco IOS XE Catalyst SD-WAN デバイス 内のネットワークのエッジで直接処理および検査されるトラフィックです。分析とセキュリティチェックのためにすべてのトラフィックを一元的な場所にルーティングする代わりに、インラインデータを使用すると、ネットワークエッジでリアルタイムの検査と意思決定が可能になります。
2. 拡張アプリケーションルートの簡易検出と SLA の適用が可能です。これには PfR のポーリング間隔を極めて低い値 (最小で 10 秒) まで減少させられることが含まれます。これにより、Cisco IOS XE Catalyst SD-WAN デバイス は徐々に進行する回線の劣化を迅速に検出できます。回線が SLA のしきい値を満たさない場合、トンネルは SLA 転送から迅速に切り替えられるため、効率的で信頼性の高いネットワークパフォーマンスが確保されます。SLA (サービスレベル契約) 転送とは、事前定義されたパフォーマンス基準または SLA に基づいてネットワークトラフィックを動的にルーティングする、Cisco Catalyst SD-WAN ソリューションの機能を指します。
3. SLA スイッチオーバーの速度が向上しました。
4. SLA ダンプニングが導入され、SLA 転送への移行がよりスムーズになります。SLA 転送を再度実装する前に、トンネルはダンプニングと呼ばれるプロセスを実行します。これは、

中断を防ぎ、不安定性を削減するのに役立ちます。これにより、SLA へのスムーズな移行が保証され、ネットワークパフォーマンスへの悪影響が最小限に抑えられます。

5. 損失、遅延、ジッターを測定するための機能が拡張されました。

拡張アプリケーション認識型ルーティングのガイドライン

- GRE トンネルと IPSEC トンネルの両方がサポートされます。
- 物理インターフェイス、サブインターフェイス、ループバックバインド、ダイヤラ、および LTE インターフェイスを含む、既存のすべての TLOC および WAN インターフェイスのタイプがサポートされます。
- TLOC Extension トンネルがサポートされています。
- IPv4 と IPv6 の両方のアンダーレイトンネルがサポートされています。
- SLA の更新とスイッチオーバーは、最小 10 秒間隔で発生します。
- トンネルのスケールは影響を受けず、メモリとパフォーマンスへの影響も最小限です。
- SLA クラスの `app-probe` クラス設定の有無にかかわらず、サポートが提供されます。
- SLA ダンプニングがサポートされています。

拡張アプリケーション認識型ルーティングを実行していない Cisco IOS XE Catalyst SD-WAN デバイス との互換性

1. それぞれ、次のシナリオの通りです。
 - ローカル側：Cisco IOS XE Catalyst SD-WAN デバイスが Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降にアップグレードされ、EAAR（拡張アプリケーション認識型ルーティング）が有効になっています。
 - リモート側：Cisco IOS XE Catalyst SD-WAN デバイスが Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a にアップグレードされず、EAAR は有効になっていません。

その後、システムは、古いリリースとの互換性があり無効になっている機能が存在する BFD ベースの測定を使用するようにフォールバックします。

2. ローカル側とリモート側の両方が Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a を使用しているが、EAAR 機能が有効になっていない場合、システムは BFD ベースの測定を使用するように戻ります。



(注) EAAR 機能は、既存の展開をサポートするため、デフォルトで無効になっています。

拡張アプリケーション認識型ルーティングに対応したデバイス

Cisco IOS XE Catalyst SD-WAN デバイスについて

拡張アプリケーション認識型ルーティングに関する制約事項

- この機能を有効にしたブランチデバイスは、ループバック アンバインド モードをサポートしません。ループバックアンバインドモードとは、ループバックデバイスがネットワークスタックから切断されるネットワーク インターフェイス設定を指します。
- GRE トンネルにはキューごとの測定はありません。キューごとの測定は、キューごとにネットワークトラフィックをモニターおよび分析するために使用されます。これには、ネットワークデバイスまたはシステム内の個々のキューごとに、さまざまなメトリックや統計情報を測定および収集することが含まれます。キューは、パケットが送信または処理される前に格納されるバッファです。

拡張アプリケーション認識型ルーティングの前提条件

Cisco IOS XE Catalyst SD-WAN デバイス でアプリケーション認識型ルーティングを有効にするには、両方の Cisco IOS XE Catalyst SD-WAN デバイス で拡張アプリケーション認識型ルーティングを有効にします。

拡張アプリケーション認識型ルーティングの設定

このセクションの手順では、拡張されたアプリケーション認識型ルーティング設定を Cisco Catalyst SD-WAN Manager から Cisco IOS XE Catalyst SD-WAN デバイス に展開する方法について説明します。

Cisco Catalyst SD-WAN Manager の機能テンプレートを使用した拡張アプリケーション認識型ルーティングの設定

1. [Cisco SD-WAN Manager] のメニューから、[設定 (Configuration)] > [テンプレート (Templates)] を選択します。
2. [Feature Templates] をクリックします。

- [Add template] をクリックします。
- デバイスを選択し、[基本情報 (Basic Information)] の下にある [Cisco システム (Cisco System)] テンプレートをクリックします。
- [拡張アプリケーション認識型ルーティング (Enhanced App-Aware Routing)] フィールドで、ドロップダウンリストから [グローバル (Global)] をクリックし、次のいずれかのモードを選択します。

Mode	[EAAR ポーリング間隔 (EAAR Poll Interval)]	[EAAR ポーリング乗数 (EAAR Poll Multiplier)]	[EAAR ポーリングウィンドウ (EAAR Poll Window)]	[SLA ダンプニング乗数 (SLA Dampening Multiplier)]	[SLA ダンプニングウィンドウ (SLA Dampening Window)]
[アグレッシブ (Aggressive)]	10 秒	6	10 秒 ~ 60 秒	120	20 分
中程度	60 s	5	60 秒 ~ 300 秒	40	40 分
[コンサーバティブ (Conservative)]	300 秒	6	300 秒 ~ 1800 秒	12	60 分



(注) 拡張アプリケーション認識型ルーティング (EAAR) のポーリング間隔、ポーリング乗数、および SLA ダンプニング乗数の設定は、CLI テンプレートを介してのみとなります。

- [Save] をクリックします。

Cisco Catalyst SD-WAN Manager の構成グループを使用した、拡張アプリケーション認識型ルーティングの設定

- [Cisco SD-WAN Manager] のメニューから、[設定 (Configuration)] > [[構成グループ (Configuration Groups)] を選択します。
- 構成グループを選択します。[アクション (Actions)] にある [編集 (Edit)] をクリックします。
- [機能プロファイル (Feature Profiles)] で、[システムプロファイル (System Profile)] をクリックします。
- [ベーシック (Basic)] を選択し、[アクション (Actions)] で [機能の編集 (Edit Feature)] をクリックします。

- [基本機能の編集 (Edit Basic Feature)] ページで、[拡張 APP ルート (Enhanced App-Route)] フィールドを使用し、次のいずれかのモードを選択します。

Mode	[EAAR ポーリング間隔 (EAAR Poll Interval)]	[EAAR ポーリング乗数 (EAAR Poll Multiplier)]	[EAAR ポーリングウィンドウ (EAAR Poll Window)]	[SLA ダンプ乗数 (SLA Dampening Multiplier)]	[SLA ダンプウィンドウ (SLA Dampening Window)]
[アグレッシブ (Aggressive)]	10 秒	6	10 秒 ~ 60 秒	120	20 分
中程度	60 s	5	60 秒 ~ 300 秒	40	40 分
[コンサーバティブ (Conservative)]	300 秒	6	300 秒 ~ 1800 秒	12	60 分

- [Save] をクリックします。

CLI テンプレートを使用した、拡張アプリケーション認識型ルーティングの設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#) および [CLI テンプレート](#) を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

- SLA 適用のための拡張 PfR 測定を有効にします。

bfd Enhanced-app-route enable

Cisco IOS XE Catalyst SD-WAN デバイス でアプリケーション認識型ルーティング機能を有効にするには、リモート Cisco IOS XE Catalyst SD-WAN デバイス とローカル Cisco IOS XE Catalyst SD-WAN デバイス の両方で PfR CLI を有効にする必要があります。

この機能は、次の 2 段階からなります。

- リモート Cisco IOS XE Catalyst SD-WAN デバイス は、ローカル Cisco IOS XE Catalyst SD-WAN デバイス に損失統計情報を提供する必要があります。
 - ローカル Cisco IOS XE Catalyst SD-WAN デバイスは、これらのメトリックを使用してサービスレベル契約 (SLA) を実施します。
- 拡張アプリケーション認識 PfR が有効になっている場合、SLA の実施とスイッチオーバーには、デフォルトのポーリング間隔 10 秒と乗数 6 が使用されます。これらの設定を変更するには、次の設定オプションを使用します。

bfd enhanced-app-route pfr-poll-interval

bfd enhanced-app-route pfr-multiplier <number>

アプリケーションルート PfR 乗数のアグレッシブモード設定では、デフォルトが 6 になっています。モデレートモードの場合は 5 です。

3. SLA のダンプニング時間を設定します。これは、SLA を満たした後、トンネルを SLA バケットに戻すまでの待機時間です。time のデフォルトは 120 秒です。拡張 PfR が有効になっている場合は、SLA ダンプニングを有効にします。

bfd sla-dampening enable

bfd sla-dampening multiplier <number>

ダンプニング乗数のアグレッシブモード設定は、デフォルトが 120 になっています。

拡張アプリケーション認識型ルーティングの設定確認

拡張アプリケーションルーティング設定を確認し、EAAR の設定済みパラメータを表示するには、**show sdwan app-route params** コマンドを使用します。

Device# show sdwan app-route params

```
*EAAR = Enhanced Application-Aware Routing
Config:                               :Enabled
Poll interval:                         :10000
Poll multiplier:                       :6

App route
Poll interval:                         :600000
Poll multiplier:                       :6

SLA dampening
Config:                               :Enabled
Multiplier:                           :120
```

show sdwan bfd sessions alt コマンドを使用して、EAAR のフラグを強調表示できます。

Device# show sdwan bfd sessions alt

```
*Sus = Suspend
*GREinUDP = GREinUDP encap
*EAAR = Enhanced Application-Aware Routing
*NA = Flag Not Set
```

SYSTEM IP	IP	SITE ID	STATE	COLOR PORT	DST PUBLIC		SOURCE TLOC		REMOTE TLOC										
					ENCAP	COLOR BFD-LD	ENCAP	COLOR BFD-LD	ENCAP	COLOR BFD-LD	ENCAP	COLOR BFD-LD	FLAGS	SOURCE UPTIME					
172.16.0.0	100	100	up	lte															
	10.0.0.0			10.0.0.1	12367	ipsec			20013	lte									NA
	0:07:48:38																		
172.16.0.1	100	100	up	lte															
	10.0.0.0			10.0.0.1	12377	ipsec			20014	lte									NA
	0:07:48:39																		
172.16.0.0	400	100	up	lte															
	10.0.0.0			10.0.0.1	12366	ipsec			20015	lte									NA
	0:07:48:39																		
172.16.0.1	500	100	up	lte															
										lte									

```

10.0.0.0          10.0.0.1          12366          ipsec          20016          EAAR
0:07:48:39

```

show sdwan app-route stats summary コマンドを使用すると、設定されたすべての APC について、異なる測定間隔で各トンネルの app-route (PfR) 統計情報の詳細を表示できます。

Device# show sdwan app-route stats summary

```

app-route statistics 10.0.0.0 10.0.0.0 ipsec 12366 12367
remote-system-ip      172.16.0.0
local-color           lte
remote-color          lte
sla-class-index       0,1,2,3
fallback-sla-class-index None
enhanced-app-route    Enabled
sla-dampening-index   4,5
app-probe-class-list  None
mean-loss             0
mean-latency          0
mean-jitter           0

```

INDEX	TOTAL		LATENCY	JITTER	AVERAGE	AVERAGE	TX DATA	RX DATA
	IPV6 TX	IPV6 RX						
PKTS	PACKETS	LOSS			PKTS		PKTS	DATA
0	664	0	0	0	0	0	0	0
1	663	0	0	0	0	0	0	0
2	666	0	0	0	0	0	0	0
3	664	0	0	0	0	0	0	0
4	662	0	0	0	0	0	0	0
5	664	0	0	0	0	0	0	0

Cisco Catalyst SD-WAN Manager を使用した拡張アプリケーション認識型ルーティングのモニター

1. Cisco Catalyst SD-WAN Manager のメニューから [モニター (Monitor)] > [デバイス (Devices)] の順に選択します。
2. [デバイス (Devices)] で、デバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [デバイスオプション (Device Options)] フィールドで、[アプリケーションルート統計情報 (App Routes Statistics)] を選択します。

EAAR-BR-SITE700 | Site Name 700 Device Model: C8000v ⓘ

Device Options:

Filter ▾

Search ▽

Total Rows: 48 ↻ ⚙️

ocol	Source Port	Destination Port	Remote System Ip	Local Color	Remote Color	Enhanced App Route	Slas Dampening Index
	12346	12346		public-internet	public-internet	Enabled	None
	12346	12346		public-internet	public-internet	Enabled	None
	12346	12346		public-internet	public-internet	Enabled	None
	12346	12346		public-internet	public-internet	Enabled	None
	12346	12346		public-internet	public-internet	Enabled	None
	12346	12346		public-internet	public-internet	Enabled	None
	12346	12346		public-internet	public-internet	Enabled	None
	12346	12346		public-internet	public-internet	Enabled	None

拡張アプリケーション認識型ルーティングのトラブルシューティング

デバイスから：

```
Device# show sdwan run | include enhanced-app-route
```

```
bfd enhanced-app-route enable
bfd enhanced-app-route pfr-poll-interval 10000
bfd enhanced-app-route pfr-multiplier 6
```

```
show sdwan run | inc sla-dampening
```

```
bfd sla-dampening enable
bfd sla-dampening multiplier 12
```

```
Device# show sdwan app-route params
```

```
Enhanced app route
  Config:                :Enabled <<< Enhanced app-aware routing enabled
  Poll interval:         :10000
  Poll multiplier:       :6
App route
  Poll interval:         :600000
  Poll multiplier:       :6
SLA dampening
  Config:                :Enabled
  Multiplier:            :120
```

```
Device# show platform hardware qfp active feature sdwan datapath pathmon
summary
```

```
Src IP          Dst IP          Src Port Dst Port  Encap  Uidb    Bfd Discrim PathMon
-----
10.0.0.0       10.0.0.1       12346   12366    IPSEC  65527   20003   in/out
```

```
Device# show sdwan bfd sessions alt
```

```
*Sus = Suspend
```

```

*GREinUDP = GREinUDP encap
*EAAR = Enhanced Application-Aware Routing
*NA = Flag Not Set

```

SYSTEM IP	DST PUBLIC		SOURCE TLOC	REMOTE TLOC		SOURCE IP	
	SITE ID	STATE		DST PUBLIC	COLOR		COLOR
UPTIME	IP		COLOR	PORT	ENCAP	BFDD-LD	FLAGS
172.16.0.0	100	down	privatel	lte		10.0.0.0	
	10.0.0.1			12367	ipsec	20011	EAAR
NA							
172.16.0.1	500	down	privatel	3g		10.0.0.0	
	10.0.0.1			12366	ipsec	20013	EAAR
NA							
172.16.0.0	600	down	privatel	3g		10.0.0.0	
	10.0.0.1			12366	ipsec	20007	EAAR
NA							

```

Device# show sdwan app-route stats remote-system-ip 172.16.0.0 app-route
statistics 10.0.0.0 10.0.0.1 ipsec 12366 12366
remote-system-ip      172.16.0.0
local-color           privatel
remote-color          3g
sla-class-index       0
fallback-sla-class-index None
enhanced-app-route    Enabled
sla-dampening-index   None

```




第 12 章

トラフィック フロー モニタリング

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、Cisco vSmart から Cisco Catalyst SD-WAN コントローラへの変更、および Cisco コントローラから Cisco Catalyst SD-WAN 制御コンポーネントへの変更。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。

- [トラフィック フロー モニタリング \(226 ページ\)](#)
- [トラフィック フロー モニタリングについて \(228 ページ\)](#)
- [トラフィック フロー モニタリングの制約事項 \(241 ページ\)](#)
- [トラフィック フロー モニタリングの設定 \(242 ページ\)](#)
- [トラフィック フロー モニタリングの確認 \(262 ページ\)](#)

トラフィック フロー モニタリング

表 35: 機能の履歴

機能名	リリース情報	説明
Flexible NetFlow での IPv6 サポートとキャッシュ サイズ変更	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	これは、Cisco IOS XE Catalyst SD-WAN デバイスの IPv6 トランスポートを介した外部コレクタへのパケットのエクスポートを可能にし、IPv6 ネットワークトラフィックを可視化できるようにする機能です。IPv4 トラフィックと IPv6 トラフィックを同時にモニターする場合は、この機能を使用することで、データプレーンのキャッシュサイズを変更できます。Cisco Flexible NetFlow (FNF) は、ネットワークトラフィックをカスタマイズして可視化できるようにするテクノロジーです。Cisco Catalyst SD-WAN では、FNF を使用して Cisco SD-WAN Manager にデータをエクスポートできるため、お客様はネットワークを簡単に監視および改善できます。
暗黙的な ACL によってドロップされたパケットのログ	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	リンク障害が発生した場合にドロップされたパケットのログを有効または無効にできるようになりました。パケットフローをログに記録する頻度も設定できます。
Flexible NetFlow の機能拡張	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	これは、Flexible NetFlow を拡張して、NetFlow レコード内のタイプオブサービス (ToS)、サンプラー ID、および再マーキングされた DSCP 値を収集する機能です。この機能拡張により、フローレコードフィールドを定義してフローレコードをカスタマイズする柔軟性がもたらされます。ToS および再マーキングされた DSCP フィールドは、IPv4 レコードでのみサポートされます。ただし、サンプラー ID フィールドは IPv4 レコードと IPv6 レコードの両方でサポートされます。

機能名	リリース情報	説明
VPN0 インターフェイス向け Flexible NetFlow	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	これは、VPN0 インターフェイスで NetFlow をサポートする機能です。 Flexible NetFlow はセキュリティツールとして機能し、Cisco SD-WAN Manager へのデータのエクスポートを可能にし、デバイスへの攻撃を検出し、トラフィックをモニターします。
Flexible NetFlow 分散エクスポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.9.x Cisco vManage リリース 20.9.1	これは、分散エクスポートを有効にして、パケットのバーストが外部コレクタに送信されたときに発生するエクスポートストームを防止する機能です。直前の間隔でのエクスポートが現在の間隔中に展開されることにより、エクスポートストームが回避されます。NetFlow パケットが低帯域幅の回線を介して送信される場合、パケットのドロップを回避するのに分散エクスポート機能が有効です。
Flexible NetFlow による BFD メトリックのエクスポート	Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1	この機能を使用すると、Bidirectional Forwarding Detection (BFD) メトリックを外部コレクタにエクスポートして、損失、遅延、およびジッターの BFD メトリックを生成できます。この機能により、ネットワーク状態データのモニタリングが強化され、収集が高速化されます。 BFD メトリックのエクスポートを有効にした後、BFD メトリックをエクスポートするためのエクスポート間隔を設定します。
Cflowd フローおよび SAIE フローをモニタリングするためのリアルタイム デバイス オプション	Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a Cisco vManage リリース 20.10.1	この機能を使用すると、選択した Cisco IOS XE Catalyst SD-WAN デバイスの VPN 内で実行されている特定の Cflowd および Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) のアプリケーションまたはアプリケーションファミリをモニタリングするためのフィルタが適用できます。 Cflowd フローおよび SAIE フローをモニタリングするためのリアルタイム デバイス オプションは、Cisco vEdge デバイスで使用できます。このリリースでは、Cisco IOS XE Catalyst SD-WAN デバイスで Cflowd および SAIE のアプリケーションをモニタリングするためのリアルタイム デバイス オプションがサポートされています。

機能名	リリース情報	説明
Cisco SD-WAN Analytics のための Flexible NetFlow の拡張機能	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	これは、Cisco SD-WAN Analytics の IPv4 および IPv6 フローレコードのために、Cisco Flexible NetFlow にロギング拡張機能を取り入れる機能です。 これらのレコードに対する show flow record コマンドの出力が拡張されました。
ループバックを TLOC として使用する場合のフローテレメトリの機能拡張。	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	ループバック インターフェイスを入力または出力トランスポート インターフェイスとして設定すると、この機能により、FNF レコードの物理インターフェイスの代わりにループバックを収集できます。この機能は、IPv4 および IPv6 でサポートされています。 ループバック インターフェイスと物理インターフェイス間のバインディング関係を表示するために、show コマンド show sdwan control local-properties wan-interface-list を更新しました。 Cisco SD-WAN Manager の既存オプションに、[インターフェイスのバインド (Bind Interface)] という新しい列が追加されました。ループバック インターフェイスと物理インターフェイス間のバインディング関係を表示するには、[モニター (Monitor)] > [デバイス (Devices)] > [リアルタイム (Real Time)] (デバイスオプションである [WAN インターフェイス情報の管理 (Control WAN Interface Information)] を選択) の順にクリックしてください。
集約トラフィックデータの最大 FNF レコードレートの設定	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN 制御コンポーネント リリース 20.14.1	デバイスでは、集約トラフィックデータの Flexible NetFlow (FNF) レコードを送信する最大レート (1分あたりのレコード数) を設定できます。これにより、デバイスのパフォーマンス要求を軽減でき、ネットワークトラフィックを生成するアプリケーションが多数ある場合に役立つ可能性があります。

トラフィック フロー モニタリングについて

ここでは、トラフィック フロー モニタリングについて説明します。

Cflowd を使用したトラフィック フロー モニタリングの概要

Cflowd は、Flexible NetFlow (FNF) トラフィックデータの分析に使用されるフロー分析ツールです。オーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイスを通過するトラフィックをモニタリングし、フロー情報をコレクタにエクスポートします。コレクタでは、フロー情報を IP Flow Information Export (IPFIX) アナライザで処理できます。トラフィックフローの場合、Cflowd は定期的にテンプレートレポートをフローコレクタに送信します。このレポートには、フローに関する情報が含まれており、データはこれらのレポートのペイロードから抽出されます。

Cflowd コレクタの場所、サンプリングされた一連のフローがコレクタに送信される頻度、およびテンプレートがコレクタに送信される頻度を定義する Cflowd テンプレートを作成できます (Cisco SD-WAN コントローラ および Cisco SD-WAN Manager)。Cisco IOS XE Catalyst SD-WAN デバイス ごとに最大 4 つの Cflowd コレクタを設定できます。Cflowd テンプレートを有効にするには、適切なデータポリシーを使用して適用します。

少なくとも 1 つの Cflowd テンプレートを設定する必要がありますが、パラメータを含める必要はありません。パラメータを指定しない場合、ノードのデータフローキャッシュはデフォルト設定で管理され、フローのエクスポートは行われません。

Cflowd トラフィック フロー モニタリングは FNF と同等です。

Cflowd ソフトウェアは、RFC 7011 および RFC 7012 で指定されている Cflowd バージョン 10 を実装しています。Cflowd バージョン 10 は、IP Flow Information Export (IPFIX) プロトコルとも呼ばれます。



Cflowd は、1:1 のサンプリングを実行します。すべてのフローに関する情報が Cflowd レコードに集約されます。フローはサンプリングされません。Cisco IOS XE Catalyst SD-WAN デバイスはコレクタにエクスポートされるレコードをキャッシュしません。



- (注) セキュアインターネットゲートウェイ (SIG) トンネル上の NetFlow は、Cisco IOS XE Catalyst SD-WAN デバイス ではサポートされていません。

Cflowd と SNMP の比較

Cflowd は、サービス側のトラフィックをモニタリングします。Cflowd は主に、LAN から WAN、WAN から LAN、LAN から LAN、および DIA へのトラフィックをモニタリングします。Cflowd と SNMP を使用して LAN インターフェイス (入力または出力) のトラフィックをモニタリングする場合、パケット数とバイト数は類似するはずですが、バイトの違いは、SNMP は L2 ヘッダーから始まりますが、Cflowd は L3 ヘッダーから始まります。ただし、Cflowd や SNMP を使用して WAN インターフェイス (入力または出力) のトラフィックをモニタリングする場合、パケットやバイトが同じになることはほぼありません。WAN インターフェイスのすべて

のトラフィックは、サービス側のトラフィックではありません。たとえば、CflowdはBFDトラフィックをモニタリングしませんが、SNMPはモニタリングします。CflowdとSNMPのトラフィックの packets または bytes は同じではありません。

Cisco IOS XE Catalyst SD-WAN デバイス のための IPFIX 情報要素

Cisco Catalyst SD-WAN Cflowd ソフトウェアは、次の IP Flow Information Export (IPFIX) 情報要素を Cflowd コレクタにエクスポートします。フィールドは、使用しているリリースによって異なります。共通フィールドは、Cisco SD-WAN Manager および外部エクスポートにエクスポートされます。機能フィールドは Cisco SD-WAN Manager にのみエクスポートされます。

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以前の場合は、Flexible NetFlow がすべてのフィールドを外部コレクタと Cisco SD-WAN Manager にエクスポートします。Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降の場合は、FNF が次の表の要素（「対応」とマークされている要素）を外部コレクタと Cisco SD-WAN Manager の両方にエクスポートします。**drop cause id** などの他のフィールドは特定の機能用であり、これらのフィールドは Cisco SD-WAN Manager にのみエクスポートされ、外部コレクタにはエクスポートされません。

Information Element (情報要素)	Element ID	外部コレクタへのエクスポート	説明	データタイプ	データ型セマンティクス	単位または範囲
sourceIPv4Address	8	対応	IP パケットヘッダー内の IPv4 送信元アドレス。	ipv4Address (4 バイト)	デフォルト	—
sourceIPv6Address	27	対応	IP パケットヘッダー内の IPv6 送信元アドレス。	ipv6Address (16 バイト)	デフォルト	—
destinationIPv4Address	12	対応	IP パケットヘッダー内の IPv4 宛先アドレス。	IPv4Address (4 バイト)	デフォルト	—
destinationIPv6Address	28	対応	IP パケットヘッダー内の IPv6 宛先アドレス。	ipv6Address (16 バイト)	デフォルト	—
ingressInterface	10	対応	このフローの packets が受信されている IP インターフェイスのインデックス。	unsigned32 (4 バイト)	identifier	—

Information Element (情報要素)	Element ID	外部コレクタへのエクスポート	説明	データタイプ	データ型セマンティクス	単位または範囲
ipDiffServCodePoint	195	対応	[差別化サービス (Differentiated Services)] フィールドでエンコードされる Differentiated Services Code Point (DSCP; DiffServ コードポイント) の値。このフィールドは、IPv4 TOS フィールドの最上位 6 ビットにまたがります。	unsigned8 (1 バイト)	identifier	0 ~ 63
protocolIdentifier	4	対応	IP パケットヘッダーのプロトコルフィールドにあるプロトコル番号の値。プロトコル番号は、IP パケットペイロードタイプを識別します。プロトコル番号は、IANA プロトコル番号レジストリで定義されています。	unsigned8 (1 バイト)	identifier	—
sourceTransportPort	7	対応	トランスポートヘッダー内の送信元ポート ID。トランスポートプロトコル (UDP、TCP、および SCTP) の場合、これは、それぞれのヘッダーで指定されている宛先ポート番号です。GRE および IPsec フローの場合、このフィールドの値は 0 です。	unsigned16 (2 バイト)	identifier	—
destinationTransportPort	11	対応	トランスポートヘッダー内の宛先ポート ID。トランスポートプロトコル (UDP、TCP、および SCTP) の場合、これは、それぞれのヘッダーで指定されている宛先ポート番号です。	unsigned16 (2 バイト)	identifier	—

Information Element (情報要素)	Element ID	外部コレクタへのエクスポート	説明	データタイプ	データ型セマンティクス	単位または範囲
tcpControlBits	6	対応	このフローのパケットに対して観測されるTCP制御ビット。この情報はビットフィールドとしてエンコードされます。TCP制御ビットごとに、このセット内にビットがあります。このフローの観測されたいずれかのパケットで、対応するTCP制御ビットが1に設定されている場合、このビットは1に設定されます。それ以外の場合、ビットは0に設定されます。このフィールドの値については、「IANA IPFIX」 Web ページを参照してください。	unsigned8 (1 バイト)	identifier	—
flowEndReason	136	対応	フロー終了の理由。このフィールドの値については、「IANA IPFIX」 Web ページを参照してください。	unsigned8 (1 バイト)	identifier	—
ingressoverlaysessionid	12432	対応	入力オーバーレイセッションIDの32ビット識別子。	unsigned32 (4 バイト)	identifier	—
VPN 識別子	企業固有	対応	Cisco IOS XE Catalyst SD-WAN デバイス VPN 識別子 デバイスはVIP_IANA_ENUM または 41916 のエンタープライズ ID を使用し、VPN 要素 ID は 4321 です。	unsigned32 (4 バイト)	identifier	0 ~ 65535
connection id long	12441	対応	クライアントとサーバー間を接続するための64ビット識別子。	Unsigned64 (8 バイト)	identifier	—
application id	95	対応	アプリケーション名の32ビット識別子	unsigned32 (4 バイト)	identifier	—
egressInterface	14	対応	このフローのパケットが送信されているIPインターフェイスのインデックス。	unsigned32 (4 バイト)	デフォルト	—

Information Element (情報要素)	Element ID	外部コネクタへのエクスポート	説明	データタイプ	データ型セマンティクス	単位または範囲
egressoverlaysessionid	12433	対応	出力オーバーレイセッションIDの32ビット識別子。	unsigned32 (4 バイト)	identifier	—
sdwan qos-queue-id	12446	未対応	QoS のキューインデックス。	unsigned8 (1 バイト)	identifier	—
drop cause id	12442	未対応	ドロップ原因名の16ビット識別子。	unsigned16 (2 バイト)	identifier	—
counter bytes sdwan dropped long	12443	未対応	観測ポイントの計測プロセスが初期化または再初期化されて以降、観測ポイントにおけるこのフローの流入パケットのうちドロップしたオクテットの総数。 この数には、IPヘッドとIPペイロードが含まれます。	unsigned64 (8 バイト)	totalCounter	Octets
sdwan sla-not-met	12444	未対応	必要なSLAが満たされているかどうかを示すboolean値。	unsigned8 (1 バイト)	identifier	—
sdwan preferred-color-not-met	12445	未対応	優先色が満たされているかどうかを示すboolean値。	unsigned8 (1 バイト)	identifier	—
counter packets sdwan dropped long	42329	未対応	観測ポイントの計測プロセスが初期化または再初期化されて以降、観測ポイントにおけるこのフローの流入パケットのうちドロップしたパケットの総数。	unsigned64 (8 バイト)	totalCounter	パケット
octetDeltaCount	1	対応	観測ポイントにおけるこのフローの流入パケットにおける前回レポート以降のオクテットの数。この数には、IPヘッダーとIPペイロードが含まれます。	unsigned64 (8 バイト)	deltaCounter	Octets
packetDeltaCount	2	対応	この観測ポイントにおけるこのフローに関する前回レポート以降の流入パケット数。	unsigned64 (8 バイト)	deltaCounter	パケット
flowStartMilliseconds	152	対応	このフローの先頭パケットの絶対タイムスタンプ。	dateTime-MilliSeconds (8 バイト)	—	—

Information Element (情報要素)	Element ID	外部コレクタへのエクスポート	説明	データ タイプ	データ型セマンティクス	単位または範囲
flowEndMilliseconds	153	対応	このフローの最終パケットの絶対タイムスタンプ。	dateTime-MilliSeconds (8 バイト)	—	—
ip tos	5	対応	IP ヘッダーの [タイプオブサービス (Type of Service)] フィールド。	unsigned8 (1 バイト)	identifier	8 ビット
dscp output	98	対応	[差別化サービス (Differentiated Services)] フィールドでエンコードされる DSCP の値。このフィールドは、IPv4 TOS フィールドの最上位 6 ビットにまたがります。	unsigned8 (1 バイト)	identifier	0 ~ 63
フロー サンプラ	48	対応	少なくとも 1 つの物理インターフェイスに適用される NetFlow サンプラマップで定義される特性のセット。	unsigned8 (1 バイト)	identifier	—
bfd avg latency	45296	対応	各トンネルの Bidirectional Forwarding Detection (BFD) 平均遅延の計算	unsigned64 (8 バイト)	identifier	—
bfd avg loss	45295	対応	各トンネルの BFD 平均損失の計算	unsigned64 (8 バイト)	identifier	—
bfd avg jitter	45297	対応	各トンネルの BFD 平均ジッターの計算	unsigned64 (8 バイト)	identifier	—
bfd rx cnt	45299	対応	受信した BFD パケットの数	unsigned64 (8 バイト)	deltaCounter	—
bfd tx cnt	45300	対応	送信された BFD パケットの数	unsigned64 (8 バイト)	deltaCounter	—
bfd rx octets	45304	対応	受信した BFD オクテットの数	unsigned64 (8 バイト)	deltaCounter	—
bfd tx octets	45305	対応	送信された BFD オクテットの数	unsigned64 (8 バイト)	deltaCounter	—

Information Element (情報要素)	Element ID	外部コネクタへのエクスポート	説明	データタイプ	データ型セマンティクス	単位または範囲
application_CATEGORY	12232	対応	アプリケーションカテゴリ名、各アプリケーションタグの第1レベルの分類	変数長	identifier	—
application_SUB_CATEGORY	12233	対応	アプリケーションサブカテゴリ名、各アプリケーションタグの第2レベルの分類	変数長	identifier	—
applicaiton_GROUP	12234	対応	アプリケーショングループ名。同じアプリケーションに属する複数のアプリケーションタグをグループ化したもの。	変数長	identifier	—
application traffic-class	12243	対応	SRND モデルに基づくアプリケーショントラフィッククラス	変数長	identifier	—
application business-relevance	12244	対応	ビジネス関連のアプリケーション	変数長	identifier	—

VPN0 インターフェイスに対する Flexible NetFlow

Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a から、Cisco IOS XE Catalyst SD-WAN デバイスの VPN0 インターフェイスで双方向トラフィックの可視性を確保するために FNF を有効にできます。

NetFlow は、デバイスを通過するパケットの統計情報を提供し、トンネルまたはサービス VPN の識別に役立ちます。VPN0 上の Flexible NetFlow は、Cisco IOS XE SD-WAN デバイス上の VPN0 に到達するすべてのトラフィック（入力と出力の両方）を可視化します。

プロファイルは、コンテキストに対して有効または無効にできる、事前定義された一連のトラフィックです。Easy Performance Monitor (ezPM) プロファイルを作成すると、モニターをすばやくプロビジョニングすることができます。この新しいメカニズムを利用すると、モニターのプロビジョニングに従来使用していた方法に影響を与えることなく新機能を導入することができます。この機能の一部として、**sdwan-fnf** プロファイルを作成して、NetFlow VPN0 設定を通過するトラフィックをモニタリングできます。

コンテキストは、インターフェイスの入力方向と出力方向の両方に付加される Performance Monitor ポリシー マップに相当します。コンテキストには、イネーブルにする必要があるトラフィック モニタに関する情報が含まれています。インターフェイスにコンテキストが付加されると 2 つのポリシーマップが作成され、入力方向と出力方向にそれぞれ 1 つずつ適用されます。トラフィック モニタで指定されている方向に基づいてポリシーマップが付加されるとトラ

フィックの監視が開始されます。コンテキストを編集して定義済みの方向を変更することもできます。

また、1つのプロファイルをベースに、トラフィック モニタ、エクスポータ、パラメータなどを変更して、選択したトラフィック モニタごとに複数のコンテキストを作成することもできます。1つの ezPM コンテキストを複数のインターフェイスに付加することもできます。1つのインターフェイスにアタッチできるコンテキストは1つだけです。

表 36: Flexible NetFlow のコンポーネント

	Cisco Catalyst SD-WAN Flexible Netflow	Cisco vManage リリース 20.7.1 以降の Cisco SD-WAN NetFlow VPN0
設定	ローカライズ型ポリシー : app-visibility または flow-visibility 一元管理型ポリシー : cflowd policy Cisco SD-WAN Manager 機能テンプレートと CLI テンプレートの両方でサポートされます。	コマンド performance monitor context xxx profile s を使用して Flexible NetFlow VPN0 モニターを定義し、VPN0 インターフェイスにアタッチします。 Cisco SD-WAN Manager の CLI テンプレートおよび CLI 機能テンプレートでサポートされています。
インターフェイス	Cisco Catalyst SD-WAN トンネルインターフェイスおよびサービス VPN インターフェイス	Cisco Catalyst SD-WAN トンネルおよび VPN インターフェイスを除く VPN0 インターフェイス
フロー レコード	デフォルトでは固定レコード。 FEC、パケット複製、SSL プロキシなどのレコードの動的モニタリングをサポートします。また、一元管理型ポリシーのタイプオブサービス (ToS)、サンプラー ID、および再マークされた DSCP 値の収集もサポートします。	固定レコード。新しいフィールドを変更または追加することはできません。
フローの方向	入力フローのみをサポート。	デフォルトで入力と出力の両方をサポートします。
アプリケーション用 NBAR	Network-Based Application Recognition (NBAR) は、 app-visibility が定義されている場合にのみ有効になります。	NBAR はデフォルトで有効になっています。
エクスポータ	JSON ファイルを Cisco SD-WAN Manager に、IPFIX を外部コレクタにエクスポートします。	Cisco SD-WAN Manager にエクスポートできません。外部コレクタへの IPFIX

VPN0 インターフェイスでの Flexible Netflow の制限

- VPN0 での Flexible NetFlow は Cisco Catalyst SD-WAN トンネルおよび Cisco Catalyst SD-WAN VPN インターフェイスでサポートされていません。

- VPN0 トラフィックの FNF レコードは固定レコードであり、変更できません。
- Cisco Catalyst SD-WANVPN0 フローエントリは、CLI 設定で定義された外部コレクタに報告されますが、Cisco SD-WAN Manager には報告されません。
- OMP、Netconf、SSH などの Cisco Catalyst SD-WAN BFD および Cisco Catalyst SD-WAN 制御接続は、Datagram Transport Layer Security (DTLS) または Transport Layer Security (TLS) トンネルによってカプセル化されます。FNF は DTLS トラフィックについてのみを報告し、カプセル化されたプロトコルパケットについては報告しません。
- VPN0 WAN インターフェイスに FNF が設定されている場合、
 - 入力フロー (WAN > Cisco Catalyst SD-WAN - トンネル > LAN) では、出力インターフェイスは NULL として報告されます。
 - 出力フロー (LAN > Cisco Catalyst SD-WAN - トンネル > WAN) では、入力インターフェイスは WAN インターフェイス (Cisco Catalyst SD-WAN アンダーレイトンネル) として報告されます。
- VPN0 モニターは、IPv4 および IPv6 プロトコルのみをサポートします。
- OSPF、BGP などのルーティングプロトコルについては、出力トラフィックのみがサポートされます。入力 OSPF および BGP トラフィックは、高プライオリティパケットとして扱われます。
- Cflowd フローエクスポートの送信元インターフェイスとしてサポートされるのは、ループバック インターフェイスのみです。
- FNF は、パケットが外部コレクタに送信されるときに、元の DSCP 値のみを記録します。FNF は入力フローのみをサポートします。

Flexible NetFlow 分散エクスポート

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1

Cisco IOS XE Catalyst SD-WAN デバイス で Flexible NetFlow 分散エクスポートを有効にする機能です。分散エクスポート機能は、モニターキャッシュ内のレコードのエクスポートを一定の時間間隔で分散して、コレクタのパフォーマンスを向上させます。同期キャッシュの場合、すべてのネットワークデバイスがモニターキャッシュ内のレコードを同時にエクスポートします。複数のネットワークデバイスに同じモニター間隔と同期キャッシュが設定されている場合、コレクタはすべてのデバイスからすべてのレコードを同時に受信することもあるため、そのパフォーマンスに影響が出る可能性があります。分散エクスポートの時間間隔を設定して、一定の時間間隔でエクスポートを分散させてください。

コレクタのパフォーマンスに影響が出ないようにするため、所定の時間間隔でレコードをエクスポートし、レコードのエクスポートをキャッシュタイムアウトの間、均等に分散させます。

FNF エクスポートはオプションテンプレートとデータテンプレートを使用して設定してください。システムレベルの属性を設定するには、オプションテンプレートを使します。フローレコードと対応するデータを設定するには、データテンプレートを使用します。

export-spread を有効化する場合は、次の 3 つの分散間隔を以下のように設定してください。

- **app-table** : application-table、application-attributes のオプションテンプレート
- **tloc-tables** : tunnel-tloc-table オプションテンプレート

Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a と Cisco vManage リリース 20.10.1 で導入された bfd-metric-table は、tloc-table カテゴリに属します。

- **other-tables** : その他のオプションテンプレート

次に、分散間隔の仕組みについて例を示します。

- app-table が 10 の application-attributes または application-table で設定されている場合、オプションテンプレート パケットはすべての属性に対して 10 秒で均等に送信されます。
- デフォルトインターバルは 1 秒です。したがって、分散エクスポートでは、10 秒の大きなトラフィックバースト 1 件が、それぞれ 1 秒の小さなバースト 10 件に分散されます。

Flexible NetFlow オプションテンプレート パケットは、timeout オプションで設定されたバーストとして定期的に送信されます。分散エクスポート間隔では、オプションテンプレート パケットをバーストとして送信する代わりに、パケットをタイムアウトおよび分散エクスポート間隔で分散させます。

Cisco vManage リリース 20.8.1 とそれ以前のリリースでは、60 秒ごとにオプションテンプレート パケットがバーストとして送信されます。たとえば、1000 個のパケットがある場合、60 秒経ったときに 1000 個すべてのパケットがキューに入れられるため、パケットがドロップされます。

分散エクスポートを設定すると、60 秒経ったときに送信されるパケットが 1000 個ある場合に、100 パケットを 10 秒で 100 パケットのレートで送信し、エクスポートバーストを回避します。エクスポートの展開が指定されない場合、デフォルトの動作は、即時エクスポートです。

分散エクスポートをサポートしていない以前のバージョンからアップグレードする場合、Cflowd テンプレートのデフォルトの分散値は無効になります。

Flexible NetFlow による BFD メトリックのエクスポート

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

Flexible NetFlow (FNF) による BFD メトリックのエクスポート機能を使用すると、BFD テレメトリデータを外部 FNF コレクタにエクスポートして、トンネルごとの平均ジッター、平均遅延、および損失を分析できます。ジッターと遅延はマイクロ秒単位で測定されます。損失は、1% の 100 分の 1 単位 (0.01%) で測定されます。この機能により、ネットワーク状態データのモニタリングが強化され、収集が高速化されます。

BFD メトリックのエクスポート用である新しいオプションテンプレート `bfd-metric-table` が追加されました。

Cisco SD-WAN Manager 機能テンプレートまたは Cisco SD-WAN コントローラ の CLI を使用して、Cisco IOS XE Catalyst SD-WAN デバイス で BFD メトリックのエクスポートを設定します。Cisco SD-WAN Manager 機能テンプレートを使用した BFD メトリックのエクスポートの設定の詳細については、「[Configure Cflowd Monitoring Policy](#)」を参照してください。CLI を使用した BFD メトリックのエクスポートの設定の詳細については、「[Configure Flexible Netflow with Export of BFD Metrics Using the CLI](#)」を参照してください。

BFD メトリックのエクスポートの仕組み

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

Cisco IOS XE Catalyst SD-WAN デバイス は、IP Flow Information Export (IPFIX) パケットを外部コレクタに送信するようになっています。Cisco SD-WAN コントローラ または Cisco SD-WAN Manager で BFD エクスポート間隔を設定すると、転送テーブルマネージャ (FTM) によって送信元メトリックが生成されます。

• 例 1 :

Cisco IOS XE Catalyst SD-WAN デバイス をリポートすると、デバイスは、設定した BFD エクスポート間隔に従って BFD メトリックをエクスポートします。この時点では、FTM にはエクスポートするデータがありません。その結果、[TLOC テーブルオーバーレイセッション ID (TLOC TABLE OVERLAY SESSION ID)] フィールドを除くすべてのフィールドに、次の無効な値が含まれることになります。

0xFFFFFFFF

例 2 :

- データを送信するための FTM 間隔が BFD エクスポート間隔より大きくなっています。この状況では、FTM がデータを 1 回だけ送信しても、データが 2 回エクスポートされる可能性があります。結果的に、FTM から新しいデータを受信しないことになります。BFD メトリックとタイムスタンプは、最後のパケットと同じになります。

外部コレクタに送信される BFD テレメトリデータの例については、「[Flexible NetFlow による BFD メトリックのエクスポート設定例](#)」を参照してください。

SAIE フローを使用した Cflowd トラフィックフローモニタリング

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1

この機能を使用すると、Cflowd フローと SAIE フローの両方をモニタリングするための 2 つの Cisco SD-WAN Manager リアルタイム デバイス オプションを選択できます。

SAIE フローの詳細については、「[SD-WAN Application Intelligence Engine Flow](#)」の章を参照してください。

この機能を使用すると、選択した Cisco IOS XE Catalyst SD-WAN デバイスの VPN 内で実行されている特定のアプリケーションまたはアプリケーションファミリを表示するためのフィルタを適用できます。

Cflowd および SAIE フローのデバイス フィルタリング オプションの詳細については、『*Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*』の「[Devices and Controllers](#)」の章を参照してください。

SAIE フローを使用した Cflowd トラフィック フロー モニタリングの利点

- ネットワークトラフィックの可視性が向上し、ネットワークオペレータがネットワークの使用状況を分析し、ネットワークパフォーマンスを向上させることができます。
- Cisco IOS XE Catalyst SD-WAN デバイスのリアルタイムモニタリングを提供します。
- Cisco IOS XE Catalyst SD-WAN デバイスの Cisco SD-WAN Manager のリアルタイム デバイス オプションのパリティを提供します。

SAIE フローを使用した Cflowd トラフィック フロー モニタリングの前提条件

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1

Cflowd with SAIE フローデバイスオプションを表示する前に、アプリケーションとフローの可視性を設定します。

アプリケーションフローの可視性の設定の詳細については、[アプリケーション可視性のグローバルな設定 \(245 ページ\)](#) を参照してください。

グローバルフローの可視性の設定の詳細については、[グローバルフローの可視性の設定 \(242 ページ\)](#) を参照してください。

SAIE フローを使用した Cflowd トラフィック フロー モニタリングに関する制約事項

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1

- Cisco SD-WAN Manager で一度に表示できる Cflowd レコードは 4001 件のみです。
- 2人の異なるユーザーが同じデバイスから同じクエリに同時にアクセスしようとした場合、Cisco IOS XE Catalyst SD-WAN デバイスが処理するのは、最初のリクエストのみです。2番目のユーザーは、最初のリクエストがタイムアウトになるため、リクエストを再送信する必要があります。
- SAIE を使用した Cflowd の検索フィルタは、取得された 4001 Cflowd フローレコードと照合されます。
- 有効な結果を返せるよう、検索フィルタには、アプリケーションまたはアプリケーションファミリをフルネームで入力します。

たとえば、**netbios-dgm** アプリケーションを検索する場合に、アプリケーションまたはアプリケーションファミリに **netbios** と入力しても、正しい結果は表示されません。

集約データの最大 FNF レコードレートの設定に関する情報

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.1

raw および集約トラフィックフローデータ

トラフィックフローの可視性が有効になっている場合（「[グローバルフローの可視性の設定](#)」を参照）、ネットワーク内のデバイスは、raw および集約トラフィックフローデータを Cisco SD-WAN Manager に送信します。

フローデータを集約するために、ルータは、複数のフローの raw データを統合するためのキーとして 4 タプルのフローデータ（VPN ID、アプリケーション名、フローの入力インターフェイス、およびフローの出力インターフェイスを含む）を使用します。ルータは、4 タプルが同一である各フローを単一の集約 FNF レコードに統合します。

Cisco SD-WAN Manager は、集約データを使用して、ネットワークトラフィックフロー情報の概要を表示します。集約データには、トラフィックを生成しているネットワークアプリケーションが表示されますが、完全なトラフィックフローデータほど詳細ではありません。トラフィックフローの送信元アドレスと宛先アドレス、または送信元ポートと宛先ポートは提供されません。

トラフィックフローの詳細を表示するには、オンデマンドのトラブルシューティングなどの機能を使用します。オンデマンドのトラブルシューティングの詳細については、「[On-Demand Troubleshooting](#)」を参照してください。

最大 FNF レコードレート

デバイスが送信できる集約トラフィックデータ FNF レコードの最大レート（1分あたりのレコード数）を設定して、デバイスのパフォーマンス要求（CPU およびメモリ）を軽減できます。これは、ネットワークトラフィックを生成するアプリケーションが多数ある場合に役立つ可能性があります。この設定の詳細については、[CLI コマンドを使用した集約データの最大 FNF レコードレートの設定](#)（261 ページ）を参照してください。

トラフィックフローモニタリングの制約事項

ここでは、トラフィックフローモニタリングに関連する注意事項、制限事項、および制約事項について説明します。

ループバックを TLOC として使用する場合のフローテレメトリでの収集ループバックの有効化に関する制約事項

- Cisco Catalyst SD-WAN コントローラ CLI または Cisco SD-WAN Manager CLI テンプレートを介した設定のみをサポートします。機能テンプレートは、このリリースではサポートされていません。
- FNF VPN0 インターフェイスでの収集ループバックはサポートされていません。
- 専用インターネットアクセス (DIA) シナリオでの収集ループバックはサポートされていません。
- マルチテナントシナリオはサポートされていません。

トラフィック フロー モニタリングの設定

ここでは、トラフィック フロー モニタリングの設定について説明します。

Cisco IOS XE Catalyst SD-WAN デバイスでのトラフィック フロー モニタリングの設定

Cflowd トラフィック フロー モニタリングでは、Flexible NetFlow (FNF) を使用してトラフィック データをエクスポートします。Cflowd モニタリングを設定するには、次の手順を実行します。

グローバルフローの可視性の設定

LAN 内のすべての VPN からルータに着信するトラフィックのトラフィック フロー モニタリングを実行できるように、すべての Cisco IOS XE Catalyst SD-WAN デバイスで Cflowd の可視性をグローバルに有効にします。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Policies]** の順に選択します。
2. **[Localized Policy]** をクリックします。
3. **[Add Policy]** をクリックします。
4. **[次へ (Next)]** をクリックして、**[ポリシー概要 (Policy Overview)]**、**[ポリシー設定 (Policy Settings)]** ページが表示されるまで、ウィザードページを進めます。
5. **[ポリシー名 (Policy Name)]** と **[ポリシーの説明 (Policy Description)]** を入力します。
6. **[Netflow]** チェックボックスをオンにして、IPv4 トラフィックのフローの可視性を有効にします。
7. **[Netflow IPv6]** チェックボックスをオンにして、IPv6 トラフィックのフローの可視性を有効にします。



- (注) SAIE 可視性で Cflowd トラフィックフローを設定する前に、IPv4 および IPv6 トラフィックのフロー可視性を有効にします。

Cflowd および SAIE フローのモニタリングの詳細については、『*Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*』の「[Devices and Controllers](#)」の章を参照してください。

8. トラフィックでドロップされたパケットをログに記録するように Cisco IOS XE Catalyst SD-WAN デバイスを設定するには、[暗黙的なACLロギング (Implicit ACL Logging)] をオンにします。

この設定では、システムでリンク障害が発生した場合に、暗黙的なアクセス制御リスト (ACL) によってドロップされたパケットを可視化できます。

9. [ログ頻度 (Log Frequency)] を入力します。

ログ頻度は、パケットフローがログに記録される頻度を決定します。最大値は 2147483647 です。最も近い 2 の累乗に切り捨てられます。たとえば、1000 の場合、ロギング頻度は 512 です。したがって、フロー内の 512 番目のパケットごとにログが記録されます。

10. IPv4 トラフィックの FNF キャッシュサイズを設定するには、[FNF IPv4 最大キャッシュエントリ (FNF IPv4 Max Cache Entries)] を入力します。

たとえば、次の例に示すように、IPv4/IPv6 トラフィックの FNF キャッシュを設定するには、100 と入力します。

11. IPv6 トラフィックの FNF キャッシュサイズを設定するには、[FNF IPv6 最大キャッシュエントリ (FNF IPv6 Max Cache Entries)] を入力します。

たとえば、次の例に示すように、IPv4/IPv6 トラフィックの FNF キャッシュを設定するには、100 と入力します。



- (注) 最小キャッシュサイズ値は 16 です。合計キャッシュサイズ (IPv4 キャッシュ + IPv6 キャッシュ) の最大値は、各プラットフォームの制限を超えることはできません。キャッシュサイズが定義されておらず、プラットフォームがリストにない場合、デフォルトの最大キャッシュエントリは 200k です。

最大キャッシュエントリは、Cflowd がモニタリングできる最大同時フローです。最大キャッシュエントリは、プラットフォームによって異なります。詳細については、[シスコサポート](#)にお問い合わせください。

次に、IPv4 と IPv6 の両方の flow-visibility を設定する例を示します。

```
policy
  flow-visibility
  implicit-acl-logging
  log-frequency 1000
  flow-visibility-ipv6
```

```
ip visibility cache entries 100
ipv6 visibility cache entries 100
```

policy flow-visibility または app-visibility を実行して FNF モニターを有効にすると、グローバルメモリ割り当ての失敗を示す次の警告メッセージが表示される場合があります。このログは、大きなキャッシュサイズで FNF モニタリング (policy flow-visibility または app-visibility) を有効にするとトリガーされます。

```
Jul  4 01:45:00.255: %CPPEXMEM-3-NOMEM: F0/0: cpp_cp_svr: QFP: 0, GLOBAL memory allocation
of 90120448 bytes by FNF failed
Jul  4 01:45:00.258: %CPPEXMEM-3-TOPUSER: F0/0: cpp_cp_svr: QFP: 0, Top User: CPR STILE
EXMEM GRAPH, Allocations: 877, Type: GLOBAL
Jul  4 01:45:00.258: %CPPEXMEM-3-TOPUSER: F0/0: cpp_cp_svr: QFP: 0, Top User: SBC, Bytes
Allocated: 53850112, Type: GLOBAL
```

警告メッセージは、必ずしもフロー モニター アプリケーションの障害を示しているわけではありません。警告メッセージは、外部メモリマネージャ (EXMEM) インフラストラクチャからメモリを適用するために FNF が使用する内部手順を示している可能性があります。

show platform hardware qfp active classification feature-manager exmem-usage コマンドを使用して、さまざまなクライアントの EXMEM メモリ使用率を表示します。

```
Device# show platform hardware qfp active active classification feature-manager exmem-usage
```

```
EXMEM Usage Information
```

```
Total exmem used by CACE: 39668
```

Client	Id	Total VMR	Total Usage	Total%	Alloc	Free
acl	0	11	2456	6	88	84
qos	2	205	31512	79	7	5
fw	4	8	892	2	2	1
obj-group	39	82	4808	12	5	2

FNF モニターが正常に有効になっていることを確認するには、**show flow monitor monitor-name** コマンドを使用して、フローモニターのステータス (allocated または not allocated) を確認します。

```
Device# show flow monitor sdwan_flow_monitor
```

```
Flow Monitor sdwan_flow_monitor:
```

```
Description:      monitor flows for vManage and external collectors
Flow Record:      sdwan_flow_record-003
Flow Exporter:    sdwan_flow_exporter_1
                  sdwan_flow_exporter_0
```

```
Cache:
```

```
Type:             normal (Platform cache)
Status:           allocated
Size:             250000 entries
Inactive Timeout: 10 secs
Active Timeout:   60 secs
```

```
Trans end aging:  off
```

```
SUCCESS
```

```
Status:          allocated
```

```
FAILURE
```

```
Status:          not allocated
```

アプリケーション可視性のグローバルな設定

LAN 内のすべての VPN からルータに着信するトラフィックのトラフィックフローモニタリングを実行できるように、すべての Cisco IOS XE Catalyst SD-WAN デバイスで Cflowd の可視性をグローバルに有効にします。

app-visibilityにより、nbar は、LAN 内のすべての VPN からルータに着信するフローの各アプリケーションを確認できます。app-visibility または app-visibility-ipv6 が定義されている場合、nbar は IPv4 と IPv6 の両方のフローに対してグローバルに有効になります。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Policies]** の順に選択します。
2. **[Localized Policy]** をクリックします。
3. **[Add Policy]** をクリックします。
4. **[次へ (Next)]** をクリックして、**[ポリシー概要 (Policy Overview)]**、**[ポリシー設定 (Policy Settings)]** ページが表示されるまで、ウィザードページを進めます。
5. **[ポリシー名 (Policy Name)]** と **[ポリシーの説明 (Policy Description)]** を入力します。
6. **[アプリケーション (Application)]** チェックボックスをオンにして、IPv4 トラフィックのアプリケーションの可視性を有効にします。
7. **[アプリケーション IPv6 (Application IPv6)]** チェックボックスをオンにして、IPv6 トラフィックのアプリケーションの可視性を有効にします。



(注) SAIE 可視性で Cflowd トラフィックフローを設定する前に、IPv4 および IPv6 トラフィックのアプリケーション可視性を有効にします。

Cflowd および SAIE フローのモニタリングの詳細については、『*Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*』の「[Devices and Controllers](#)」の章を参照してください。

8. IPv4 トラフィックの FNF キャッシュサイズを設定するには、**[FNF IPv4 最大キャッシュエントリ (FNF IPv4 Max Cache Entries)]** を入力します。
たとえば、IPv4 トラフィックの FNF キャッシュサイズを設定するには、次の例に示すように 100 と入力します。
9. IPv6 トラフィックの FNF キャッシュサイズを設定するには、**[FNF IPv6 最大キャッシュエントリ (FNF IPv6 Max Cache Entries)]** を入力します。
たとえば、IPv6 トラフィックの FNF キャッシュサイズを設定するには、次の例に示すように 100 と入力します。

次の例は、IPv4 と IPv6 の両方に対する application visibility の設定を示しています。

```
policy
  app-visibility

  app-visibility-ipv6
```

```
ip visibility cache entries 100
ipv6 visibility cache entries 100
!
```



(注) **policy app-visibility** コマンドは、**nbar** を有効にしてアプリケーション名を取得することで、グローバルフローの可視性も有効にします。



(注) Cflowd global flow-visibility を設定しても、Cflowd app-visibility を設定していない場合、Cisco SD-WAN Manager にエクスポートされたアプリケーションは不明という結果を返します。IPFIX アナライザを使用して外部コレクタにエクスポートされた同じアプリケーションに、誤ったアプリケーション名が含まれている可能性があります。

アプリケーション名を保持する場合は、Cflowd app-visibility を定義してこの問題を回避します。

Cflowd モニタリングポリシーの設定

Cflowd トラフィック フロー モニタリングのポリシーを設定するには、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、4連続のページ構成となっており、これに従って操作を進めていくと、次のようなポリシーコンポーネントの作成および編集ができます。

1. [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、ポリシーのマッチ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。
2. [トポロジの設定 (Configure Topology)] : ポリシーが適用されるネットワーク構造を作成します。
3. [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。
4. [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。

ポリシー構成ウィザードの最初の3ページで、ポリシーコンポーネント、つまりブロックを作成します。最後のページで、オーバーレイネットワークのサイトとVPNにポリシーブロックを適用します。Cflowd ポリシーを有効にするには、ポリシーをアクティブ化します。

1. Cisco SD-WAN Manager メニューから、[設定 (Configuration)] > [ポリシー (Policies)] の順に選択します。
2. [カスタムオプション (Custom Options)] をクリックします。
3. [一元管理型ポリシー (Centralized Policy)] で、[トラフィックポリシー (Traffic Policy)] をクリックします。

4. [Cflowd] をクリックします。
5. [ポリシーの追加 (Add Policy)] をクリックしてから、[新規作成 (Create New)] をクリックします。
6. 新しいポリシーの名前と説明を [名前 (Name)] と [説明 (Description)] に入力します。
7. [Cflowd テンプレート (Cflowd Template)] セクションで、アクティブフローのタイムアウト範囲を [アクティブフロータイムアウト (Active Flow Timeout)] に入力します。
8. [非アクティブフロータイムアウト (Inactive Flow Timeout)] フィールドに、非アクティブフローのタイムアウト範囲を入力します。
9. [フローの更新 (Flow Refresh)] フィールドに、フローの更新間隔を入力します。
10. [サンプリング間隔 (Sampling Interval)] フィールドに、サンプル期間を入力します。
11. [プロトコル (Protocol)] ドロップダウンリストで、オプションを選択します。

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降では、オプションから [IPv4] または [両方 (Both)] を選択すると、[詳細設定 (Advanced Settings)] フィールドが表示されます。

12. [詳細設定 (Advanced Settings)] で次の手順を実行して、追加の IPv4 フローレコードを収集します。
 - [TOS] チェックボックスをオンにします。
 - [DSCPのリマーク (Re-marked DSCP)] チェックボックスをオンにします。
13. [コレクタリスト (Collector List)] で [新しいコレクタ (New Collector)] をクリックします。コレクタは最大 4 つまで設定できます。
 1. [VPN ID] フィールドには、コレクタが配置されている VPN の番号を入力します。
 2. [IPアドレス (IP Address)] フィールドには、コレクタの IP アドレスを入力します。
 3. [ポート (Port)] フィールドには、コレクタのポート番号を入力します。
 4. [トランスポートプロトコル (Transport Protocol)] ドロップダウンリストでは、コレクタに到達するために使用するトランスポートタイプを選択します。
 5. [送信元インターフェイス (Source Interface)] フィールドに、フローをコレクタに送信するために使用するインターフェイスの名前を入力します。
 6. [分散エクスポート (Export Spreading)] フィールドにある、[有効 (Enable)] または [無効 (Disable)] オプションボタンをクリックします。

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降では、[分散エクスポート (Export Spreading)] フィールドを使用して、キャッシュの同期化によって発生するエクスポートストームを防ぐことができます。直前の間隔でのエクスポートが現在の間隔中に展開されることにより、エクスポートストームが回避されます。

7. [BFDメトリックのエクスポート (BFD Metrics Exporting)]フィールドにある、[有効 (Enable)]または[無効 (Disable)]オプションボタンをクリックします。

Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1 以降では、[BFDメトリックのエクスポート (BFD Metrics Exporting)]フィールドを使用して、損失、ジッター、および遅延の BFD メトリックを収集できます。

8. [エクスポート間隔 (Exporting Interval)]フィールドで、BFD メトリックを送信する間隔を秒単位で指定します。

Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1 以降では、[エクスポート間隔 (Exporting Interval)]フィールドを使用して、BFD メトリックのエクスポート間隔を指定できます。

BFD メトリックのエクスポートを有効にすると、[エクスポート間隔 (Exporting Interval)]フィールドが表示されます。

[エクスポート間隔 (Exporting Interval)]フィールドにより、BFD メトリックが送信される間隔が制御されます。

デフォルトの BFD エクスポート間隔は 600 秒です。

フィールド	説明
[Cflowd ポリシー名 (Cflowd Policy Name)]	Cflowd ポリシーの名前を入力します。
説明	Cflowd ポリシーの説明を入力します。
[アクティブフロータイムアウト (Active Flow Timeout)]	アクティブフローのタイムアウト値を入力します。指定できる範囲は 30 ~ 3600 秒です。 アクティブフロータイムアウトは、長時間継続したフローの NetFlow レコードがエクスポートされる時間間隔です。
[非アクティブフロータイムアウト (Inactive Flow Timeout)]	非アクティブフローのタイムアウト値を入力します。指定できる範囲は 1 ~ 3600 秒です。 非アクティブフロータイムアウトは、フローキャッシュからエクスポートされる一定期間 (15秒など) にフローがアクティブでない時間間隔です。
[フローの更新 (Flow Refresh)]	Cflowd レコードを外部コレクタに送信する間隔を入力します。指定できる範囲は 60 ~ 86400 秒です。
Sampling Interval	サンプル期間を入力します。指定できる範囲は 1 ~ 65536 秒です。 サンプリング間隔は、パケット内のサンプルの 1 つを収集するのにかかる時間です。

フィールド	説明
Protocol	ドロップダウンリストからトラフィックプロトコルのタイプを選択します。オプションは、[IPv4]、[IPv6]、または [両方 (Both)] です。 デフォルトのプロトコルは [IPv4] です。
TOS	[TOS] チェックボックスをオンにします。 こうすることで、IPv4 ヘッダーのフィールドタイプが示されます。
[DSCPのリマーク (Re-marked DSCP)]	[DSCPのリマーク (Re-marked DSCP)] チェックボックスをオンにします。 こうすることで、リマークされたデータポリシーによって指定されたトラフィック出力が示されます。
VPN ID	VPN ID を入力します。指定できる範囲は 0 ~ 65536 です。
IP Address	コレクタの IP アドレスを入力します。
Port	コレクタのポート番号を入力します。指定できる範囲は 1024 ~ 65535 です。
トランスポート プロトコル	ドロップダウンリストから、コレクタに到達するためのトランスポートタイプを選択します。 オプションは、[TCP] または [UDP] です。
Source Interface	ドロップダウンリストから送信元インターフェイスを選択します。
分散エクスポート	[有効 (Enable)] または [無効 (Disable)] オプションボタンをクリックして、分散エクスポートを設定します。 デフォルトは [無効 (Disable)] です。
[BFD メトリックのエクスポート (BFD Metrics Exporting)]	[有効 (Enable)] または [無効 (Disable)] オプションボタンをクリックして、Bidirectional Forwarding Detection (BFD) メトリックのエクスポートを設定します。 デフォルトは [無効 (Disable)] です。
[エクスポート間隔 (Exporting Interval)]	BFD メトリックを外部コレクタに送信するエクスポート間隔を秒単位で入力します。整数値を入力してください。 このフィールドは、BFD メトリックのエクスポートを有効にした場合にのみ表示されます。 デフォルトの BFD エクスポート間隔は 600 秒です。

14. [Cflowdポリシーの保存 (Save Cflowd Policy)] をクリックします。

Cflowd 情報の表示

Cflowd の情報を表示するには、Cisco IOS XE Catalyst SD-WAN デバイス で次のコマンドを使用します。

- show sdwan app-fwd cflowd collector
- show sdwan app-fwd cflowd flow-count
- show sdwan app-fwd cflowd flows [vpn *vpn-id*] format table
- show sdwan app-fwd cflowd statistics
- show sdwan app-fwd cflowd template [name *template-name*]
- show sdwan app-fwd cflowd flows format table

次の出力例は、Cflowd の情報を表示したものです。

```
Device# show sdwan app-fwd cflowd flows
Generating output, this might take time, please wait ...
app-fwd cflowd flows vpn 1 src-ip 10.2.2.11 dest-ip 10.20.24.17 src-port 0 dest-port
2048 dscp 63 ip-proto 1
tcp-cntrl-bits          0
icmp-opcode            2048
total-pkts             6
total-bytes            600
start-time             "Fri May 14 02:57:23 2021"
egress-intf-name       GigabitEthernet5
ingress-intf-name      GigabitEthernet1
application            unknown
family                 network-service
drop-cause             "No Drop"
drop-octets            0
drop-packets           0
sla-not-met            0
color-not-met         0
queue-id               2
tos                    255
dscp-output            63
sampler-id             3
fec-d-pkts             0
fec-r-pkts             0
pkt-dup-d-pkts-orig    0
pkt-dup-d-pkts-dup     0
pkt-dup-r-pkts         0
pkt-cxp-d-pkts         0
traffic-category       0
```

Cflowd フローの詳細については、[show sdwan app-fwd cflowd flows](#) コマンドページを参照してください。

CLI を使用した、Cflowd トラフィック フロー モニタリングの設定

Cisco IOS XE Catalyst SD-WAN デバイス を制御している Cisco SD-WAN コントローラ の CLI から、次の手順を実行します。

1. Cflowd テンプレートを設定して、フローの可視性とフローのサンプリングパラメータを指定します。

```
vSmart(config)# policy cflowd-template template-name
vSmart(config-cflowd-template)# flow-active-timeout seconds
vSmart(config-cflowd-template)# flow-inactive-timeout seconds
vSmart(config-cflowd-template)# flow-sampling-interval number
vSmart(config-cflowd-template)# template-refresh seconds
vSmart(config-cflowd-template)# protocol ipv4|ipv6|Both
```



- (注) Cisco IOS XE Catalyst SD-WAN デバイス では、**flow-active-timeout** は 60 秒に固定されています。**flow-inactive-timeout** が 10 秒に固定されている場合、Cisco SD-WAN コントローラ または Cisco SD-WAN Manager で設定されている **flow-active-timeout** および **flow-inactive-timeout** の値は、Cisco IOS XE Catalyst SD-WAN デバイス では有効になりません。

2. フローモニターで TOS、DSCP 出力、および TLOC ループバックを収集するには、次の手順を実行します。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降、ループバック インターフェイスを入力または出力トランスポート インターフェイスとして設定すると、この機能により、FNF レコードの物理インターフェイスの代わりにループバックを収集できるようになりました。この機能は、IPv4 および IPv6 でサポートされています。

```
vSmart(config-cflowd-template)# customized-ipv4-record-fields
vSmart(config-customized-ipv4-record-fields)# collect-tos
vSmart(config-customized-ipv4-record-fields)# collect-dscp-output
vSmart(config-cflowd-template)# collect-tloc-loopback
```

3. フローコレクタを設定します。

```
vSmart(config-cflowd-template)# collector vpn vpn-id address
ip-address port port-number transport transport-type
source-interface interface-name
export-spread
enable
app-tables app-tables
tloc-tables tloc-tables
other-tables other-tables
```



- (注) **app-tables**、**tloc-tables**、**other-tables** オプションは、Cisco SD-WAN コントローラ を使用してのみ設定できます。



- (注) Cisco IOS XE Catalyst SD-WAN デバイスは UDP コレクタのみをサポートします。設定されているトランスポートプロトコルに関係なく、UDP は Cisco IOS XE Catalyst SD-WAN デバイスのデフォルトコレクタです。

4. トラフィック マッチ パラメータを定義し、アクション **cflowd** を含むデータポリシーを設定します。

```
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy)# sequence number
vSmart(config-sequence)# match match-parameters
vSmart(config-sequence)# action cflowd
```

5. トラフィック フロー モニタリング ポリシーを適用する Cisco IOS XE Catalyst SD-WAN デバイスを含むオーバーレイネットワーク内のサイトのリストを作成します。リストに複数のサイトを含めるには、複数の **vpn vpn-id** コマンドを設定します。

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

6. Cisco IOS XE Catalyst SD-WAN デバイス を含むオーバーレイネットワーク内のサイトにデータポリシーを適用します。

```
vSmart(config)# apply-policy site-list list-name
vSmart(config-site-list)# data-policy policy-name
vSmart(config-site-list)# cflowd-template template-name
```

VPN0 インターフェイスでの Flexible NetFlow の設定

CLI テンプレートまたは CLI アドオンテンプレートを使用して、VPN0 インターフェイスで FNF を有効にできます。ezPM プロファイルは、すべての NetFlow VPN0 モニター設定を伝送する新しいプロファイルを作成するのに役立ちます。プロファイルを選択していくつかのパラメータを指定するだけで、残りのプロビジョニング情報は ezPM により自動的に設定されます。プロファイルは、コンテキストに対して有効または無効にできる、事前定義された一連のトラフィックモニターです。Easy Performance Monitor (ezPM) を設定し、次のように FNF を有効にすることができます。

```
Device# config-transaction
Device(config)# performance monitor context <monitor_name> profile <sdwan-fnf>
traffic-monitor <all> [ipv4/ipv6]
Device(config-perf-mon)# exporter destination <destination address> source <source
interface> transport udp vrf <vrf-name> port <port-number> dscp <dscp>
```

次の例は、sdwan-fnf プロファイルを使用してパフォーマンスモニターのコンテキストを設定する方法を示しています。この設定により、トラフィックメトリックのモニタリングが有効になります。ここで、10.1.1.1 はサードパーティ製コレクタの IP アドレス、GigabitEthernet5 は送信元インターフェイス、4739 はサードパーティ製コレクタのリスニングポートです。

```
Device# config-transaction
Device(config)# performance monitor context <monitor_name> profile sdwan-fnf
```

```
traffic-monitor all [ipv4/ipv6]
Device(config-perf-mon)# exporter destination <10.1.1.1> source <GigabitEthernet5>
transport udp vrf <vrf1> port <4739> dscp <1>
```

CLIを使用したBFDメトリックのエクスポートに対するFlexibleNetFlowの設定

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

Cisco IOS XE Catalyst SD-WAN デバイス を制御している Cisco SD-WAN コントローラ の CLI から、データポリシーを使用して BFD メトリックのエクスポートを有効にするか無効にするかに応じて、次のコマンドを入力します。

1. BFD メトリックのエクスポートを有効にします。

```
policy
  cflowd-template template-name
    collector vpn vpn-id address ip-address port port transport transport
    source-interface interface
    bfd-metrics-export
    export-interval export-interval
```

デフォルトの BFD エクスポート間隔は 600 秒です。BFD エクスポート間隔は、Cflowd テンプレートの更新には影響を受けません。BFD エクスポート間隔では、bfd-metrics-export テーブルからデータを送信する間隔のみを制御します。tunnel-tloc テーブルでは、BFD エクスポート間隔は、BFD エクスポート間隔と Cflowd テンプレート更新間の最小値を、データ送信間隔に使用しています。

2. BFD メトリックのエクスポートを無効にします。

```
policy
  cflowd-template template-name
    collector vpn vpn-id address ip-address port port transport transport
    source-interface interface
    no bfd-metrics-export
```

BFD メトリックのエクスポートを有効にする一連の設定例を次に示します。

```
policy
  cflowd-template fnf
    template-refresh 600
    collector vpn 0 address 10.0.100.1 port 4739 transport transport_udp
    bfd-metrics-export
    export-interval 30
  !
!
!
lists
  site-list 500
  site-id 500
!
!
!
apply-policy
```

```

site-list 500
  cflowd-template fnf
!
!

```

Flexible NetFlow による BFD メトリックのエクスポート設定例

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

以下は、BFD メトリックのエクスポートを有効にする場合の一元管理型ポリシーの設定例です。

```

Device# show sdwan policy from-vsmart
from-vsmart cflowd-template fnf
flow-active-timeout 600
flow-inactive-timeout 60
template-refresh 600
flow-sampling-interval 1
protocol ipv4
customized-ipv4-record-fields
no collect-tos
no collect-dscp-output
collector vpn 0 address 10.0.100.1 port 4739 transport transport_udp
bfd-metrics-export
export-interval 600

```

以下は、平均ジッター、平均遅延、および損失メトリックに関する FNF BFD テレメトリデータの例です。

```

{ 'Data_Template': 'Data_Flow',
  'ObservationDomainId': 6,
  'Version': 10,
  'arrive_time': 1658807309.2496994,
  'dfs_tfs_length': 200,
  'export_dfs_tfs_templates_list_dict': { 'FlowSequence': 3354,
                                          'Flowset_id': '258',
                                          'Flowset_length': 200,
                                          'Length': 286,
                                          'ObservationDomainId': 6,
                                          'TimeStamp': 1658807269,
                                          'Version': 10,
                                          'flow': [ { 'bfd_avg_jitter': 1000,
                                                    'bfd_avg_latency': 1000,
                                                    'bfd_loss': 15,
                                                    'bfd_pfr_update_ts': 1658806692155,
                                                    'bfd_rx_cnt': 0,
                                                    'bfd_tx_cnt': 0,
                                                    'ipDiffServCodePoint': 48,
                                                    'tloc_table_overlay_session_id':
10},
                                          ...
                                          ]},
  'flow_length': 4,
  'flow_time': 1658807269,
  'flowset_id': '258',
  'header': { 'FlowSequence': 3354,
              'Length': 286,
              'ObservationDomainId': 6,
              'TimeStamp': 1658807269,

```

```
        'Version': 10},
    'host': '10.0.100.15',
    'ipfix_length': 286,
    'packet_number': 2,
    'template_id': '258'}
```

Cflowd ポリシーの適用と有効化

一元管理型データポリシーを有効にするには、次のようにオーバーレイネットワーク内のサイトのリストに適用します。

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name
```

Cflowd テンプレートをアクティブにするには、データポリシーに関連付けます。

```
vSmart(config)# apply-policy cflowd-template template-name
```

apply-policy コマンドで適用するすべての **data-policy** ポリシーについて、すべてのサイトリストのサイト ID は一意である必要があります。つまり、サイトリストに重複するサイト ID が含まれてはなりません。重複するサイト ID の例には、2つのサイトリスト **site-list 1**、**site-id 1-100**、および **site-list 2 site-id 70-130** のサイト ID があります。ここでは、サイト 70 ~ 100 が両方のリストに含まれています。これらの2つのサイトリストを2つの異なる **data-policy** ポリシーに適用すると、Cisco Catalyst SD-WAN コントローラ で設定をコミットする試行が失敗します。

同じタイプの制限は、次のポリシーのタイプにも適用されます。

- アプリケーション認識型ルーティングポリシー (**app-route-policy**)
- 一元管理型制御ポリシー (**control-policy**)
- 一元管理型データポリシー (**data-policy**)

ただし、異なるタイプのポリシーに適用するサイトリストのサイト ID は重複させることができません。たとえば、**control-policy** ポリシーと **data-policy** ポリシーのサイトリストでは、サイト ID が重複している可能性があります。したがって、上記2つのサイトリストの例 (**site-list 1 site-id 1-100** および **site-list 2 site-id 70-130**) では、1つを制御ポリシーに、もう1つをデータポリシーに適用できます。

commit コマンドを発行して設定を正常にアクティブにすると、Cisco Catalyst SD-WAN コントローラは、指定されたサイトにある Cisco IOS XE Catalyst SD-WAN デバイスにデータポリシーをプッシュします。Cisco Catalyst SD-WAN コントローラ で設定されたポリシーを表示するには、Cisco Catalyst SD-WAN コントローラ で **show running-config** コマンドを使用します。デバイスにプッシュされたポリシーを表示するには、デバイスで **show policy from-vsmart** コマンドを使用します。

Cisco Catalyst SD-WAN コントローラ で設定されている一元管理型データポリシーを表示するには、**show running-config** コマンドを使用します。

```
vSmart# show running-config policy
vSmart# show running-config apply-policy
```

Cisco IOS XE Catalyst SD-WAN デバイスにプッシュされた一元管理型データポリシーを表示するには、デバイスで **show omp data-policy** コマンドを発行します。

```
デバイス# show sdwan policy from-vsmart
```

Cisco IOS XE Catalyst SD-WAN デバイス での Cflowd の可視性の有効化

データポリシーを設定せずに Cisco IOS XE Catalyst SD-WAN デバイス で Cflowd の可視性を直接有効にすることもできます。これにより、LAN 内のすべての VPN からルータに着信するトラフィックのトラフィックフローモニタリングを実行できます。これを行うには、デバイスで Cflowd の可視性を設定します。

```
デバイス (config) # policy flow-visibility
```

アプリケーションをモニタリングするには、デバイスで **show app cflowd flows** および **show app cflowd statistics** コマンドを使用します。

Cflowd トラフィック フロー モニタリングの設定例

このトピックでは、トラフィック フロー モニタリングの設定例を示します。

設定手順

一元管理型データポリシーを使用して Cflowd トラフィックモニタリングを有効にします。これにより、すべての設定が Cisco Catalyst SD-WAN コントローラ で実行されます。すべての TCP トラフィックをモニタリングし、単一のコレクタに送信する手順の例を次に示します。

1. Cflowd テンプレートを作成してコレクタの場所を定義し、Cflowd タイマーを変更します。

```
vsmart (config) # policy cflowd-template test-cflowd-template
vsmart (config-cflowd-template-test-cflowd-template) # collector vpn 1 address
172.16.155.15 port 13322 transport transport_udp
vsmart (config-cflowd-template-test-cflowd-template) # flow-inactive-timeout 60
vsmart (config-cflowd-template-test-cflowd-template) # template-refresh 90
```

2. トラフィックをモニタリングする VPN のリストを作成します。

```
vsmart (config) # policy lists vpn-list vpn_1 vpn 1
```

3. データポリシーを適用するサイトのリストを作成します。

```
vsmart (config) # policy lists site-list cflowd-sites site-id 400,500,600
```

4. データポリシーを設定します。

```
vsmart (config) # policy data-policy test-cflowd-policy
vsmart (config-data-policy-test-cflowd-policy) # vpn-list vpn_1
vsmart (config-vpn-list-vpn_1) # sequence 1
vsmart (config-sequence-1) # match protocol 6
vsmart (config-match) # exit
vsmart (config-sequence-1) # action accept cflowd
vsmart (config-action) # exit
vsmart (config-sequence-1) # exit
vsmart (config-vpn-list-vpn_1) # default-action accept
```

5. オーバーレイネットワーク内のサイトにポリシーと Cflowd テンプレートを適用します。

```
vsmart (config) # apply-policy site-list cflowd-sites data-policy test-cflowd-policy
デバイス (config-site-list-cflowd-sites) # cflowd-template test-cflowd-template
```

6. データポリシーを有効にします。

```
vsmart(config-site-list-cflowd-sites)# validate
Validation complete
vsmart(config-site-list-cflowd-sites)# commit
Commit complete.
vsmart(config-site-list-cflowd-sites)# exit configuration-mode
```

設定例

Cflowd 設定の完全な例を次に示します。

```
vsmart(config)# show configuration
apply-policy
  site-list cflowd-sites
  data-policy test-cflowd-policy
  cflowd-template test-cflowd-template
!
!
policy
data-policy test-cflowd-policy
  vpn-list vpn_1
  sequence 1
  match
    protocol 6
  !
  action accept
  cflowd
  !
  !
  default-action accept
  !
!
cflowd-template test-cflowd-template
flow-inactive-timeout 60
template-refresh 90
collector vpn 1 address 192.168.0.1 protocol ipv4 port 13322 transport transport_udp
!
lists
  vpn-list vpn_1
  vpn 1
  !
  site-list cflowd-sites
  site-id 400,500,600
  !
!
!
```

show sdwan run policy コマンドの次の出力例は、SAIE フローを使用した Cflowd の IPv4 および IPv6 アプリケーションの可視性とフローの可視性の設定を示しています。

```
Device# show sdwan run policy
policy
  app-visibility
  app-visibility-ipv6
  flow-visibility
  flow-visibility-ipv6
```

Cflowd 設定の検証

Cisco Catalyst SD-WAN コントローラ で Cflowd の設定をアクティブ化した後に検証するには、**show running-config policy** コマンドと **show running-config apply-policy** コマンドを使用します。

次に、**show sdwan policy from-vsmart cflowd-template** コマンドの出力例を示します。

```

デバイス# show sdwan policy from-vsmart cflowd-template
from-vsmart cflowd-template test-cflowd-template
  flow-active-timeout 30
  flow-inactive-timeout 60
  template-refresh 90
  flow-sampling-interval 1
  protocol ipv4/ipv6/both
  customized-ipv4-record-fields
    collect-tos
    collect-dscp-output

collector vpn 1 address 192.0.2.1 protocol ipv4 port 13322 transport transport_udp

```

次に、**show sdwan policy from-vsmart** コマンドの出力例を示します。

```

デバイス# show sdwan policy from-vsmart
from-vsmart data-policy test-cflowd-policy
  vpn-list vpn_1
  sequence 1
  match
    protocol 6
    action accept
    cflowd
  default-action accept
from-vsmart cflowd-template test-cflowd-template
  flow-active-timeout 30
  flow-inactive-timeout 60
  protocol ipv4/ipv6/both
  template-refresh 90
  customized-ipv4-record-fields
    collect-tos
    collect-dscp-output
  collector vpn 1 address 192.0.2.1 port 13322 transport transport_udp
from-vsmart lists vpn-list vpn_1
  vpn 1

```

Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降、**cflowd** コマンドは、IPv4 と IPv6 の両方のフローレコードに対して拡張されています。

次に、**show flow record** コマンドの出力例を示します。フローの方向を指定する新しいフィールド [collect connection initiator] の追加によって拡張されています。

```
Device# show flow record sdwan_flow_record-xxx
```

IPv4 フローレコード :

```

flow record sdwan_flow_record-1666223692122679:
  Description:      flow and application visibility records
  No. of users:    1
  Total field space: 102 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port

```



```

match routing vrf service
collect ipv4 dscp
collect transport tcp flags
collect interface input
collect interface output
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
collect application name
collect flow end-reason
collect connection initiator
collect overlay session id input
collect overlay session id output
collect connection id long
collect drop cause id
collect counter bytes sdwan dropped long
collect sdwan sla-not-met
collect sdwan preferred-color-not-met
collect sdwan qos-queue-id
collect counter packets sdwan dropped long

```

IPv6 フロー形式 :

```

flow record sdwan_flow_record_ipv6-1667963213662363:
  Description:          flow and application visibility records
  No. of users:         1
  Total field space:    125 bytes
  Fields:
    match ipv6 protocol
    match ipv6 source address
    match ipv6 destination address
    match transport source-port
    match transport destination-port
    match routing vrf service
    collect ipv6 dscp
    collect transport tcp flags
    collect interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
    collect application name
    collect flow end-reason
    collect connection initiator
    collect overlay session id input
    collect overlay session id output
    collect connection id long
    collect drop cause id
    collect counter bytes sdwan dropped long
    collect sdwan sla-not-met
    collect sdwan preferred-color-not-met
    collect sdwan qos-queue-id
    collect counter packets sdwan dropped long

```

次に、**show flow monitor *monitor-name* cache** コマンドの拡張出力例を示します。フロー方向を示す新しい [connection initiator] フィールドが出力に追加されました。[connection initiator] フィールドには、initiator (クライアントからサーバーへのトラフィックフローの場合)、reverse (サーバーからクライアントの場合)、unknown (トラフィックフローの方向が不明の場合) のいずれかの値を指定できます。

```

Device# show flow monitor sdwan_flow_monitor cache
Cache type: Normal (Platform cache)
Cache size: 128000
Current entries: 4
High Watermark: 5
Flows added: 6
Flows aged: 2
- Inactive timeout ( 10 secs) 2
IPV4 SOURCE ADDRESS: 10.20.24.110
IPV4 DESTINATION ADDRESS: 10.20.25.110
TRNS SOURCE PORT: 40254
TRNS DESTINATION PORT: 443
IP VPN ID: 1
IP PROTOCOL: 6
tcp flags: 0x02
interface input: Gi5
interface output: Gi1
counter bytes long: 3966871
counter packets long: 52886
timestamp abs first: 02:07:45.739
timestamp abs last: 02:08:01.840
flow end reason: Not determined
connection initiator: Initiator
interface overlay session id input: 0
interface overlay session id output: 4
connection connection id long: 0xD8F051F000203A22

```

フローを確認します。

Cflowd データポリシーの影響を受ける Cisco IOS XE Catalyst SD-WAN デバイスでは、さまざまなコマンドで Cflowd フローのステータスを確認できます。

```

デバイス# show sdwan app-fwd cflowd statistics

```

```

data_packets           :      0
template_packets      :      0
total-packets         :      0
flow-refresh          :     123
flow-ageout           :     117
flow-end-detected     :      0
flow-end-forced       :      0

```

IPv6 トラフィックの FNF IPv6 設定例

IPv6 トラフィック用の Cflowd を使用した一元管理型ポリシーの設定例を次に示します。

```

policy
data-policy vpn_1_accept_cflowd_vpn_1
vpn-list vpn_1
sequence 102
match
source-ipv6          2001:DB8:0:/32
destination-ipv6    2001:DB8:1:/32
!
action accept
count cflowd_ipv6_1187157291
cflowd
!
!
default-action accept
!

```

```
!  
cflowd-template cflowd_server  
  flow-active-timeout 60  
  flow-inactive-timeout 30  
  protocol ipv6  
!  
lists  
  vpn-list vpn_1  
    vpn 1  
  site-list vedgel  
    site-id 500  
!  
  
apply-policy  
  site-list vedgel  
  data-policy _vpn_1_accept_cflowd_vpn_1_all  
  cflowd-template cflowd_server
```

FNF 展開エクスポートの設定例

展開エクスポートの設定例を次に示します。

```
Device# show sdwan policy from-vsmart  
from-vsmart cflowd-template cflowd  
  flow-active-timeout 600  
  flow-inactive-timeout 60  
  template-refresh 60  
  flow-sampling-interval 1  
  protocol ipv4  
  customized-ipv4-record-fields  
    no collect-tos  
    no collect-dscp-output  
  collector vpn 0 address 10.0.100.1 port 4739 transport transport_udp  
  export-spread  
    app-tables 20  
    tloc-tables 10  
    other-tables 5
```

CLI コマンドを使用した集約データの最大 FNF レコードレートの設定

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.14.1

はじめる前に

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および[CLI テンプレート](#)を参照してください。デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

最大 FNF レコードレートの設定

デバイスが集約トラフィックデータを Cisco SD-WAN Manager に送信する際の最大レート（1 分あたりの FNF レコード数）を設定します。

```
policy app-agg-node max-records-per-minute
```

例

次に、集約トラフィックデータを 1 分あたり最大 1000 個の FNF レコードで送信するようにデバイスを設定します。

```
policy app-agg-node 1000
```

例

次に、集約トラフィックデータを 1 分あたり最大 10000 個の FNF レコードで送信するデフォルト値にデバイスを復元します。

```
no policy app-agg-node
```

トラフィック フロー モニタリングの確認

ここでは、トラフィック フロー モニタリングの確認について説明します。

収集ループバックの確認

次のコマンドを使用して、入力および出力インターフェイスの出力を確認できます。

show sdwan app-fwd cflowd flows

次に、**show sdwan app-fwd cflowd flows** で **flows** キーワードを指定した場合の出力例を示します。

```
Device#show sdwan app-fwd cflowd flows
app-fwd cflowd flows vpn 1 src-ip 10.10.15.12 dest-ip 10.20.15.12 src-port 0 dest-port
0 dscp 0 ip-proto 1
tcp-cntrl-bits          24
icmp-opcode            0
total-pkts             5
total-bytes            500
start-time             "Tue Jun 27 09:21:09 2023"
egress-intf-name       Loopback1
ingress-intf-name      GigabitEthernet5
application            ping
family                 network-service
drop-cause              "No Drop"
drop-octets            0
drop-packets           0
sla-not-met            0
color-not-met          0
queue-id               2
initiator              2
tos                    0
dscp-output            0
sampler-id             0
fec-d-pkts             0
fec-r-pkts             0
pkt-dup-d-pkts-orig    0
pkt-dup-d-pkts-dup     0
pkt-dup-r-pkts        0
pkt-cxp-d-pkts        0
category               0
service-area           0
```

```

cxp-path-type          0
region-id              0
ssl-read-bytes         0
ssl-written-bytes      0
ssl-en-read-bytes      0
ssl-en-written-bytes   0
ssl-de-read-bytes      0
ssl-de-written-bytes   0
ssl-service-type       0
ssl-traffic-type       0
ssl-policy-action      0
appqoe-action          0
appqoe-sn-ip           0.0.0.0
appqoe-pass-reason     0
appqoe-dre-input-bytes 0
appqoe-dre-input-packets 0
appqoe-flags           0
    
```

次のコマンドを使用して、入力および出力インターフェイスの出力を確認できます。

show sdwan app-fwd cflowd table

次に、**show sdwan app-fwd cflowd table** で **table** キーワードを指定した場合の出力例を示します。

```

show sdwan app-fwd cflowd flows table
PKT  PKT  PKT  PKT
      SSL
      APPQOE  APPQOE
      TCP
      SLA  COLOR
      FEC  FEC  DUP D  DUP D  DUP  CXP
      EN  EN  DE  DE  DE  SSL  SSL  SSL  SSL
      APPQOE  DRE  DRE
      ICMP  TOTAL  TOTAL
      DSCP  SAMPLER D  R  PKTS  PKTS  DROP  DROP  NOT  NOT  QUEUE
      PATH  REGION  READ  WRITTEN  READ  WRITTEN  READ  WRITTEN  SERVICE  TRAFFIC  POLICY
      APPQOE  APPQOE  PASS  INPUT  INPUT  APPQOE
      VPN  SRC  IP  DEST  IP  PORT  PORT  DSCP  PROTO  BITS
      OPCODE  PKTS  BYTES  START  TIME  NAME
      APPLICATION  FAMILY  DROP  CAUSE  OCTETS  PACKETS  MET  MET  ID  INITIATOR
      TOS  OUTPUT  ID  PKTS  PKTS  ORIG  DUP  PKTS  PKTS  CATEGORY  AREA  TYPE
      ID  BYTES  BYTES  BYTES  BYTES  BYTES  BYTES  BYTES  TYPE  TYPE  ACTION  ACTION
      SN  IP  REASON  BYTES  PACKETS  FLAGS
-----
1  10.10.15.11  10.20.20.10  0  0  0  1  24
0  5  500  Tue Jun 27 09:21:06 2023  Loopback1  GigabitEthernet5
ping  network-service  No Drop  0  0  0  0  2  2
0  0  0  0  0  0  0  0  0  0  0  0
0  0.0.0.0  0  0  0  0  0
0  10.0.5.5  10.0.15.10  58048  22  4  6  24
0  41  1752  Tue Jun 27 09:21:06 2023  internal0/0/rp:0  GigabitEthernet9
unknown  network-service  No Drop  0  0  0  0  2  0
0  0  0  0  0  0  0  0  0  0  0  0
0  0.0.0.0  0  0  0  0  0
1  10.10.15.11  10.20.20.10  0  2048  0  1  24
2048  5  500  Tue Jun 27 09:21:06 2023  GigabitEthernet5  Loopback1
ping  network-service  No Drop  0  0  0  0  2  2
0  0  0  0  0  0  0  0  0  0  0  0
    
```

```

0 0 0 0 0 0 0 0 0 0 0 0 0
0.0.0.0 0 0 0 0
1 10.10.15.11 10.5.10.15 0 2048 0 1 31
2048 20 960 Tue Jun 27 09:21:06 2023 Null GigabitEthernet5
ping network-service Ipv4NoRoute 960 20 0 0 2 2
0 0 0 0 0 0 0 0 0 0 0 0 0
0.0.0.0 0 0 0 0
1 10.10.15.11 10.20.20.10 50920 4739 0 17 31
0 473 524768 Tue Jun 27 09:21:06 2023 GigabitEthernet5 internal0/0/rp:0
ipfix network-management No Drop 0 0 0 0 2 1
0 0 0 0 0 0 0 0 0 0 0 0 0
0.0.0.0 0 0 0 0
0 10.0.5.10 10.0.5.10 22 58048 48 6 24
0 39 3020 Tue Jun 27 09:21:05 2023 GigabitEthernet9 internal0/0/rp:0
ssh terminal No Drop 0 0 0 0 2 2
0 0 0 0 0 0 0 0 0 0 0 0 0
0.0.0.0 0 0 0 0
1 10.10.15.11 10.20.20.10 0 771 48 1 31
771 8 4192 Tue Jun 27 09:21:05 2023 internal0/0/rp:0 GigabitEthernet5
icmp network-service No Drop 0 0 0 0 2 2
0 0 0 0 0 0 0 0 0 0 0 0 0
0.0.0.0 0 0 0 0
1 fe40::6044:ff:feb7:c2db ff01::1:ff00:10 0 34560 0 58 0
34560 6 432 Tue Jun 27 09:20:41 2023 internal0/0/rp:0 GigabitEthernet5
ipv6-icmp network-service No Drop 0 0 0 0 0 2
0 0 0 0 0 0 0 0 0 0 0 0 0
0.0.0.0 0 0 0 0
1 10:20:20::10 fe40::6024:ff:feb6:c1db 0 34816 56 58 0
34816 4 288 Tue Jun 27 09:20:41 2023 GigabitEthernet5 internal0/0/rp:0
ipv6-icmp network-service No Drop 0 0 0 0 2 2
0 0 0 0 0 0 0 0 0 0 0 0 0
0.0.0.0 0 0 0 0

```

デバイスのインターフェイスバインドの確認

次のコマンドを使用してデバイスのインターフェイスバインドを確認することができます。

show sdwan control local-properties wan-interface-list

次に、**wan-interface-list** キーワードを使用した **show sdwan control local-properties wan-interface-list** の出力例を示します。

コマンドは次を表示します。

- バインドモードでループバック WAN インターフェイスにバインドされた物理インターフェイス。
- バインド解除モードでのループバック WAN インターフェイスのバインド解除。
- その他の場合は該当なし。

```

Device#show sdwan control local-properties wan-interface-list
NAT TYPE: E -- indicates End-point independent mapping
          A -- indicates Address-port dependent mapping
          N -- indicates Not learned

```

Note: Requires minimum two vbonds to learn the NAT type

MAX	RESTRICT/ INTERFACE	PRIVATE	PUBLIC	PUBLIC	PRIVATE	PRIVATE	STUN
CNTRL	CONTROL/ CONTROL	PORT	LAST IPv4	SPI TIME PORT	NAT IPv4	VM STATE	BIND IPv6
		LR/LB	VS/VM CONNECTION	REMAINING	TYPE	CON REG	INTERFACE
			PRF	IDs			
GigabitEthernet1			10.0.10.10	12346	10.0.10.10	2	::
		12346	2/1 lte		up		no/yes/no No/No
0:20:20:27	0:01:14:20	N	5 Default	N/A			
GigabitEthernet4			10.0.10.10	12346	10.0.10.10	2	::
		12346	2/0 blue		up		no/yes/no No/No
0:20:20:27	0:01:14:20	N	5 Default	N/A			
Loopback1			1.1.1.1	12366	1.1.1.1	2	::
		12366	2/0 custom1		up		no/yes/no No/No
0:20:20:27	0:01:14:20	N	5 Default	GigabitEthernet1			
Loopback2			2.2.2.2	12406	2.2.2.2	2	::
		12406	2/0 custom2		up		no/yes/no No/No
0:20:20:27	0:01:14:20	N	5 Default	Unbind			

VPN0 インターフェイスでの Flexible NetFlow 設定の確認

Flexible NetFlow レコード設定の概要の表示

次のコマンドを使用して、FNF レコードの設定を確認できます。

```
Device# show flow record <monitor-context-name>
```



(注) 次の例では、temp0 というモニター名が使われます。

次の出力例は、ezPM プロファイルを使用した IPv4 トラフィックフローレコードに関する情報を示しています。

```
Device# show flow record temp0-sdwan-fnf-vpn0-monitor_ipv4
flow record temp0-sdwan-fnf-vpn0-monitor_ipv4:
  Description:      ezPM record
  No. of users:    1
  Total field space: 66 bytes
  Fields:
    match ipv4 dscp
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match flow direction
    collect routing next-hop address ipv4
    collect transport tcp flags
    collect interface input
    collect interface output
    collect flow sampler
    collect counter bytes long
    collect counter packets long
```

```

collect timestamp absolute first
collect timestamp absolute last
collect application name
collect flow end-reason

```

次の出力例は、ezPM プロファイルを使用した IPv6 トラフィックフローレコードに関する情報を示しています。

```
Device# show flow record temp0-sdwan-fnf-vpn0-monitor_ipv6
```

```

flow record temp0-sdwan-fnf-vpn0-monitor_ipv6:
Description:          ezPM record
No. of users:         1
Total field space:    102 bytes
Fields:
  match ipv6 dscp
  match ipv6 protocol
  match ipv6 source address
  match ipv6 destination address
  match transport source-port
  match transport destination-port
  match flow direction
  collect routing next-hop address ipv6
  collect transport tcp flags
  collect interface input
  collect interface output
  collect flow sampler
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last
  collect application name
  collect flow end-reason

```

次の出力例は、ezPM プロファイルを使用した IPv4 トラフィックの NetFlow 設定に関するモニター情報を示しています。

```
Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv4
```

```

Flow Monitor temp0-sdwan-fnf-vpn0-monitor_ipv4:
Description:          ezPM monitor
Flow Record:          temp0-sdwan-fnf-vpn0-monitor_ipv4
Cache:
  Type:                normal (Platform cache)
  Status:              allocated
  Size:                5000 entries
  Inactive Timeout:    10 secs
  Active Timeout:      60 secs

  Trans end aging:    off

```

次の出力例は、ezPM プロファイルを使用した IPv6 トラフィックの NetFlow 設定に関するモニター情報を示しています。

```
Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv6
```

```

Flow Monitor temp0-sdwan-fnf-vpn0-monitor_ipv6:
Description:          ezPM monitor

```



```

Flow Record:      temp0-sdwan-fnf-vpn0-monitor_ipv6
Cache:
  Type:           normal (Platform cache)
  Status:         allocated
  Size:           5000 entries
  Inactive Timeout: 10 secs
  Active Timeout: 60 secs

  Trans end aging: off

```

フローレコードキャッシュの表示

次の出力例は、指定したモニター（この場合は temp0-sdwan-fnf-vpn0-monitor_ipv4）のフローレコードキャッシュを示しています。

```

Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv4 cache
Cache type:           Normal (Platform cache)
Cache size:           5000
Current entries:      14
High Watermark:       14

Flows added:          170
Flows aged:           156
  - Active timeout    ( 60 secs) 156

IPV4 SOURCE ADDRESS: 10.0.0.0
IPV4 DESTINATION ADDRESS: 10.255.255.254
TRNS SOURCE PORT:    0
TRNS DESTINATION PORT: 0
FLOW DIRECTION:      Input
IP DSCP:              0x00
IP PROTOCOL:          1
ipv4 next hop address: 10.0.0.1
tcp flags:            0x00
interface input:      Gi1
interface output:     Gi2
flow sampler id:      0
counter bytes long:   840
counter packets long: 10
timestamp abs first:  02:55:24.359
timestamp abs last:   02:55:33.446
flow end reason:      Not determined
application name:     layer7 ping
.....

```

次の出力例は、指定した IPv6 モニター（temp0-sdwan-fnf-vpn0-monitor_ipv6）のフローレコードキャッシュを示しています。

```

Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv6 cache
Cache type:           Normal (Platform cache)
Cache size:           5000
Current entries:      6
High Watermark:       6

Flows added:          10
Flows aged:           4
  - Inactive timeout  ( 10 secs) 4

IPV6 SOURCE ADDRESS: 2001:DB8::/32
IPV6 DESTINATION ADDRESS: 2001:DB8::1
TRNS SOURCE PORT:    0
TRNS DESTINATION PORT: 32768
FLOW DIRECTION:      Output

```

```

IP DSCP:                0x00
IP PROTOCOL:            58
ipv6 next hop address:  2001:DB8:1::1
tcp flags:              0x00
interface input:       Gi2
interface output:      Gi1
flow sampler id:       0
counter bytes long:    2912
counter packets long:  28
timestamp abs first:   02:57:06.025
timestamp abs last:    02:57:33.378
flow end reason:       Not determined
application name:      prot ipv6-icmp

```

次の出力例は、フローエクスポートの詳細を示しています。

```

Device# show flow exporter temp0
Flow Exporter temp0:
  Description:          performance monitor context temp0 exporter
  Export protocol:      IPFIX (Version 10)
  Transport Configuration:
    Destination type:   IP
    Destination IP address: 10.0.0.1
    VRF label:         1
    Source IP address:  10.0.0.0
    Source Interface:   GigabitEthernet5
    Transport Protocol: UDP
    Destination Port:  4739
    Source Port:       51242
    DSCP:              0x1
    TTL:               255
    Output Features:   Used
  Export template data timeout:      300
  Options Configuration:
    interface-table (timeout 300 seconds) (active)
    vrf-table (timeout 300 seconds) (active)
    sampler-table (timeout 300 seconds) (active)
    application-table (timeout 300 seconds) (active)
    application-attributes (timeout 300 seconds) (active)

```

BFD メトリックのエクスポートに対する Flexible NetFlow 設定の確認

最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

以下は、**show flow exporter** コマンドの出力例で、各フローエクスポートの設定を示したものです。

```

Device# show flow exporter
...
Flow Exporter sdwan_flow_exporter_1:
  Description:          export flow records to collector
  Export protocol:      IPFIX (Version 10)
  Transport Configuration:
    Destination type:   IP
    Destination IP address: 10.0.100.1
    Source IP address:   10.0.100.15
    Transport Protocol:  UDP
    Destination Port:   4739
    Source Port:        54177

```

```
DSCP:                0x0
TTL:                 255
MTU:                 1280
Output Features:     Used
Options Configuration:
  interface-table (timeout 600 seconds) (active)
  tunnel-tloc-table (timeout 600 seconds) (active)
  bfd-metrics-table (timeout 600 seconds) (active)
```

以下は、**show flow exporter statistics** コマンドの出力例で、各フローエクスポートのクライアント送信統計情報を示したものです。

```
Device# show flow exporter statistics
...
Flow Exporter sdwan_flow_exporter_1:
Packet send statistics (last cleared 3d05h ago):
  Successfully sent:      1433                (907666 bytes)

Client send statistics:
  Client: Option options interface-table
    Records added:        6552
    - sent:                6552
    Bytes added:          694512
    - sent:                694512

  Client: Option options tunnel-tloc-table
    Records added:        1916
    - sent:                1916
    Bytes added:          99632
    - sent:                99632

  Client: Flow Monitor sdwan_flow_monitor
    Records added:        0
    Bytes added:          0

  Client: Option options bfd-metrics-table
    Records added:        4
    - sent:                4
    Bytes added:          196
    - sent:                196
```

以下は、**show flow exporter templates** コマンドの出力例で、各テンプレートの詳細を示したものです。

```
Device# show flow exporter templates
...
Client: Option options tunnel-tloc-table
  Exporter Format: IPFIX (Version 10)
  Template ID    : 257
  Source ID      : 6
  Record Size    : 52
  Template layout
```

Field	ID	Ent.ID	Offset	Size
TLOC TABLE OVERLAY SESSION ID	12435	9	0	4
tloc local color	12437	9	4	16
tloc remote color	12439	9	20	16
tloc tunnel protocol	12440	9	36	8
tloc local system ip address	12436	9	44	4
tloc remote system ip address	12438	9	48	4

```
Client: Option options bfd-metrics-table
```

```
Exporter Format: IPFIX (Version 10)
Template ID      : 262
Source ID       : 6
Record Size     : 49
Template layout
```

Field	ID	Ent.ID	Offset	Size
TLOC TABLE OVERLAY SESSION ID	12435	9	0	4
IP DSCP	195		4	1
bfd loss	12527	9	5	4
bfd pfr update ts	12530	9	9	8
bfd avg latency	12528	9	17	8
bfd avg jitter	12529	9	25	8
bfd rx cnt	12531	9	33	8
bfd tx cnt	12532	9	41	8



第 13 章

アプリケーションパフォーマンスモニター



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 37: 機能の履歴

機能名	リリース情報	説明
アプリケーションパフォーマンスモニター	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能は、事前定義されたモニタリングプロファイルを使用してインテントベースのパフォーマンスモニターを設定するための明示的な方法を提供します。 Cisco SD-WAN Manager の CLI アドオン機能テンプレートを使用して、この機能を設定します。

- [アプリケーションパフォーマンスモニターの概要 \(272 ページ\)](#)
- [制限事項と制約事項 \(274 ページ\)](#)
- [アプリケーションパフォーマンスモニターの設定 \(274 ページ\)](#)
- [パフォーマンスモニタリング設定の確認 \(275 ページ\)](#)

アプリケーションパフォーマンス モニターの概要

アプリケーションパフォーマンス モニター機能は、インテントベースのパフォーマンスモニターを設定できる、簡素化されたフレームワークです。この機能を使用すると、クライアントセグメント、ネットワークセグメント、サーバーセグメントでフィルタリングされたエンドツーエンドのアプリケーションパフォーマンスをリアルタイムで表示できます。この情報は、アプリケーションのパフォーマンスを最適化するのに役立ちます。

アプリケーションパフォーマンス モニターは、特定のトラフィックの評価指標を収集するのに使用される、事前定義された設定です。

アプリケーションパフォーマンス モニタリングの主なコンセプト

モニタリングプロファイル：プロファイルは、コンテキストに対して有効または無効にすることができる、事前定義された一連のトラフィックモニターです。この機能の一部として `sdwan-performance` プロファイルが強化され、Cisco Catalyst SD-WAN トンネルインターフェイスを通過するトラフィックをモニタリングするためのアプリケーション応答時間（ART）とメディアモニターが含まれるようになりました。`sdwan-performance` プロファイルには、インテントに基づいてトラフィックをフィルタリングする専用ポリシーがあります。

`sdwan-performance` プロファイルを選択すると、関連する設定が自動的に生成および適用されます。

コンテキスト：インターフェイスの入力トラフィックと出力トラフィックの両方にアタッチされるパフォーマンス モニター ポリシー マップに相当します。コンテキストには、有効にする必要があるトラフィックモニターに関する情報が含まれます。インターフェイスにコンテキストがアタッチされると、入力トラフィックと出力トラフィックにそれぞれ1つずつ、合計2つのポリシーマップが作成されます。トラフィックモニターで指定されている方向に基づいてポリシーマップがアタッチされると、トラフィックのモニターが開始されます。



- (注) コンテキストは複数のインターフェイスにアタッチできます。1つのインターフェイスにアタッチできるコンテキストは1つだけです。コンテキストは、インターフェイスにアタッチしていない場合にのみ変更できます。

トラフィックモニタリング仕様：分類とサンプラーを使用して、評価指標をフィルタリングすることを選択できます。

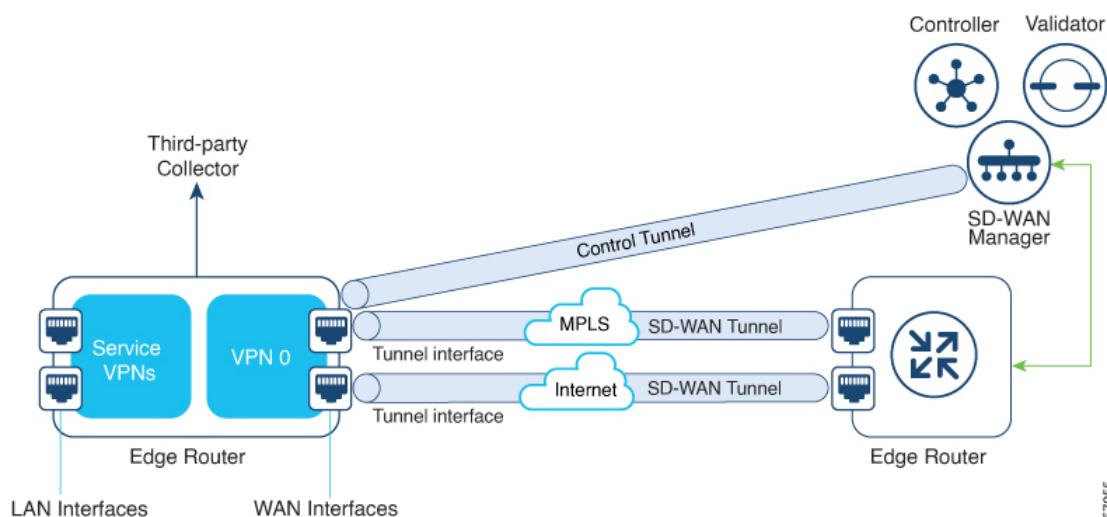
- **分類**：指定されたアプリケーションについてモニターする必要があるトラフィックを定義するフィルタです。このフィルタがモニターする必要があるのは特定のアプリケーションのパフォーマンスのみであるため、デバイスおよびパフォーマンスコレクタの負荷を軽減します。
- **サンプラー**：すべてのフローではなく、指定されたサンプリングレートに基づいて、ランダムなトラフィックフローをモニターします。有効にすると、トラフィックの規模が大きい場合のスケールリングやパフォーマンスへの影響が軽減されます。

機能と利点

- TCPフローのARTをモニターできます。モニターできるパラメータには、サーバーのネットワーク遅延、クライアントのネットワーク遅延、アプリケーション遅延があります。
- Real-time Transport Protocol (RTP) のオーディオおよびビデオトラフィックのジッターをモニターできます。
- パフォーマンスモニターと一致するすべてのフローについて、入力インターフェイスと出力インターフェイス、ローカル TLOC とリモート TLOC に関する情報を収集できます。
- パフォーマンスモニターは、CLI コマンドを使用して、すべての WAN トンネルインターフェイスまたは特定の WAN トンネルインターフェイスで設定できます。
- グローバルパフォーマンス サンプラーがサポートされています。サンプラーを使用すると、トラフィック全体ではなく、設定されたサンプリングレートに基づいてランダムフローをモニターできるため、パフォーマンスとスケーリングのオーバーヘッドが削減されます。

アプリケーションパフォーマンス モニターの仕組み

図 15: パフォーマンスモニタリングのワークフロー



この図では、パフォーマンスモニターがグローバルに（すべてのトンネルインターフェイスに）適用されています。特定のインターフェイスで有効にするオプションもあります。モニタリング対象は、WAN トンネルインターフェイスで送受信されるトラフィックのパフォーマンスです。収集されたメトリックは、モニタリングプロファイルで開始されたコンテキストで定義されたエクスポートパラメータに基づいて、定義されたサードパーティコレクタに送信されます。その後、さまざまな show コマンドを使用することで、モニタリングしているアプリケーションまたはメディアの詳細を表示できます。

制限事項と制約事項

- パフォーマンスのモニタリングは、IPv4 トラフィックでのみサポートされます。IPv6 トラフィックはサポートされていません。
 - パフォーマンスモニターがデバイスに適用されると、その設定を変更してデバイスに再適用することはできません。パフォーマンスモニターの設定を変更するには、次の手順を実行します。
 - CLI アドオン機能テンプレートまたはデバイス CLI テンプレートを編集して、テンプレートから **performance monitor apply** コマンドを削除します。デバイス CLI テンプレートまたは CLI アドオン機能テンプレートがアタッチしているデバイステンプレートを更新します。
 - CLI アドオン機能テンプレートで **performance monitor context** を編集し、**performance monitor apply** コマンドを使用してパフォーマンスモニターを再度適用します。CLI アドオン機能テンプレートがアタッチしているデバイステンプレートを更新します。
- または、同じモニタリングプロファイルに基づいて新しいコンテキストを設定し、以前のコンテキスト設定を削除します。
- コネクタのインシエータ値を適切に設定できるようにするには、ポリシー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。

アプリケーションパフォーマンス モニターの設定

アプリケーションパフォーマンスモニターは、グローバル（すべての WAN トンネルインターフェイス）で有効にすることも、特定の WAN トンネルインターフェイスで有効にすることもできます。ART、メディアモニター、またはその両方のパフォーマンスモニタリングを有効にすることもできます。

Cisco SD-WAN Manager を使用してアプリケーションパフォーマンス モニタリングを設定するには、[CLI アドオン機能テンプレートを作成し、デバイステンプレートに添付します。](#)

パフォーマンスモニターのグローバルな有効化

次の例は、`sdwan-performance` プロファイルを使用してパフォーマンスモニターのコンテキストを設定する方法を示しています。この設定により、ART およびメディアのトラフィックメトリックのモニタリングが有効になり、すべての SD-WAN トンネルインターフェイスに設定が適用されます。ここで、`10.0.1.128` はサードパーティ製コネクタの IP アドレス、`GigabitEthernet9` は送信元インターフェイス、`2055` はサードパーティ製コネクタのリスニングポートです。

```
performance monitor context CISCO-APP-MONITOR profile sdwan-performance
  exporter destination 10.0.1.128 source GigabitEthernet9 port 2055
  traffic-monitor application-response-time
  traffic-monitor media
```



```
!  
performance monitor apply CISCO-APP-MONITOR sdwan-tunnel
```

特定のインターフェイスでのパフォーマンスモニターの有効化

次の例は、`sdwan-performance` プロファイルを使用してパフォーマンスモニターのコンテキストを設定する方法を示しています。この設定により、ART およびメディアのトラフィックメトリックのモニタリングが有効になり、特定のトンネルインターフェイス（この場合は `Tunnel1`）に適用されます。ここで、`10.0.1.128` はサードパーティ製コレクタの IP アドレス、`GigabitEthernet9` は送信元インターフェイス、`2055` はサードパーティ製コレクタのリスニングポートです。

```
performance monitor context CISCO-APP-MONITOR profile sdwan-performance  
  exporter destination 10.0.1.128 source GigabitEthernet9 port 2055  
  traffic-monitor application-response-time  
  traffic-monitor media  
!  
interface Tunnel1  
  performance monitor context CISCO-APP-MONITOR
```

追加のモニタリングフィルタとサンプリングレートの指定

特定のタイプのトラフィックをモニタできるようにする例を次に示します。この場合、`rtp-audio` の一致プロトコルは `match-audio` という名前のクラスマップで定義されます。このクラスは `traffic-monitor media class-and mmatch-audio` で参照されるため、`rtp-audio` トラフィックが具体的にモニタリングされます。別の方法として、`class-and` キーワードを使用することもできます。このような場合、カスタマイズされたクラスマップは、`sdwan-performance` プロファイルを有効にすると自動的に作成されるデフォルトのクラスマップを置き換えます。

この例では、パフォーマンスモニターはグローバルに適用されます。つまり、すべての Cisco Catalyst SD-WAN トンネルインターフェイスに適用されます。サンプリングレート `10` は、`10` 個のフローのうち `1` 個がモニタリングされることを示します。サンプリングレート `100` は、`100` 個のフローのうち `1` 個がモニターされることを示します。

```
class-map match-any match-audio  
  match protocol rtp-audio  
!  
performance monitor context CISCO-APP-MONITOR profile sdwan-performance keyword  
  exporter destination 10.75.212.84 source GigabitEthernet0/0/0 port 2055  
  traffic-monitor application-response-time  
  traffic-monitor media class-and (or class-replace) match-audio  
!  
performance monitor apply CISCO-APP-MONITOR sdwan-tunnel  
performance monitor sampling-rate 10
```

パフォーマンスモニタリング設定の確認

パフォーマンスモニタリング設定に関する概要の表示

以下は、有効になっているトラフィックモニタリングと、それらが適用されているインターフェイスに関する情報を示したサンプル出力です。

```
Device# show performance monitor context CISCO-MONITOR summary
```

```
=====
|                               CISCO-MONITOR                               |
=====
```

```
Description: User defined
```

```
Based on profile: sdwan-performance
```

```
Coarse-grain NBAR based profile
```

```
Configured traffic monitors
```

```
=====
application-response-time:
media: class-and match_audio
```

```
Attached to Interfaces
```

```
=====
```

```
Tunnel1
```

以下は、指定されたコンテキストにアタッチされたサードパーティエクスポートの動作情報を示したサンプル出力です。

```
Device# show performance monitor context CISCO-MONITOR exporter
```

```
=====
|                               Exporters information of context CISCO-MONITOR                               |
=====
```

```
Flow Exporter 175_SDWAN-1:
```

```
Description:                performance monitor context CISCO-MONITOR exporter
```

```
Export protocol:            IPFIX (Version 10)
```

```
Transport Configuration:
```

```
Destination type:          IP
```

```
Destination IP address:    10.75.212.84
```

```
Source IP address:         10.74.28.19
```

```
Source Interface:          GigabitEthernet0/0/0
```

```
Transport Protocol:    UDP
Destination Port:     2055
Source Port:          63494
DSCP:                 0x0
TTL:                  255
Output Features:      Used
```

Options Configuration:

```
interface-table (timeout 600 seconds) (active)
sampler-table (timeout 600 seconds) (active)
application-table (timeout 600 seconds) (active)
sub-application-table (timeout 600 seconds) (active)
application-attributes (timeout 600 seconds) (active)
tunnel-tloc-table (timeout 600 seconds) (active)
```

Flow Exporter 175_SDWAN-1:

Packet send statistics (last cleared 04:13:19 ago):

```
Successfully sent:      10270                (13709142 bytes)
```

Client send statistics:

Client: Option options interface-table

```
Records added:         312
- sent:                 312
Bytes added:           31824
- sent:                 31824
```

Client: Option options sampler-table

```
Records added:         28
- sent:                 28
Bytes added:           1344
- sent:                 1344
```

Client: Option options application-name

```
Records added:         38766
```

```
- sent: 38766
Bytes added: 3217578
- sent: 3217578
```

Client: Option sub-application-table

```
Records added: 858
- sent: 858
Bytes added: 144144
- sent: 144144
```

Client: Option options application-attributes

```
Records added: 38038
- sent: 38038
Bytes added: 9813804
- sent: 9813804
```

Client: Option options tunnel-tloc-table

```
Records added: 26
- sent: 26
Bytes added: 1352
- sent: 1352
```

Client: MMA EXPORTER GROUP MMA-EXP-1

```
Records added: 0
Bytes added: 0
```

Client: Flow Monitor 175_SDWAN-art_ipv4

```
Records added: 0
Bytes added: 0
```

詳細については、「[show performance monitor context](#)」コマンドページを参照してください。

フローレコードキャッシュの表示

次の出力例は、指定したモニター（この場合は CISCO-MONITOR-art_ipv4）のフローレコードキャッシュを示しています。

```
Device# show performance monitor cache
```

```
Monitor: CISCO-MONITOR
```

```
Data Collection Monitor:
```

```
Cache type:                               Synchronized (Platform cache)
Cache size:                                4000
Current entries:                            0

Flows added:                               0
Flows aged:                                0
Synchronized timeout (secs):               60
```

```
Monitor: CISCO-MONITOR-art_ipv4
```

```
Data Collection Monitor:
```

```
Cache type:                               Synchronized (Platform cache)
Cache size:                                11250
Current entries:                            0

Flows added:                               0
Flows aged:                                0
Synchronized timeout (secs):               60
```

詳細については、「[show performance monitor cache](#)」コマンドページを参照してください。

パフォーマンス モニター テンプレートの表示

次の出力例は、指定したモニターのフロー エクスポータ テンプレート情報を示しています。

```
Device# show flow exporter CISCO-MONITOR templates
```

```
Flow Exporter CISCO-MONITOR:
```

```
Client: Option options sampler-table
```

```
Exporter Format: IPFIX (Version 10)
```

```
Template ID      : 257
```

```
Source ID       : 6
```

```
Record Size    : 48
```

```
Template layout
```

Field	ID	Ent.ID	Offset	Size
FLOW SAMPLER	48		0	4
flow sampler name	84		4	41
flow sampler algorithm export	49		45	1
flow sampler interval	50		46	2

```
Client: Option options application-name
```

```
Exporter Format: IPFIX (Version 10)
```

```
Template ID      : 258
```

```
Source ID       : 6
```

```
Record Size    : 83
```

```
Template layout
```

Field	ID	Ent.ID	Offset	Size
APPLICATION ID	95		0	4
application name	96		4	24
application description	94		28	55

Client: Option sub-application-table

Exporter Format: IPFIX (Version 10)

Template ID : 259

Source ID : 6

Record Size : 168

Template layout

Field	ID	Ent.ID	Offset	Size
APPLICATION ID	95		0	4
SUB APPLICATION TAG	97		4	4
sub application name	109		8	80
sub application description	110		88	80

Client: Option options application-attributes

Exporter Format: IPFIX (Version 10)

Template ID : 260

Source ID : 6

Record Size : 258

Template layout

Field	ID	Ent.ID	Offset	Size
APPLICATION ID	95		0	4
application category name	12232	9	4	32
application sub category name	12233	9	36	32
application group name	12234	9	68	32
application traffic-class	12243	9	100	32
application business-relevance	12244	9	132	32
p2p technology	288		164	10
tunnel technology	289		174	10

```

| encrypted technology          | 290 |   | 184 | 10 |
| application set name         | 12231 | 9 | 194 | 32 |
| application family name     | 12230 | 9 | 226 | 32 |

```

Client: Option options tunnel-tloc-table

Exporter Format: IPFIX (Version 10)

Template ID : 261

Source ID : 6

Record Size : 52

Template layout

```

-----
| Field                               | ID | Ent.ID | Offset | Size |
-----
| TLOC TABLE OVERLAY SESSION ID     | 12435 | 9 | 0 | 4 |
| tloc local color                    | 12437 | 9 | 4 | 16 |
| tloc remote color                   | 12439 | 9 | 20 | 16 |
| tloc tunnel protocol                | 12440 | 9 | 36 | 8 |
| tloc local system ip address        | 12436 | 9 | 44 | 4 |
| tloc remote system ip address       | 12438 | 9 | 48 | 4 |
-----

```

Client: Flow Monitor CISCO-MONITOR-art_ipv4

Exporter Format: IPFIX (Version 10)

Template ID : 0

Source ID : 0

Record Size : 208

Template layout

```

-----
| Field                               | ID | Ent.ID | Offset | Size |
-----
| interface input snmp                | 10 |   | 0 | 4 |
| connection client ipv4 address      | 12236 | 9 | 4 | 4 |
-----

```


connection server ipv4 address	12237	9	8	4
ip dscp	195		12	1
ip protocol	4		13	1
ip ttl	192		14	1
connection server transport port	12241	9	15	2
connection initiator	239		17	1
timestamp absolute monitoring-interval	359		18	8
flow observation point	138		26	8
overlay session id input	12432	9	34	4
routing vrf service	12434	9	38	4
application id	95		42	4
interface output snmp	14		46	4
flow direction	61		50	1
flow sampler	48		51	1
overlay session id output	12433	9	52	4
timestamp absolute first	152		56	8
timestamp absolute last	153		64	8
connection new-connections	278		72	4
connection sum-duration	279		76	8
connection server counter bytes long	232		84	8
connection server counter packets long	299		92	8
connection client counter bytes long	231		100	8
connection client counter packets long	298		108	8
connection server counter bytes network	8337	9	116	8
connection client counter bytes network	8338	9	124	8
connection delay response to-server sum	9303	9	132	4
connection server counter responses	9292	9	136	4
connection delay response to-server his	9300	9	140	4
connection client counter packets retra	9268	9	144	4
connection delay application sum	9306	9	148	4
connection delay response client-to-ser	9309	9	152	4
connection transaction duration sum	9273	9	156	4

connection transaction duration min	9275	9	160	4	
connection transaction duration max	9274	9	164	4	
connection transaction counter complete	9272	9	168	4	
connection client counter bytes retrans	9267	9	172	4	
connection server counter bytes retrans	9269	9	176	4	
connection server counter packets retrans	9270	9	180	4	
connection delay network long-lived to-	9255	9	184	4	
connection delay network to-client num-	9259	9	188	4	
connection delay network long-lived to-	9254	9	192	4	
connection delay network to-server num-	9258	9	196	4	
connection delay network long-lived cli	9256	9	200	4	
connection delay network client-to-serv	9257	9	204	4	

Client: Flow Monitor CISCO-MONITOR-media_ipv4

Exporter Format: IPFIX (Version 10)

Template ID : 0

Source ID : 0

Record Size : 180

Template layout

Field	ID	Ent.ID	Offset	Size
ipv4 source address	8		0	4
ipv4 destination address	12		4	4
interface input snmp	10		8	4
ip dscp	195		12	1
ip protocol	4		13	1
ip ttl	192		14	1
ipv6 source address	27		15	16
ipv6 destination address	28		31	16
transport source-port	7		47	2
transport destination-port	11		49	2

connection initiator	239		51	1	
timestamp absolute monitoring-interval	359		52	8	
flow observation point	138		60	8	
overlay session id input	12432	9	68	4	
routing vrf service	12434	9	72	4	
application id	95		76	4	
routing forwarding-status	89		80	1	
interface output snmp	14		81	4	
flow direction	61		85	1	
flow sampler	48		86	1	
overlay session id output	12433	9	87	4	
transport rtp ssrc	4254	9	91	4	
transport rtp payload-type	4273	9	95	1	
counter bytes long	1		96	8	
counter packets	2		104	4	
timestamp absolute first	152		108	8	
timestamp absolute last	153		116	8	
connection new-connections	278		124	4	
transport packets expected counter	4246	9	128	4	
transport packets lost counter	4251	9	132	4	
transport packets lost rate	4253	9	136	4	
transport rtp jitter mean	4255	9	140	4	
transport rtp jitter minimum	4256	9	144	4	
transport rtp jitter maximum	4257	9	148	4	
counter bytes rate	4235	9	152	4	
application media bytes counter	4236	9	156	4	
application media bytes rate	4238	9	160	4	
application media packets counter	4239	9	164	4	
application media packets rate	4241	9	168	4	
transport rtp jitter mean sum	4325	9	172	8	

 詳細については、「[show flow exporter](#)」 コマンドページを参照してください。



第 14 章

拡張型ポリシーベースルーティング



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 38: 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN の拡張版ポリシーベースルーティング	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	このリリースでは、拡張版ポリシーベースルーティング (ePBR) が Cisco Catalyst SD-WAN に拡張されています。ePBR は、トラフィックフローの柔軟なポリシーに基づいてトラフィックをルーティングする、プロトコルに依存しないトラフィックステアリングメカニズムです。ePBR ポリシーの作成には、Cisco SD-WAN Manager の CLI アドオンテンプレートを使用できます。

- [ePBR の概要 \(288 ページ\)](#)
- [ePBR の設定 \(289 ページ\)](#)
- [ePBR のモニター \(293 ページ\)](#)

ePBR の概要

拡張ポリシーベースルーティング (ePBR) は、ポリシーベースルーティング (PBR) の高度なバージョンです。この機能を使用すると、トラフィック転送はルーティングテーブルではなくポリシーに基づいて行われるため、ルーティングをより詳細に制御できます。ePBRはルーティングプロトコルが提供する既存のメカニズムを拡張および補完し、IPv4およびIPv6アドレス、ポート番号、プロトコル、パケットサイズなどの柔軟な一致基準に基づいてトラフィックをルーティングする、高度なローカルデータポリシーです。

ePBR は、柔軟性の高い Cisco Common Classification Policy Language (C3PL 言語) を使用してトラフィックを照合します。プレフィックス、アプリケーション、Differentiated Services Code Point (DSCP; DiffServ コードポイント)、セキュリティグループタグ (SGT) などの照合をサポートします。ePBR ではマッチ条件に基づいて、トラフィック転送用に単一または複数のネクストホップを設定できます。また、インターネットプロトコル サービス レベル契約 (IP SLA) トラッキングを設定するオプションもあります。設定されたネクストホップが使用できない場合、トラフィックは IP SLA トラッカーによって有効にされたダイナミックプローブを介して、使用可能なネクストホップにルーティングされます。

機能と利点

- IPv4 と IPv6 の両方をサポートします。
- 複数のネクストホップをサポートします。ネクストホップに到達できない場合、ePBR は次に利用可能なネクストホップに自動的に切り替えます。
- IP SLA トラッキングを設定するオプションがあります。これが設定されている場合、ネクストホップは IP SLA プロブが成功した場合にのみ選択されます。
SLA プロブは、同じ VRF または異なる VRF で設定できます。
- 現在のホップに到達できない場合は syslog メッセージが生成され、ユーザーに通知されます。

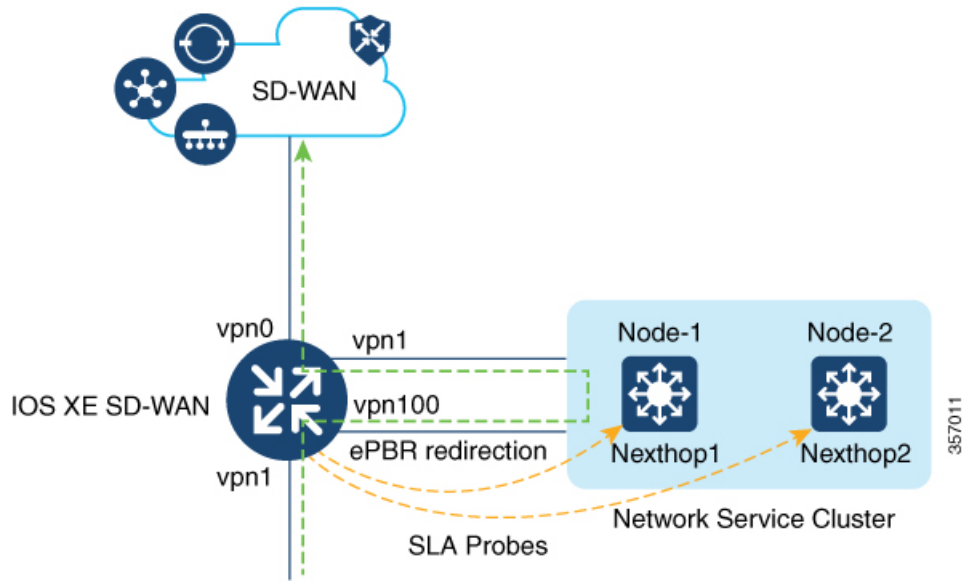
ePBR の仕組み

- ePBR はユニキャストルーティングにのみ適用され、C3PL を使用したトラフィック照合に基づきます。
- ePBR が有効なインターフェイスで受信されたすべてのパケットは、ポリシーマップを通過します。ePBR で使用するポリシーマップはポリシーを規定し、パケットの転送先を判断します。
- ePBR ポリシーは、トラフィックフローに適用される分類基準 (match) とアクション基準 (set) に基づきます。
- ePBR を有効にするには、パケットの一致基準と目的のポリシールーティングアクションを指定するポリシーマップを作成する必要があります。次に、そのポリシーマップを必要なインターフェイスに関連付けます。

- 一致基準は、クラスで指定されます。その後、ポリシーマップはクラスを呼び出し、set ステートメントに基づいてアクションを実行します。
- ePBR ポリシーの set ステートメントは、ネクストホップ、DSCP、VRF などの観点からルートを定義します。

使用例

図 16: ePBR を使用したトラフィックのリダイレクト



この例は、トラフィックがVPN1 インターフェイスに着信することを示しています。トラフィックはVPN1 で設定された分類に基づき、通常のルート転送をオーバーライドしてVPN100 のネクストホップにリダイレクトされます。トラフィックがVPN100 にリダイレクトされると、追加のネットワークサービスが着信トラフィックに適用されます。WAN 最適化などのネットワークサービスは、リダイレクトされたトラフィックに適用された後、VPN0 を介して Cisco Catalyst SD-WAN オーバーレイネットワークに転送されます。

ePBR の設定

Cisco SD-WAN Manager を使用して ePBR を設定するには、[CLI アドオン機能テンプレートを](#)作成し、[デバイステンプレートに](#)添付します。

このセクションでは、CLI アドオンテンプレートに追加できる ePBR の設定例を示します。

IPv4 での ePBR の設定

この例では、次のようになります。

- 拡張 ACL は、ネットワークまたはホストを定義します。
- クラスマップでは、ACL のパラメータを照合します。
- ePBR を使用したポリシーマップは、設定された set ステートメントに基づいて詳細なアクションを実行します。
- 複数のネクストホップが設定されています。ePBR は使用可能な最初のネクストホップを選択します。

```
ip access-list extended test300
 100 permit ip any 192.0.2.1 0.0.0.255
ip access-list extended test100
 100 permit ip any 192.0.2.20 0.0.0.255
!
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test1
!
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop 10.0.0.2 10.0.40.1 10.0.50.1 ...
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop 10.10.0.2 10.20.20.2 10.30.30.2 ...
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

IPv4 トラッキングの設定

トラッキングとともに ePBR を設定する例を次に示します。この例では次の動作になります。

- ICMP エコータイプの IP SLA 動作が設定され、ACL が定義されます。
- その後、クラスマップを使用して ACL 内のパラメータを照合し、ポリシーマップは設定された set ステートメントに基づいてアクションを実行します。
- set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2 の番号 10 は、シーケンス番号を表します。

```
ip sla 1
 icmp-echo 10.0.0.2
 vrf 100
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 state
ip sla 2
 icmp-echo 10.10.0.2
 vrf 300
ip sla schedule 2 life forever start-time now
track 2 ip sla 2 state
ip access-list extended test300
 100 permit ip any 10.10.0.2 0.0.0.255
ip access-list extended test100
 100 permit ip any 10.10.0.3 0.0.0.255
```



```

class-map match-any test300
  match access-group name test300
class-map match-any test100
  match access-group name test100
policy-map type epbr test300
  class test300
    set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2
policy-map type epbr test100
  class test100
    set ipv4 vrf 100 next-hop verify-availability 10.0.0.2 10 track 1
!
interface GigabitEthernet0/0/1
  service-policy type epbr input test300
interface GigabitEthernet0/0/2
  service-policy type epbr input test100

```

IPv6 での ePBR の設定

この例では、次のようになります。

- 拡張 ACL は、ネットワークまたはホストを定義します。
- クラスマップは、ACL のパラメータを照合するために使われます。
- ePBR を使用したポリシーマップは、設定された set ステートメントに基づいて詳細なアクションを実行します。
- 単一または複数のネクストホップアドレスを設定できます。ePBR は、使用可能な最初のネクストホップアドレスを選択します。

```

ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2001:DB81::/32
ipv6 access-list test100_v6
  sequence 100 permit ipv6 any 2001:DB82::/32
!
class-map match-any test300_v6
  match access-group name test300_v6
class-map match-any test100_v6
  match access-group name test100_v6
policy-map type epbr test300_v6
  class test300_v6
    set ipv6 vrf 300 next-hop 2001:DB8::1
policy-map type epbr test100_v6
  class test100_v6
    set ipv6 vrf 100 next-hop 2001:DB8::2 2001:DB8:FFFF:2 ...
!
interface GigabitEthernet0/0/1
  service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
  service-policy type epbr input test100_v6

```

IPv6 トラッキングの設定

IPv6 の ePBR を設定し、トラッキングを有効にする例を次に示します。この例では、次のようになります。

- ICMP エコータイプの IP SLA 動作が設定され、ACL が定義されます。

- その後、クラスマップを使用して ACL 内のパラメータを照合し、ポリシーマップは設定された set ステートメントに基づいてアクションを実行します。
- トラッキングは、IP SLA の結果が使用できない場合、クラスで設定されたネクストホップにパケットが送信されないように設定されます。

```
ip sla 3
  icmp-echo 2001:DB8::1
  vrf 100
ip sla schedule 3 life forever start-time now
track 3 ip sla 3 state
ip sla 4
  icmp-echo 2001:DB8::2
  vrf 300
ip sla schedule 4 life forever start-time now
track 4 ip sla 4 state
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2001:DB8::/32
ipv6 access-list test100_v6
  sequence 100 permit ipv6 any 2001:DB8::1/32
class-map match-any test300_v6
  match access-group name test300_v6
class-map match-any test100_v6
  match access-group name test100_v6
policy-map type epbr test300_v6
  class test300_v6
    set ipv6 vrf 300 next-hop verify-availability 2001:DB8::2 10 track 4
policy-map type epbr test100_v6
  class test100_v6
    set ipv6 vrf 100 next-hop verify-availability 2001:DB8::1 10 track 3
interface GigabitEthernet0/0/1
  service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
  service-policy type epbr input test100_v6
```

複数のネクストホップと SLA トラッキングを使用した IPv4 での ePBR の設定

この例では、次のようになります。

- ICMP エコータイプの IP SLA 動作が設定され、ACL が定義されます。
- その後、クラスマップを使用して ACL 内のパラメータを照合し、ポリシーマップは設定された set ステートメントに基づいてアクションを実行します。
- ネクストホップに対するトラッキングの設定は、前の IP アドレスが到達不能であり、IP SLA がネクストホップを到達可能であると確認した場合、パケットはネクストホップアドレスに流れます。

```
ip sla 1
  icmp-echo 10.0.0.2
  vrf 100
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 state
ip sla 2
  icmp-echo 10.10.0.2
  vrf 300
ip sla schedule 2 life forever start-time now
track 2 ip sla 2 state
ip sla 3
  icmp-echo 10.20.0.2
```

```

    vrf 400
ip sla schedule 3 life forever start-time now
track 3 ip sla 3 state
ip access-list extended test300
  100 permit ip any 192.0.2.1 255.255.255.0
ip access-list extended test100
  100 permit ip any 192.0.2.10 255.255.255.0
!
class-map match-any test300
  match access-group name test300
class-map match-any test100
  match access-group name test100
!
policy-map type epbr test300
  class test300
    set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2
    set ipv4 vrf 400 next-hop verify-availability 10.20.0.2 11 track 3
policy-map type epbr test100
  class test100
    set ipv4 vrf 100 next-hop verify-availability 10.0.0.2 10 track 1
!
interface GigabitEthernet0/0/1
  service-policy type epbr input test300
interface GigabitEthernet0/0/2
  service-policy type epbr input test100
!

```



- (注) ネクストホップがトラッカーとともに設定されているとき、ネクストホップが到達不能であるか、または IP SLA が失敗した場合、次に使用可能なホップが選択されます。つまり、トラッカーが設定された場合、ネクストホップの可用性と IP SLA の結果の両方がチェックされることとなります。

ePBR のモニター

ePBR は Cisco SD-WAN Manager ではモニタリングできません。設定の確認や、ePBR 統計情報のモニタリングを行うには、以下の show コマンドを使用します。

ネクストホップの可用性の確認

show platform software epbr track コマンドの出力例を次に示します。

```

Device# show platform software epbr track
Track Object:
obj num:2:
  track:0x7F94B4376760
  seq:10, nhop:123.0.0.2, nhop_reachable:1, track_handle:0x7F94AFDAE240,
  global:0, vrf_name:300, track_reachable:1
  parent:0x7F94B4383778, oce:0x7F94B81193A8
obj num:1:
  track:0x7F94B8187810
  seq:10, nhop:100.0.0.2, nhop_reachable:1, track_handle:0x7F94AFDAE1D0,
  global:0, vrf_name:100, track_reachable:1
  parent:0x7F94B8187778, oce:0x7F94B81188B8

```

この例では `nhop_reachable` の値は 1 で、ネクストホップが到達可能であることを示します。
`track_reachable` は SLA プロブの結果を表し、値は 1 で、ネクストホップが到達可能であることを示します。ネクストホップに到達できない場合、これらのパラメータの値は 0 になります。

ネクストホップの設定の表示

`show platform software epbr R0 feature-object redirect` でネクストホップの設定を表示します。



(注) 出力を表示するには、トラッカーを設定する必要があります。

```
Device# show platform software epbr r0 feature-object redirect
FMAN EPBR Redirect Feature Objectep

Feature Object ID: 9876543211
  Flags: 0x3
  Table ID: 0x4
  Next-hop: 10.10.10.2
  P2P ADJ-ID: 0

Feature Object ID: 1234567890
  Flags: 0x3
  Table ID: 0x2
  Next-hop: 172.16.0.0
  P2P ADJ-ID: 0
```



第 15 章

前方誤り訂正



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 39: 機能の履歴

機能名	リリース情報	説明
前方誤り訂正	Cisco IOS XE SD-WAN リリース 16.11.x	導入された機能。FEC は、4 つのパケットのグループごとに、「パリティ」パケットを付加して送信することで、リンク上で失われたパケットを回復するメカニズムです。

前方誤り訂正 (FEC) は、4 つのパケットのグループごとに、「パリティ」パケットを付加して送信することで、リンク上で失われたパケットを回復するメカニズムです。受信者がグループ内のパケットのサブセット (少なくとも N-1) とパリティパケットを受信する限り、グループ内で失われたパケットは 1 つまで回復できます。FEC は、Cisco IOS XE Catalyst SD-WAN デバイスでサポートされています。



- (注) FEC を使用する場合は、最小リリースとして Cisco IOS XE リリース 17.6.3 を推奨します。

- [前方誤り訂正に対応したデバイス \(296 ページ\)](#)

- ポリシーへの前方誤り訂正の設定 (296 ページ)
- 前方誤り訂正によるトンネル情報のモニター (297 ページ)
- 前方誤り訂正によるアプリケーションファミリー情報のモニター (298 ページ)
- CLI を使用した、前方誤り訂正のステータスのモニター (298 ページ)

前方誤り訂正に対応したデバイス

前方誤り訂正は、すべての Cisco IOS XE Catalyst SD-WAN デバイスでサポートされています。

ポリシーへの前方誤り訂正の設定

手順

- ステップ 1 Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
- ステップ 2 [一元管理型ポリシー (Centralized Policy)] をクリックし、[ポリシーの追加 (Add Policy)] をクリックします。
- ステップ 3 **[Next]** をクリックします。
- ステップ 4 もう一度 [次へ (Next)] をクリックし、[トラフィックルールの設定 (Configure Traffic Rules)] をクリックします。
- ステップ 5 [トラフィックデータ (Traffic Data)] をクリックし、[ポリシーの追加 (Add Policy)] ドロップダウンリストから、[新規作成 (Create New)] を選択します。
- ステップ 6 [シーケンスタイプ (Sequence Type)] をクリックします。
- ステップ 7 [データポリシーの追加 (Add Data Policy)] ポップアップメニューから、[QoS] を選択します。
- ステップ 8 [Sequence Rule] をクリックします。
- ステップ 9 [アプリケーション/アプリケーションファミリーリスト (Applications/Application Family List)] で、1 つ以上のアプリケーションまたはリストを選択します。
- ステップ 10 [承認 (Accept)] をクリック
- ステップ 11 [アクション (Actions)] をクリックし、[損失の修正 (Loss Corretion)] をクリックします。
- ステップ 12 [Actions] 領域で、次のいずれかを選択します。
 - **FEC 適応 (FEC Adaptive)** : システムによって検出された損失がパケット損失しきい値を超えた場合にのみ、FEC 情報を送信します。
 - **FEC 常時 (FEC Always)** : 送信ごとに常に FEC 情報を送信します。
 - **パケット複製 (Packet Duplication)** チェックボックス : 1 つのリンクがダウンした場合のパケット損失を減らすために、セカンダリリンクを介してパケットを複製します。
- ステップ 13 [Save Match and Actions] をクリックします。

ステップ 14 [データポリシーの保存 (Save Data Policy)] をクリックします。

ステップ 15 [次へ (Next)] をクリックし、次のアクションを実行して一元管理型ポリシーを作成します。

- a) [名前 (Name)] と [説明 (Description)] を入力します。
- b) [トラフィックデータ (Traffic Data)] を選択します。
- c) ポリシーの VPN とサイトリストを選択します。
- d) ポリシーを保存します。

前方誤り訂正によるトンネル情報のモニター

手順

ステップ 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。

ステップ 2 デバイスグループを選択します。

ステップ 3 左側のパネルで、**[WAN]** の下に表示される **[トンネル (Tunnel)]** をクリックします。

WAN トンネル情報には、次の情報が含まれます。

- 選択したトンネルの合計トンネル損失を示すグラフ。
- 各トンネルエンドポイントに関する次の情報を提供するテーブル。
 - トンネルエンドポイント名
 - エンドポイントが使用する通信プロトコル
 - エンドポイントの状態
 - エンドポイントのジッター (ミリ秒単位)
 - エンドポイントの packets 損失率
 - エンドポイントでの遅延 (ミリ秒単位)
 - エンドポイントから送信された合計バイト数
 - エンドポイントが受信した合計バイト数
 - アプリケーションの使用状況へのリンク

前方誤り訂正によるアプリケーションファミリー情報のモニター

手順

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

Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.6.1 以前 : Cisco SD-WAN Manager のメニューから [モニター (Monitor)]>[ネットワーク (Network)]の順に選択します。

ステップ2 デバイスグループを選択します。

ステップ3 左パネルの [アプリケーション (Applications)]の下に表示される [SAIE アプリケーション (SAIE Applications)]をクリックします。

(注) Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.7.1 以前のリリースでは、**SAIE アプリケーション**は**DPI アプリケーション**と呼ばれていました。

FEC 回復率アプリケーション情報には、次の情報が含まれます。

- 次のパースペクティブを選択できるグラフ。
 - [アプリケーションの使用率 (Application Usage)] : 選択したアプリケーションファミリーのさまざまなタイプのトラフィックの使用率 (KB 単位)。
- アプリケーションファミリーごとに次の情報を提示するテーブル。
 - アプリケーションファミリーの名前。
 - アプリケーションファミリーの packets 配信パフォーマンス。
 - (注) 選択したアプリケーションファミリーの packets 配信パフォーマンスを確認する必要がある場合は、packets 複製が有効になっていることを確認します。packets 配信パフォーマンスは、[packets 配信パフォーマンス (Packet Delivery Performance)]列の Cisco SD-WAN Manager ツールチップに表示される式に基づいて計算されます。
- 選択したアプリケーションファミリーのトラフィック使用量 (KB、MB、または GB 単位)。

CLI を使用した、前方誤り訂正のステータスのモニター

次のように、`show sdwan tunnel statistics fec` コマンドを使用して Cisco IOS XE Catalyst SD-WAN デバイス で FEC ステータスを確認します。


```

Device# show sdwan tunnel statistics fec
tunnel stats ipsec 80.80.10.19 80.80.10.25 12346 12366
fec-rx-data-pkts      0
fec-rx-parity-pkts   0
fec-tx-data-pkts     0
fec-tx-parity-pkts   0
fec-reconstruct-pkts 0
fec-capable          true
fec-dynamic          false
tunnel stats ipsec 80.80.10.19 80.80.10.50 12346 12346
fec-rx-data-pkts     122314
fec-rx-parity-pkts   30578
fec-tx-data-pkts     125868
fec-tx-parity-pkts   31467
fec-reconstruct-pkts 3
fec-capable          true
fec-dynamic          false

```

次の表で、**show sdwan tunnel statistics fec** コマンドの出力に関連する FEC カウンタを説明します。

カウンタの名前	説明
fec-rx-data-pkts	デバイスが受信したデータパケットの数を表示します。
fec-rx-parity-pkts	デバイスが受信したパリティパケットの数を表示します。
fec-tx-data-pkts	デバイスから送信されたデータパケットの数を表示します。
fec-tx-parity-pkts	デバイスから送信されたパリティパケットの数を表示します。
fec-reconstruct-pkts	デバイスによって再構築された受信パケットの数を表示します。



第 16 章

ノイズの多いチャネルに対するパケット複製



(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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 40: 機能の履歴

機能名	リリース情報	説明
ノイズの多いチャネルに対するパケット複製	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	これは、ノイズの多いチャネルでのパケット損失を軽減し、音声とビデオに対する高いアプリケーション QoE を維持するのに役立つ機能です。

- [パケット複製について \(301 ページ\)](#)
- [パケット複製の設定 \(302 ページ\)](#)

パケット複製について

Cisco IOS XE Catalyst SD-WAN デバイス では、パケット複製を使用してパケット損失を回避します。

パケット複製は、Cisco IOS XE Catalyst SD-WAN デバイス に到達するために使用可能な代替パスにパケットの複製を送信する機能です。パケットの1つが失われると、複製をサーバーに転送します。受信側 Cisco IOS XE Catalyst SD-WAN デバイス はパケットの複製を破棄し、1つのパケットをサーバーに転送します。

パケット複製は、複数のアクセスリンクを持つエッジに適しています。パケット複製が設定され、デバイスにプッシュされると、トンネルパケットの複製統計情報を確認できます。

パケット複製は、ポリシー内のローカルまたはリモートの TLOC と組み合わせて機能することはできません。パケット複製トンネルを指定するとき、データポリシーまたは AAR は設定されません。



(注) Cisco IOS XE Catalyst SD-WAN デバイスでのパケット複製の相互運用性、前方誤り訂正 (FEC)、および TCP 最適化は、Cisco IOS XE リリース 16.x と Cisco IOS XE Catalyst SD-WAN リリース 17.x バージョンの間ではサポートされていません。

パケット複製の設定

1. [設定 (Configuration)] > [ポリシー (Policies)] を選択します。
2. ページ上部にある [一元管理型ポリシー (Centralized Policy)] を選択し、[ポリシーの追加 (Add Policy)] をクリックします。
3. [次へ (Next)] を 2 回クリックして、[トラフィックルールの設定 (Configure Traffic Rules)] を選択します。
4. [トラフィックデータ (Traffic Data)] を選択し、[ポリシーの追加 (Add Policy)] ドロップダウンから [新規作成 (Create New)] をクリックします。
5. 左側のペインで、[シーケンスタイプ (Sequence Type)] をクリックします。
6. [データポリシーの追加 (Add Data Policy)] ポップアップから、[QoS] を選択します。
7. [Sequence Rule] をクリックします。
8. [アプリケーション/アプリケーションファミリリスト/データプレフィックス (Applications/Application Family List/Data Prefix)] で、1 つ以上のアプリケーションまたはリストを選択します。
9. [アクション (Actions)] をクリックし、[損失の修正 (LossCorrection)] を選択します。
10. [アクション (Actions)] エリアで、[パケット複製 (Pack Duplication)] オプションを選択して、パケット複製機能を有効にします。
 - **FEC 適応 (FEC Adaptive)** : システムがパケット損失を検出した場合にのみ、前方誤り訂正 (FEC) 情報を送信します。
 - **FEC 常時 (FEC Always)** : 送信ごとに常に FEC 情報を送信します。

- なし (None) : 損失保護が必要ない場合に使用します。
- パケット複製 (Packet Duplication) : パケット損失を減らすため、パケットを複製して次に使用可能なリンクに送信する必要がある場合に有効にします。

11. [Save Match and Actions] をクリックします。
12. [データポリシーの保存 (Save Data Policy)] をクリックします。
13. [次へ (Next)] をクリックし、次のアクションを実行して一元管理型ポリシーを作成します。
 - [名前 (Name)] と [説明 (Description)] を入力します。
 - [トラフィックデータ (Traffic Data)] を選択します。
 - ポリシーの [VPN/サイトリスト (VPNs/site list)] を選択します。
 - ポリシーを保存します。



第 17 章

ポリシー構成のタグ付け



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 41:機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN コントローラの CLI テンプレートを 使用した Cisco Catalyst SD-WAN ポリシー設定のタグ 付けのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能を使用すると、複数のポリシーオブジェクトを1つのタグにグループ化できます。Cisco Catalyst SD-WAN の一元管理型ポリシーまたはローカライズ型ポリシーでタグメカニズムを使用すると、次の機能を利用できます。 <ul style="list-style-type: none"> • Cisco Catalyst SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイスの間のポリシーのダウンロード速度を制御する。 • Cisco Catalyst SD-WAN コントローラ で定義されたリストの管理を改善する。 • インテントベース ネットワークの設定をより適切に整理する。

- [ポリシー構成のタグ付けに対応したデバイス \(307 ページ\)](#)
- [ポリシー構成のタグ付けに関する制約事項 \(307 ページ\)](#)
- [ポリシー構成のタグ付けについて \(308 ページ\)](#)
- [ポリシー構成のタグ付けの利点 \(310 ページ\)](#)
- [CLI テンプレートを
使用したポリシー構成のタグ付け設定 \(311 ページ\)](#)
- [CLI を使用した Tag-Instances 設定の確認 \(313 ページ\)](#)

ポリシー構成のタグ付けに対応したデバイス

表 42: 対応デバイスとリリース

リリース	サポートされるデバイス数
Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a 以降	<ul style="list-style-type: none"> • Cisco Catalyst 8500 シリーズ エッジプラットフォーム • Cisco Catalyst 8300 シリーズ エッジプラットフォーム • Cisco Catalyst 8200 シリーズ エッジプラットフォーム • Cisco Catalyst 8200 uCPE シリーズ エッジプラットフォーム • Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ • Cisco ISR 1000 および ISR 4000 シリーズ サービス統合型ルータ (ISR) • Cisco ISR 1100 および ISR 1100X シリーズ サービス統合型ルータ (ISR) • Cisco IR1101 耐環境性能 サービス統合型ルータ • Cisco CSR 1000v シリーズクラウドサービスルータ (CSR 1000V) • Cisco Catalyst 8000V Edge ソフトウェア (Catalyst 8000V)

これらの各デバイスファミリでサポートされるモデルの詳細については、「[Cisco SD-WAN Device Compatibility](#)」のページを参照してください。

ポリシー構成のタグ付けに関する制約事項

- data-prefix-lists、data-ipv6-prefix-lists、および app-lists タグメンバーのみが対応しています。
- 同一タグ内で方向属性ありとなし両方のタグを設定することはできません。
- Cisco SD-WAN コントローラ CLI テンプレートののみを使用したタグの構成がサポートされています。
- マルチテナントには対応していません。

- 構成できるタグの数は、最大 255 までです。
- 構成できるタグごとのオブジェクトは 64 までです。

ポリシー構成のタグ付けについて

ポリシー構成のタグ付けは、ポリシーオブジェクトをグループ化し、ポリシーを定義してさまざまなトラフィックフローにタグの値を割り当てることができる機能です。タグは、インテントベースのネットワーク設定を実現するために使用されるポリシーオブジェクトの機能に基づいて、名前を付けることができます。Cisco SD-WAN コントローラを通じてプロビジョニングされるこれらのタグは、トラフィック分類のポリシールールで使用されます。

各タグの作成時には、一意のタグ ID を割り当てることができます。

タグメンバーは、タグオブジェクトで直接参照されるタグ名で定義できます。タグメンバーは、方向属性ありにもなしにもできます。対応タグメンバーのタイプは次のとおりです。

- Data-prefix-list
- Data-ipv6-prefix-list
- App-list

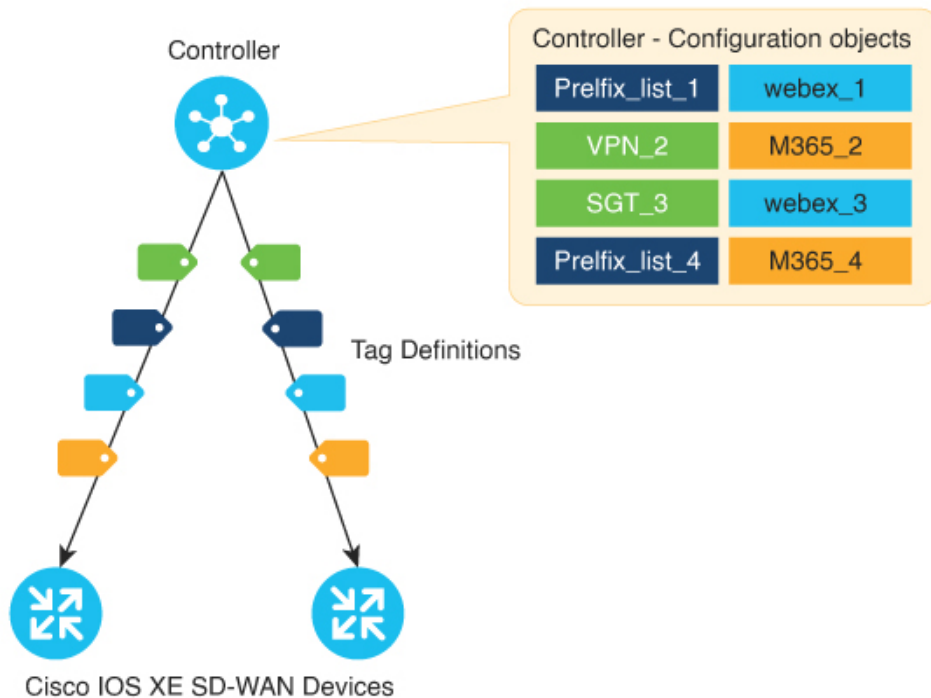
Data-prefix-list および data-ipv6-prefix-list は方向属性であり、data-policy のマッチステートメントで送信元または宛先のキーワードとして照合されます。アプリケーションリストは方向を示さない属性です。アプリケーションリストポリシーのマッチステートメントでは、アプリケーション ID などの方向を示さないキーワードを使用できます。方向を示す属性と方向を示さない属性を同一タグ内でグループ化することはできません。

ローカライズ型ポリシーと一元管理型ポリシーの下で、マッチ基準に設定されたタグを適用できます。デバイスはタグ設定を処理し、タグがポリシーで参照されると、その設定をデータプレーンに適用します。

構成タイプ機能を使用して、構成内のオブジェクトにタグを付けることができます。構成タグは、データポリシー、アプリケーション認識型ルーティングポリシー、ローカライズ型アクセスリストポリシーなどの Cisco Catalyst SD-WAN 一元管理型ポリシーで使用されます。次のタグ属性は、以下のようなポリシー マッチ シーケンス ステートメントで使用されます。

- Source-tag-instance
- Destination-tag-instance
- Tag-instance

図 17: Cisco Catalyst SD-WAN ネットワークでのポリシー構成のタグ付け



357815

図に示すように、Cisco SD-WAN コントローラ で一意のタグ ID を持つポリシーオブジェクトを使用してタグを設定できます。タグ ID が割り当てられると、これらのタグはネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイスにプッシュされ、そこでこれらのタグが参照されます。デバイスは次に、ポリシールールで使用されるタグからポリシーリストオブジェクトを抽出します。

ポリシー構成のタグ付け機能

- 対応しているのは、構成タイプのタグのみです。
- オブジェクト構成グループのタグ付けに対応しています。
- 対応しているタグメンバーは、data-prefix-lists、data-ipv6-prefix-lists、および app-lists です。
- **定義済みタグ**と呼ばれるタグ中心のモデルによる構成タグの定義をサポートします。
- Cisco SD-WAN Manager からの Cisco SD-WAN コントローラ CLI テンプレートを介した構成の追加のみをサポートします。

タグ付けのワークフロー

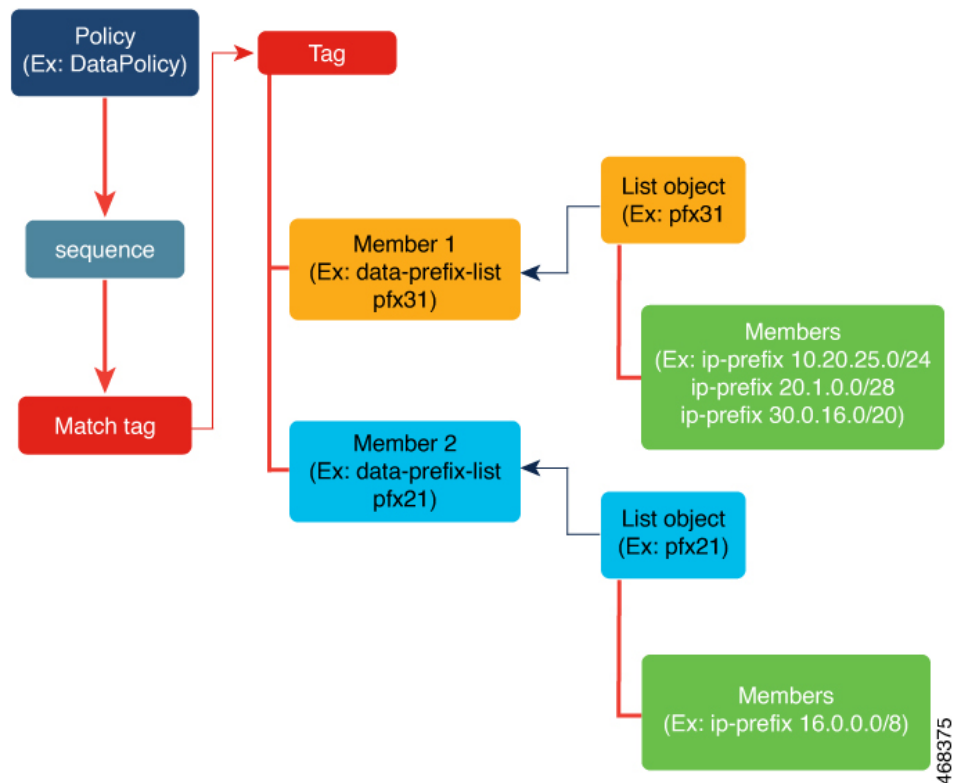
1. Cisco SD-WAN コントローラ で、ネットワークインテントに基づくタグを作成します。
2. 次のポリシー リスト オブジェクト メンバーを追加します。
 - 各ロケーションのデータプレフィックス

- アプリケーションの app-lists

ポリシーリストオブジェクトは、タグインスタンスに追加した後も、ワークフローでいつでも定義できます。

3. これらのタグをネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイスにプッシュします。
4. 複数のマッチシーケンスを含むポリシーを作成し、Cisco Catalyst SD-WAN のデータポリシー、アプリケーション認識型ルーティングポリシー、およびアクセスリストポリシーにタグオブジェクトを含めます。
5. タグを追加または削除すると、ステータスが自動的にポリシーに反映されます。
6. ポリシーを更新して、新しいタグオブジェクトを含めます。

図 18: タグ付けワークフローの例示



ポリシー構成のタグ付けの利点

ポリシー構成のタグ付けを使用する利点は次のとおりです。

- ポリシーオブジェクトの再利用を有効化。

- 構成サイズとシーケンスを削減して、デバイスでのポリシーのダウンロードを高速化。
- 異なるポリシー間でのタグ共有のサポート。
- ユーザー定義のインテントで、ネットワーク全体の可視性または相関関係を有効化。
- Cisco SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス の間のポリシー設定のダウンロード速度を制御。
- コントローラで定義されたリストの管理を改善。
- インテントベースネットワークの設定について整理。

CLI テンプレートを使用したポリシー構成のタグ付け設定

はじめる前に

コントローラとエッジデバイスがすべて最新バージョン（Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.9.x、Cisco vManage リリース 20.9.1、およびCisco IOS XE Catalyst SD-WAN リリース 17.9.1a）に更新されていることを確認します。

CLI テンプレートを使用したポリシー構成のタグ付け設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および [CLI テンプレート](#)を参照してください。



- (注) デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

このセクションでは、Cisco SD-WAN コントローラ CLI テンプレートを使用してタグインスタンスと一元管理型ポリシーを設定するための CLI 設定の例を示します。

ポリシー構成のタグ付けの作成

1. Cisco SD-WAN コントローラ で新しいオブジェクトである `tag-instance` を設定します。

```
tag-instances [tag-instance] [lists]
```

2. `app-lists`、`data-ipv6-prefix-list`、`data-prefix-list` などのメンバー属性を持つタグインスタンスを作成します。タグインスタンスはタグ名ごとにグローバルな一意の ID を持つようになります。タグ設定は、次のタグを参照するデバイスにのみプッシュされます。

```
tag-instance tag-instance-name [id global-unique-id] [app-list app-list-name]  
[data-prefix-list prefix-list-name] [data-ipv6-prefix-list  
ipv6-prefix-list-name]
```

3. タグインスタンスリストを設定します。

```
lists [app-list app-list-name] [data-prefix-list prefix-list-name]
[data-ipv6-prefix-list ipv6-prefix-list-name]
```

ポリシー一致基準へのタグインスタンスの追加

1. ローカライズされたアクセスリストポリシー（ACL および IPv6 ACL）を設定して、一致する属性に宛先タグまたは送信元タグインスタンスを含めます。

```
match [destination-tag-instance dest-tag-name | source-tag-instance
src-tag-name]
```

2. 一致する属性に destination-tag-instance、source-tag-instance、または tag-instance を含めるように、一元管理型データポリシーを設定します。

```
match [destination-tag-instance dest-tag-name | source-tag-instance
src-tag-name | tag-instance tag-name]
```

3. 一致する属性に destination-tag-instance、source-tag-instance、または tag-instance を含めるように、一元管理型のアプリケーション認識型ルーティング（AAR）ポリシーを設定します。

```
match [destination-tag-instance dest-tag-name | source-tag-instance
src-tag-name | tag-instance tag-name]
```

タグインスタンスを作成するための設定例の全容を次に示します。これにはローカライズ型ポリシーと一元管理型ポリシーの一致属性としてのタグインスタンスも含まれます。

```
****Tag Configuration****
tag-instances
tag-instance blue
  id 2000
  data-ipv6-prefix-list v6_pfx1 v6_pfx2
!
tag-instance orange
  id 3000
  app-list appl1 appl2
!
lists
data-prefix-list pfx1
  ip-prefix 10.0.0.1/32
!
data-ipv6-prefix-list v6_pfx1
  ipv6-prefix 2001::1/128
!
app-list appl1
  app amazon
!
!
****Localized Policy****
policy
lists
  data-prefix-list pfx1
  ip-prefix 10.20.24.0/24
!
!
access-list acl
  sequence 10
  match
```

```
        source-tag-instance blue
        !
        action accept
        count acl_input_wc
        !
        !
        default-action drop
        !
    !
    ****Centralized Policy ****
    policy
    data-policy DP1
    vpn-list vpn1
    sequence 100
    match
    tag-instance orange
    !
    action accept
    !
    !
    sequence 200
    match
    source-tag-instance blue
    !
    action drop
    count count1
    !
    !
    sequence 300
    match
    destination-tag-instance blue
    !
    action accept
    !
```

CLI を使用した Tag-Instances 設定の確認

以下は、Cisco IOS XE Catalyst SD-WAN デバイスの Cisco SD-WAN コントローラ からダウンロードされたタグを表示する **show sdwan tag-instances from-vsmart** コマンドの出力例です。

```
Device# show sdwan tag-instances from-vsmart
tag-instances-from-vsmart
tag-instance APP_facebook_TAG9
  id 60000
  app-list apps_facebook
tag-instance APP_office_TAG10
  id 70000
  app-list apps_ms apps_zoom
tag-instance APP_webex_TAG8
  id 50000
  app-list apps_webex
lists data-prefix-list multicast_pfx
  ip-prefix 10.10.20.30/8
lists data-prefix-list pfx1
  ip-prefix 10.20.24.0/24
lists data-prefix-list pfx21
  ip-prefix 172.16.10.10/8
lists data-prefix-list pfx22
  ip-prefix 172.16.20.20/16
  ip-prefix 192.168.10.20/8
lists data-ipv6-prefix-list v6_pfx1
```

```

ipv6-prefix 2001::/64
lists data-ipv6-prefix-list v6_pfx21
  ipv6-prefix 2001::1/128
  ipv6-prefix 2001::/64
lists app-list apps_facebook
  app dns
  app facebook
lists app-list apps_ms
  app ms-office-365
  app ms-office-web-apps
  app ms-services
  app ms-teams
  app pop3
lists app-list apps_webex
  app sip
  app webex-audio
  app webex-control
  app webex-media
  app webex-meeting
  app webex-video
lists app-list apps_zoom
  app zoom-meetings

```

以下は、Cisco IOS XE Catalyst SD-WAN デバイスの Cisco SD-WAN コントローラ からダウンロードされたポリシーを表示する **show sdwan policy from-vsmart** コマンドの出力例です。

```

Device# show sdwan policy from-vsmart
from-vsmart sla-class SLA1
  latency 100
from-vsmart data-policy DATA_POLICY
  direction from-service
  vpn-list vpn_1
  sequence 11
    match
      destination-port      5060
      protocol               17
      source-tag-instance   DP_V4_TAG1
      destination-tag-instance DP_V4_TAG3
    action accept
      count src_dst_legacy_v4
  sequence 21
    match
      source-tag-instance DP_V4_TAG1
    action drop
      count src_v4
  sequence 31
    match
      source-tag-instance   DP_V4_TAG2
      destination-tag-instance DP_V4_TAG3
      tag-instance         APP_webex_TAG8
    action drop
      count src_dst_app_v4
  sequence 41
    match
      source-tag-instance   DP_V4_TAG1
      destination-tag-instance DP_V4_TAG3
      tag-instance         APP_facebook_TAG9
    action accept
      count src_dst_app2_v4

```

以下は、フォワーディングプレーン (FMAN-FP) のフォワーディングマネージャからのタグ情報を表示する **show platform software common-classification** コマンドの出力例です。


```

Device# show platform software common-classification F0 tag all
Total Number of TAGs: 9
tag id      tag name      tag type      num clients  num sets      num member
types      total members
-----
900         special_TAG7  Per Type OR  0             2             1
  2
10000      DP_V4_TAG1    Per Type OR  1             1             1
  1
11000      DP_V4_TAG2    Per Type OR  1             2             1
  2
12000      DP_V4_TAG3    Per Type OR  1             6             1
  6
20000      DP_V6_TAG4    Per Type OR  1             1             1
  1
21000      DP_V6_TAG5    Per Type OR  1             2             1
  2
50000      APP_webex_TAG8 Per Type OR  1             1             1
  1
60000      APP_facebook_TAG9 Per Type OR  1             1             1
  1
70000      APP_office_TAG10 Per Type OR  1             2             1
  2
    
```

```

Device# show platform software common-classification f0 tag 1 summary
TAG ID: 1
TAG TYPE: Per Type OR
TAG Name: net1
Is Dummy: F
    
```

```

client data:
  client id      client name
-----
  166            SDWAN
    
```

```

member data:
  Prefix List      6
  App List         3
    
```

```

Device# show platform software common-classification f0 tag 1 prefixList
member details:
member detail type      member id      member data
-----
IPv4 Prefix List       65537          100
IPv6 Prefix List       65538          101
IPv4 Prefix List       65540          103
IPv6 Prefix List       65541          104
IPv6 Prefix List       65544          107
IPv4 Prefix List       65546          109
    
```

```

Device# show platform software common-classification f0 tag 1 appList
member details:
member detail type      member id      member data
-----
App List                65539          102
App List                65542          105
App List                65545          108
    
```

```

Device# show platform software common-classification f0 tag 1 set
Total Number of SETs: 18
Set ID      member detail type      member id      member data
-----
  1          IPv4 Prefix List       65537          100
  1          App List               65539          102
  2          IPv4 Prefix List       65537          100
  2          App List               65542          105
    
```

3	IPv4 Prefix List	65537	100
3	App List	65545	108
4	IPv6 Prefix List	65538	101
4	App List	65539	102
5	IPv6 Prefix List	65538	101



第 18 章

Cisco IOS XE Catalyst SD-WAN デバイスと ACI の統合



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 43: 機能の履歴

機能名	リリース情報	説明
ACI との統合	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	Cisco IOS XE Catalyst SD-WAN と ACI の統合機能で、事前定義された SLA クラウドベッドがサポートされるようになりました。また、データプレフィックスリストから動的に生成されたマッピングをサポートし、ACI によって提供される SLA クラスへの VPN リストが含まれています。

ACI リリース 4.1(1) では、WAN SLA ポリシーのサポートが追加されています。この機能を使用すると、テナント管理者は事前構成されたポリシーを適用して、WAN 経由のテナントトラフィックのパケット損失、ジッター、および遅延のレベルを指定できます。WAN SLA ポリシーをテナントトラフィックに適用すると、Cisco APIC は事前設定されたポリシーを Cisco Catalyst SD-WAN コントローラに送信します。Cisco IOS XE Catalyst SD-WAN 機能を提供する外部デバイスマネージャとして ACI で設定されている Cisco Catalyst SD-WAN コントローラは、SLA ポリシーで指定された損失、ジッター、および遅延パラメータを満たす最適な WAN リンクを選択します。

WAN SLA ポリシーは、契約を通じてテナントトラフィックに適用されます。

この機能が役立つ例として、MPLS、インターネット、4Gなどの複数の転送技術を使用して、ブランチがデータセンターにWANを介して接続するという展開を考えてみます。このような展開では、ブランチとデータセンターの間に複数のパスが存在する可能性があります。この機能は、アプリケーショングループとSLAに基づき、このような状況下でも最適化パスを選択できるようにします。

- [Cisco ACI との統合に関するガイドライン \(318 ページ\)](#)
- [Cisco ACI 登録の確認 \(319 ページ\)](#)
- [SLA クラス \(319 ページ\)](#)
- [データプレフィックス \(319 ページ\)](#)
- [VPNs \(320 ページ\)](#)
- [SLA へのデータプレフィックスと VPN のマッピング \(320 ページ\)](#)
- [App-Route-Policy の作成 \(320 ページ\)](#)
- [ACI サイトのマッピング \(321 ページ\)](#)
- [ACI サイトのマッピング解除 \(322 ページ\)](#)
- [コントローラの削除 \(322 ページ\)](#)

Cisco ACI との統合に関するガイドライン

統合を設定するために Cisco SD-WAN Manager で実行する一般的な手順は次のとおりです。

1. [Cisco ACI 登録の確認 \(319 ページ\)](#) の手順の説明に従って、Cisco ACI が目的のコントローラを Cisco Catalyst SD-WAN コントローラのパートナーとして登録したことを確認します。
2. 「ACI サイトのマッピング」セクションの説明に従って、デバイスを Cisco Catalyst SD-WAN コントローラに接続します。

Cisco ACI と Cisco SD-WAN Manager を統合する場合は、次のガイドラインが適用されます。

- この統合は、新しい Cisco IOS XE Catalyst SD-WAN 展開でのみサポートされます。
- Cisco APIC がポリシーを送信するデバイスに、アプリケーション認識型ルーティングポリシーが設定されていないことを確認します。
- Cisco APIC がポリシーを送信する各デバイスにテンプレートが添付されていることを確認します。
- 統合を開始する前に、CLI ポリシービルダーを使用して一元管理型ポリシーを作成し、Cisco SD-WAN Manager ポリシービルダーを使用してアクティブにします。
- WAN SLA ポリシーを適用する前に、Cisco Catalyst SD-WAN コントローラ と Cisco APIC 間の接続を確立します。手順については、「Cisco ACI と Cisco IOS XE Catalyst SD-WAN 統合」を参照してください。
- デバイスを接続する前に、この統合用に Cisco ACI を設定します。

Cisco ACI 登録の確認

Cisco SD-WAN Manager との統合用に Cisco ACI を設定した後、Cisco SD-WAN Manager の次の手順を実行して、Cisco ACI が目的のコントローラを Cisco SD-WAN Manager パートナーとして登録したことを確認します。

1. Cisco SD-WAN Manager で、[管理 (Administration)] > [統合管理 (Integration Management)] を選択します。

[統合管理 (Integration Management)] ページが表示されます。

2. [統合管理 (Integration Management)] ページで、Cisco APIC がポリシーを送信するコントローラの [説明 (Description)] に ACI パートナー登録が表示されていることを確認します。

SLA クラス

Cisco SD-WAN Manager は、ACI 統合で使用する事前設定された SLA クラスを提供します。これらの SLA クラスは自動的に使用可能になり、変更または削除できません。

これらの SLA を表示するには、次の手順に従います。

1. Cisco SD-WAN Manager で、[設定 (Configuration)] > [ポリシー (Policies)] の順に選択します。
2. [カスタムオプション (Custom Options)] ドロップダウンリストから、[リスト (Lists)] を選択します。
3. 左側のタイプ一覧から [SLA クラス (SLA Class)] を選択します。

次の SLA クラスを使用できます。

- [ビジネス通常 (Business Normal)] : 通常の事業運営向けに設計されたもの
- [音声 (Voice)] : 音声操作用に設計されたもの
- [ビジネス重要 (Business Critical)] : 低パケット損失と低遅延を必要とする重要な事業運営向けに設計されたもの
- [ビジネス高 (Business High)] : 非常に重要なビジネス運営向けに設計されたもの

データプレフィックス

Cisco ACI は、統合に必要なデータプレフィックスリストを作成し、必要に応じてこれらのリストを動的に更新します。Cisco SD-WAN Manager でデータプレフィックスを設定する必要はありません。

これらのデータプレフィックスを表示するには、次の手順に従います。

1. Cisco SD-WAN Manager で、[設定 (Configuration)] > [ポリシー (Policies)] を選択します。
2. [カスタムオプション (Custom Options)] ドロップダウンリストから、[リスト (Lists)] を選択します。
3. 左側のタイプリストから [データプレフィックス (Data Prefix)] を選択します。

Cisco ACI はこれらのデータプレフィックスを自動的に提供するため、このリストの情報は異なる場合があります。最新の情報を表示するため、随時ページを更新してください。

VPNs

ACI は、統合に必要な VPN を作成し、Cisco SD-WAN Manager に送信します。これらの VPN は Cisco SD-WAN Manager で自動的に使用可能になります。Cisco SD-WAN Manager で VPN を設定する必要はありません。

これらの VPN を表示するには、次の手順に従います。

1. Cisco SD-WAN Manager で、[設定 (Configuration)] > [ポリシー (Policies)] の順に選択します。
2. [カスタムオプション (Custom Options)] ドロップダウンリストから、[リスト (Lists)] を選択します。
3. 左側のタイプ一覧から [VPN] を選択します。

SLA へのデータプレフィックスと VPN のマッピング

ACI はデータプレフィックスリストと VPN リストから SLA クラスへのマッピングを確立した後、そのマッピングを Cisco SD-WAN Manager に送信します。これらのマッピングは、Cisco SD-WAN Manager のアプリケーションルート ポリシーを設定するページで確認できます。

App-Route-Policy の作成

ACI によってデータプレフィックスと VPN が SLA クラスリストにマッピングされると、app-route-policy を作成して Cisco ACI 統合のシーケンスルールを定義できます。

App-route-policy を作成するには、次の手順を実行します。

1. Cisco SD-WAN Manager で、[設定 (Configuration)] > [ポリシー (Policies)] の順に選択します。
2. 一元管理型ポリシーを含む行の右側にある [その他のアクション (More Actions)] アイコンをクリックして、[編集 (Edit)] をクリックします。

3. [トラフィックルール (Traffic Rules)] を選択します。
4. [ポリシーの追加 (Add Policy)] > [新規作成 (Create New)] の順に選択します。
5. [ACIシーケンスルール (ACI Sequence Rules)] をクリックします。
6. [VPN] ドロップダウンから、VPN ID を選択します。Cisco SD-WAN Manager で、この VPN にマッピングされているデータプレフィックスと SLA クラスのリストが表示されます。(これらのマッピングを送信したのは ACI です)。
7. ポリシーに含めるデータプレフィックスと SLA クラスの左側にあるチェックボックスをオンにし、[インポート (Import)] をクリックします。
8. [名前 (Name)] フィールドにはポリシーの名前を、[説明 (Description)] フィールドにはポリシーの説明を入力し、[アプリケーション認識型ルーティングポリシーの保存 (Save Application Aware Routing Policy)] をクリックします。Cisco SD-WAN Manager によってポリシーが作成されます。
9. サイトリストと VPN リストをポリシーに適用するには、[ポリシーアプリケーション (Policy Application)] を選択して、[アプリケーション認識型ルーティング (Application-Aware Routing)] を選択し、[新規サイトリストと VPN リスト (New Site Lists and VPN List)] をクリックします。
10. ポリシーに適用するサイトリストと VPN リストを選択します。
11. 必要に応じて、ポリシーにシーケンスルールを追加します。
12. [ポリシーの変更の保存 (Save Policy Changes)] をクリックします。

ACI サイトのマッピング

ACI サイトのマッピングは、Cisco APIC からのポリシーが適用されるコントローラデバイスを指定します。

開始する前に、[Cisco ACI との統合に関するガイドライン](#)セクションのガイドラインを確認してください。

デバイスをコントローラにアタッチするには、次の手順に従います。

1. Cisco SD-WAN Manager で、[管理 (Administration)] > [統合管理 (Integration Management)] を選択します。
2. 該当するサイトの行の右側にある [その他のアクション (More Actions)] アイコンをクリックし、[デバイスのアタッチ (Attach Devices)] を選択します。
3. 左側の [Available Devices] 列で、グループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[Select All] をクリックします。
4. 右向きの矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。



- (注) [選択されたデバイス (Selected Devices)] 列からデバイスを削除するには、その列でグループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[すべて選択 (Select All)] をクリックしてから左向きの矢印をクリックします。

5. [Attach] をクリックします。

ACI サイトのマッピング解除

ACI サイトのマッピングを解除すると、マッピングが解除されたデバイスに Cisco APIC ポリシーが適用されなくなります。

コントローラからデバイスを切り離すには、次の手順に従います。

1. Cisco SD-WAN Manager で、[管理 (Administration)] > [統合管理 (Integration Management)] を選択します。
[統合管理 (Integration Management)] ページが表示されます。
2. 該当するサイトの行の右側にある [その他のアクション (More Actions)] アイコンをクリックし、[デバイスの切断 (Detach Devices)] を選択します。
3. 左側の [Available Devices] 列で、グループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[Select All] をクリックします。
4. 右向きの矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。



- (注) [選択されたデバイス (Selected Devices)] 列からデバイスを削除するには、その列でグループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[すべて選択 (Select All)] をクリックしてから左向きの矢印をクリックします。

5. [Detach] をクリックします。

コントローラの削除

ACI のパートナーとしてのコントローラを削除する場合は、Cisco SD-WAN Manager で削除するのではなく、ACI を使用してその登録を削除することを推奨します。Cisco SD-WAN Manager から ACI パートナーを削除すると、ACI がパートナー用に作成したデータプレフィックスと VPN が自動的に削除されます。

開始する前に、ポリシー定義、および ACI が作成したデータプレフィックスリストと VPN リストから登録を削除し、これらのリストがどのポリシーからも参照されていないことを確認します。

1. Cisco SD-WAN Manager で、[管理 (Administration)] > [統合管理 (Integration Management)] を選択します。
2. コントローラにアタッチされているすべてのデバイスを切り離します。
手順については、「コントローラからのデバイスの切り離し」のセクションを参照してください。
3. 該当するサイトの行の右側にある [さらに多くのアクション (More Actions)] アイコンをクリックし、[コントローラの削除 (Delete Controller)] を選択します。



第 19 章

カスタムアプリケーション



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 44: 機能の履歴

機能名	リリース情報	説明
カスタムアプリケーション定義のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、カスタムアプリケーション定義のサポートが追加されます。

- [カスタムアプリケーションについて \(325 ページ\)](#)
- [Cisco SD-WAN Manager を使用した、カスタムアプリケーションの設定 \(329 ページ\)](#)
- [カスタムアプリケーションの確認 \(331 ページ\)](#)

カスタムアプリケーションについて

Cisco Network-Based Application Recognition (NBAR) とは、ネットワークトラフィックに対して SD-WAN Application Intelligence Engine (SAIE) フローを実行し、トラフィック特性に応じてネットワークアプリケーションを識別する、シスコのテクノロジーです。



(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。

ネットワーク アプリケーションにはそれぞれ特有のトラフィック特性があり、それはアプリケーションシグネチャと呼ばれています。シスコでは、こうしたアプリケーションシグネチャを他の情報とともにプロトコルとしてパッケージ化しています。パッケージ化されているのは、一般的に使用される多数のネットワーク アプリケーションをカバーした大規模なプロトコルのセット、プロトコルパックです。プロトコルパックは定期的に更新および配布しています。これらは、NBAR がネットワークのアプリケーショントラフィックを識別するために使用するネットワーク アプリケーションシグネチャのデータベースとなります。

ネットワーク アプリケーションという用語の定義は広く、次に挙げたものすべてを含めることもあれば、それ以外も含めることがあります。

- ソーシャルメディア Web サイト
- Voice over IP (VoIP) アプリケーション
- Cisco Webex などの音声とビデオのストリーミング
- クラウドストレージ用などのクラウドアプリケーション
- SaaS アプリケーション
- 組織専用のカスタム ネットワーク アプリケーション

アプリケーションの識別は、ネットワークトラフィックのモニタリング、アプリケーション認識型トラフィックポリシーの設定などに役立ちます。

ネットワーク アプリケーションシグネチャ、プロトコル、およびプロトコルパックと、NBAR によるそれらの使い方をまとめると、次のようになります。

- ネットワーク アプリケーションのトラフィックには、特定のアプリケーションに属するトラフィックを識別するために使用できる固有の特性がある。これらの特性は、アプリケーションシグネチャと呼ばれている。
- シスコでは、特定のネットワーク アプリケーションのシグネチャをプロトコルとしてパッケージ化している。
- シスコでは、一般的に使用されるインターネット アプリケーションをカバーした大規模なプロトコルセットをプロトコルパックとしてパッケージ化している。
- Cisco NBAR は、トラフィックに対して SAIE フローを実行して、トラフィックの送信元を識別するために必要な情報を収集し、プロトコルパックで提供されるようなプロトコルを使用して、その情報を特定のネットワーク アプリケーションと照合する。こうして NBAR は、ネットワーク内でトラフィックを生成するネットワーク アプリケーションを識別する。

Cisco Software-Defined Application Visibility and Control (SD-AVC) は、Cisco NBAR アプリケーション識別を使用して、ネットワーク内のアプリケーション使用状況に関する情報を提供します。

カスタムアプリケーション

プロトコルパックで提供される標準プロトコルに加えて、カスタムアプリケーションと呼ばれるプロトコルを定義してインターネットトラフィックを識別できます。組織にとって特に関心の高い、独自のネットワークアプリケーションのために行われます。カスタムアプリケーションは、プロトコルパックで提供されるプロトコルを強化します。

カスタムアプリケーションは他のプロトコルと同じように、設定時に使用できます。

- Cisco Catalyst SD-WAN ポリシー
- アプリケーション認識型ルーティング、TCP アクセラレーション、Quality of Service (QoS) など、アプリケーションの Quality of Experience (AppQoE) ポリシー



(注) 次の用語は、関連するテクノロジーのマニュアル内で、同じ意味で使われます：カスタムアプリケーション、カスタムプロトコル、ユーザー定義アプリケーション

Cisco Catalyst SD-WAN のカスタムアプリケーション

Cisco Software-Defined AVC (SD-AVC) は Cisco Application Visibility and Control (AVC) のコンポーネントです。一元化されたネットワークサービスとして機能し、ネットワーク内の特定の参加デバイスとともに動作します。Cisco Catalyst SD-WAN のコンポーネントとして含まれている Cisco SD-AVC の機能の 1 つは、カスタムアプリケーションを作成および管理することです。Cisco Catalyst SD-WAN は、SD-AVC REST API を介してこの Cisco SD-AVC 機能を使用して、Cisco Catalyst SD-WAN 内でカスタムアプリケーションを定義できるようにします。

Cisco Catalyst SD-WAN ユーザーとして、Cisco SD-WAN Manager を使用してカスタムアプリケーションを定義できます。その後、Cisco SD-AVC はカスタムアプリケーションをネットワーク内のデバイスにプッシュします。ネットワーク内のデバイスは、カスタムアプリケーションやその他のアプリケーションプロトコルを使用して、デバイスを通るトラフィックを分析します。

カスタムプロトコルを定義するプロセスには、ネットワークトラフィックを特定のネットワークアプリケーションからのものとして識別する基準を選択することが含まれます。基準には、サーバー名、IP アドレスなど、トラフィックの発信元ホストの特性を含めることができます。

プロトコルとカスタムアプリケーションの優先順位

Cisco NBAR で動作するプロトコルパックに含まれるプロトコルと同じトラフィックの一部に一致するカスタムアプリケーションを定義できます。トラフィックを照合する場合、カスタムアプリケーションは、プロトコルパックのプロトコルよりも優先されます。既存のネットワーク内に SD-AVC を展開する場合、ネットワークトポロジを変更する必要はありません。

カスタムアプリケーションに関する制約事項

- カスタムアプリケーションの最大数：1100
- L3/L4 ルールの最大数：20000
- サーバー名の最大数：50000
- サーバー名の場合、ワイルドカードとその後に続くピリオド (.) の最大インスタンス数：50000
例：*.cisco.com は www.cisco.com、developer.cisco.com とマッチします
- サーバー名の場合、サーバー名の一部としてのプレフィックスワイルドカードの最大インスタンス数: 256
例：*ample.com は www.example.com とマッチします
- 2つの異なるカスタムアプリケーションへの同じドメインのマッピングはサポートされていません。
- SD-AVC が最初のパケット分類を実行するには、DNS トラフィックとアプリケーショントラフィックが同じ VRF にある必要があります。
- CLI を使用したカスタムアプリケーションの作成は、Cisco Catalyst SD-WAN ポリシーではサポートされていません。
- カスタムアプリケーションのアクティブ化：
 - Cisco vManage リリース 20.5.1 以前のリリースを使用している場合：Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以前のリリースを使用しているデバイスの場合、カスタムアプリケーションのアクティブ化は次のようになります。
 - Cisco SD-WAN Manager で作成されたカスタムアプリケーションは、カスタムアプリケーションを使用するポリシーが適用されるまで、可視性機能（トラフィックのモニタリング）または制御機能（トラフィックポリシー）に対してアクティブ化されません。
 - Cisco vManage リリース 20.5.1 以降を使用する場合：Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降を使用しているデバイスの場合、カスタムアプリケーションのアクティブ化は次のようになります。
 - Cisco SD-WAN Manager で作成されたカスタムアプリケーションは、プロトコル検出カウンタや Flexible NetFlow (FNF) などのアプリケーション可視性機能（トラフィックのモニタリング）に対してのみすぐにアクティブ化されます。可視性機能のためにのみアクティブ化されている場合、カスタムアプリケーションがトラフィックポリシーに影響を及ぼすことはありません。
 - カスタムアプリケーションがポリシーで使用されている場合は、制御機能（トラフィックポリシー）に対してもアクティブ化されます。

Cisco SD-WAN Manager を使用した、カスタムアプリケーションの設定

前提条件

Cisco Catalyst SD-WAN のコンポーネントとして Cisco SD-AVC をインストールします。Cisco SD-WAN Manager で SD-AVC を有効にする方法については、「[Cisco SD-WAN デバイスで SD-AVC を有効にする方法に関する情報](#)」を参照してください。

次の手順を実行して、カスタムアプリケーションを設定してください。

1. Cisco SD-WAN Manager で、[設定 (Configuration)] > [ポリシー (Policies)] を選択します。
2. [Centralized Policy] を選択します。
3. [カスタムオプション (Custom Options)] をクリックし、[一元管理型ポリシー (Centralized Policy)] > [リスト (Lists)] の順に選択します。
4. [カスタムアプリケーション (Custom Applications)] をクリックし、[新規カスタムアプリケーション (New Custom Application)] をクリックします。
5. アプリケーションを定義するには、アプリケーション名を指定し、マッチ条件を入力します。マッチ条件には、提供される属性 (サーバー名、IP アドレスなど) を 1 つ以上含めることができます。すべてのフィールドにマッチ条件を入力する必要はありません。

マッチ論理は次のルールに沿っています。

- すべての L3/L4 属性の間には、論理 AND があります。トラフィックはすべての条件にマッチする必要があります。
- L3/L4 とサーバー名の間には、論理 OR があります。トラフィックは、サーバー名または L3/L4 属性のいずれかとマッチする必要があります。

フィールド	説明
アプリケーション	(必須) カスタムアプリケーションの名前を入力します。 最大長 : 32 文字

フィールド	説明
サーバー名	1 つ以上のサーバー名を、コンマで区切ります。 サーバー名の先頭にのみ、アスタリスクのワイルドカードマッチ文字 (*) を含めることができます。 次に例を示します。 *cisco.com, *.cisco.com (www.cisco.com、developer.cisco.com などにマッチ)
L3/L4 属性	
[IPアドレス (IP Address)]	1 つ以上の IPv4 アドレスをコンマで区切って入力します。 例： 10.0.1.1, 10.0.1.2 (注) サブネットプレフィックスの範囲は 24 ~ 32 です。
ポート	ポートまたはポート範囲をコンマで区切って入力します。 例： 30, 45-47
L4 Protocol	次のいずれかを選択します。 TCP、UDP、TCP-UDP

- [Add] をクリックします。カスタムアプリケーションのテーブルに新しいカスタムアプリケーションが表示されます。



- (注) 新しいカスタムアプリケーションの作成の進行状況を確認するには、[タスク (Tasks)] (クリップボードアイコン) をクリックします。パネルが開き、アクティブなプロセスと完了したプロセスが表示されます。

カスタムアプリケーション基準の例

基準	フィールドの設定方法
ドメイン名	[サーバー名 (Server Names)] : cisco.com
IP アドレスのセット、ポートのセット、および L4 プロトコル	[IP アドレス (IP Address)] : 10.0.1.1, 10.0.1.2 [ポート (Ports)] : 20, 25-37 [L4 プロトコル (L4 Protocol)] : TCP-UDP

基準	フィールドの設定方法
ポートと L4 プロトコルのセット	[ポート (Ports)] : 30, 45-47 [L4 プロトコル (L4 Protocol)] : TCP

カスタムアプリケーションの確認

Cisco SD-WAN Manager におけるカスタムアプリケーションの確認

カスタムアプリケーションを定義すると、[カスタムアプリケーションリスト (Custom Application List)] に表示されます。このリストには、使用可能なすべてのプロトコルとカスタムアプリケーションが表示されます。カスタムアプリケーションリストは、次の場所から入手できます。

[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)] > [カスタムアプリケーション (Custom Applications)]

デバイスのプロトコルとカスタムアプリケーションの検証

ルータにロードされているすべてのプロトコルおよびカスタムアプリケーションを表示するには、**show ip nbar protocol-id** コマンドを使用します。結果をフィルタリングするのに役立ちます。たとえば、名前に「custom」が含まれるすべてのプロトコルとカスタムアプリケーションを表示するには、次のように使用します。

```
vm5#show ip nbar protocol-id | include custom
custom_amazon          3899          PPKD LOCAL
custom_facebook        3284          PPKD LOCAL
```

詳細は「[show ip nbar protocol-id](#)」をご確認ください。



第 20 章

サービス挿入



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 45: 機能の履歴

機能名	リリース情報	説明
ワークフローを使用したサービス挿入	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN Manager リリース 20.13.1	この機能を使用すると、 ワークフローライブラリ からサービスチェーンを作成し、ポリシーのサービスチェーンアクションを設定できます。サービスチェーンは、トラフィックのフローに一連のサービスを挿入し、必要に応じてトラフィックに影響を与えるように設計できます。
信頼できるポスチャと信頼できないポスチャ	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN Manager リリース 20.14.1	この機能を使用すると、信頼できるトラフィックがサービスチェーン内の信頼できる高可用性ペアに流れるように設定できます。

- ・ [サービス挿入に関する情報 \(334 ページ\)](#)
- ・ [サービス挿入の制約事項 \(339 ページ\)](#)

- サービス挿入の使用例 (340 ページ)
- サービス挿入の設定 (340 ページ)
- データポリシーでのサービスチェーンアクションの設定 (341 ページ)
- サービスチェーンへのトラフィックステアリング (343 ページ)
- Path Preference (346 ページ)
- ユーザー VPN 間でのサービスチェーンの共有 (347 ページ)
- 送信トラフィックと受信トラフィックの別々のインターフェイス (347 ページ)
- 信頼できるトラフィックと信頼できないトラフィックのサービスチェーン (348 ページ)
- 2つのルータ間のサービスチェーン (348 ページ)
- サービスチェーンを介したトラフィックのフォールバックおよび制限動作の設定 (349 ページ)
- サービスチェーン内のサービスをルータに接続するためのインターフェイス (349 ページ)
- Software Defined Cloud Interconnect Bring Your Own Service を使用したサービスチェーン (350 ページ)
- CLI テンプレートをを使用したサービス挿入の設定 (351 ページ)

サービス挿入に関する情報

サービス挿入は、サービスチェーンとも呼ばれ、Cisco Catalyst SD-WAN オーバーレイファブリック内の特定のデータトラフィックのパスに1つ以上のネットワークサービスまたはセキュリティサービスを配置することを指します。これらのサービスは、トラフィックがルーティングされる一連のサービスであるサービスチェーンで定義されます。トラフィックは、データポリシーに設定したサービスチェーンアクションに従ってルーティングされます。

サービスチェーンは任意のデバイスに配置でき、フルメッシュ、ハブスポーク、Cisco Catalyst SD-WAN マルチリージョンファブリック (MRF) など、任意のトポロジで使用できます。

Cisco Catalyst SD-WAN サービスチェーンは柔軟性があり、完全に自動化されており、VPN ごとに展開できます。サービスチェーンには、次の主な機能が含まれます。

- サービスチェーンは、オーバーレイ、ローカル入力と出力、VPN間とVPN内、トランジット、ブランチ間、ブランチからインターネット、ブランチからクラウド、およびクラウド間のトラフィックに使用できます。
- チェーン内のすべてのサービスを通過するトラフィックの自動転送
- IPv4、IPv6、デュアルスタック、およびトンネル化のサービス接続メソッド
- 単一サービスのインスタンス間で設定可能な高可用性
- 単一サービスのインスタンス間での組み込みのロードバランシングにより、高可用性ペア間で等コストマルチパスルーティング (ECMP) をサポート
- 高度なサービストラッキング
- 複数のユーザー VPN (ユーザートラフィック VPN と異なる場合も同じ場合もあり) 間でのサービスチェーン共有

- 制御ポリシー、データポリシー、インターフェイスACL、およびサポートされている一致条件を使用したトラフィック ステアリング メソッド
- フォールバックおよび制限動作
- パスの設定と対称ルーティング
- サービストランスポートとの間のセキュリティサービス
- 信頼できる高可用性ペアと信頼できない高可用性ペアおよびトラフィックマーキング (Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降)
- 有用性に関する定期的なオンデマンド状態通知
- Cisco Catalyst SD-WAN Manager オーケストレーション：ワークフローベースのサービスチェーンとトラフィックポリシーの設定

サービス挿入機能

次の表に、Cisco Catalyst SD-WAN Manager リリース 20.13.1 の前後のリリースにおけるサービスチェーン機能の機能に関する情報を示します。

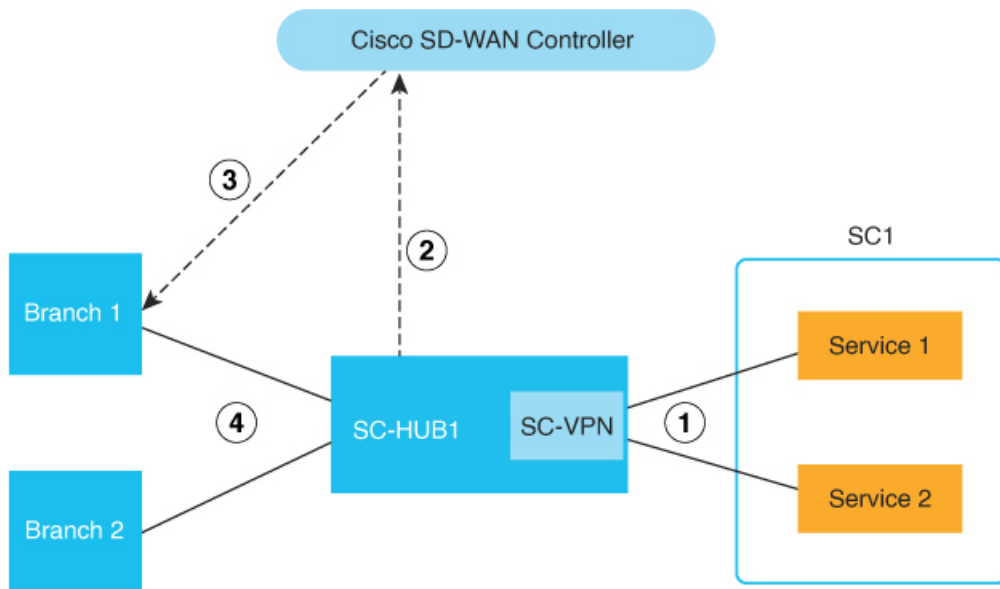
機能	Cisco Catalyst SD-WAN Manager リリース 20.13.1 より前のリ リース	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降のリリ ース
チェーン内の複数のサービス	ネイティブサポートなし	ネイティブサポート
トラフィックステアリング	制御ポリシー	制御ポリシー、データポリ シー、インターフェイス ACL
ポリシーバインディング	リモート	リモートおよびローカル
トラフィックのタイプ	IPv4	IPv4、IPv6、デュアルスタッ ク、トンネル
ロードバランシング	サービスエンドポイントとし て機能する 4 つの IP アドレス 間	すべてのトラフィックタイプ のアクティブバックアップペ アの 4 つのインスタンス間
高可用性	ロードバランシングによって 提供されるとおり	アクティブおよびバックアッ プペア
トラッキング	サービスインスタンスごとに 1 つの接続	抽象サービスへのすべての接 続
設定可能なトラッカープロ ブ	サポート対象外	すべてのトラッカーは個別に 設定可能
バックグラウンドでのトラッ キング	サポート対象外	対応

機能	Cisco Catalyst SD-WAN Manager リリース 20.13.1 より前のリ リース	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降のリリー ス
アフィニティ（サービスルー トとデータポリシー）	サポート対象外	対応
TLOC 設定	サポート対象	サポート対象
フォールバック、制限	サポート対象外	対応
トンネル接続サービス	サポート対象外	対応
共有サービス VPN	サポート対象外	対応
サービストランスポートとの 間	サポート対象外	対応
信頼できるポスチャと信頼で きないポスチャ	サポート対象外	Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降でサポー ト対象
定期的およびオンデマンドの 有用性	サポート対象外	対応
Cisco Catalyst SD-WAN Manager オーケストレーション	機能テンプレートを使用	ワークフローライブラリと設 定グループを使用（機能テン プレートはサポート対象外）
展開	オンプレミス	オンプレミス、クラウド、ミ ドルマイルのコロケーション
サービスインスタンスタイプ	物理	物理または仮想

サービス挿入の主要な概念と実装

次の図は、サービスチェーンの基本概念と、サービスチェーンの作成と実行に関連する一般的な手順を示しています。

図 19: サービス挿入の概念と手順



<p>1</p>	<p>サービスの起動：</p> <ul style="list-style-type: none"> • サービスを起動し、Cisco Catalyst SD-WAN ルータに接続します。 • Cisco Catalyst SD-WAN Manager を使用して目的のサービスを起動します。
<p>2</p>	<p>サービスチェーンの設定とアドバタイジング：</p> <ul style="list-style-type: none"> • ワークフローライブラリまたは CLI コマンドを使用して、SC1 として表示されるルータのサービスチェーンを設定します。 • 設定グループを使用して SC-HUB1 を設定します。ワークフローライブラリ設定により、入力に基づいて自動生成されたサービスチェーン設定が設定グループのサービス VPN 部分に追加されます。 • SC-HUB はサービスチェーンを Cisco SD-WAN コントローラにアドバタイズします。

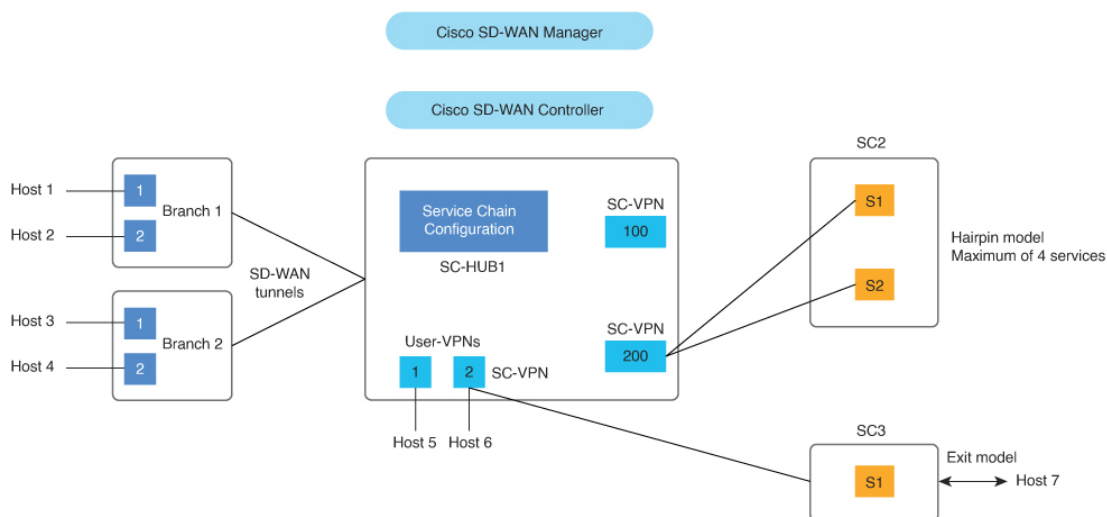
3	<p>サービスチェーンポリシー：</p> <ul style="list-style-type: none"> • トラフィックまたはルートを照合し、サービスチェーンアクションを実行します。 • トラフィックの発信元サイトにサービスチェーンポリシーを適用します。 • Cisco SD-WAN コントローラはサービスチェーンを解決し、ターゲットサイトにアドバタイズします。
4	<p>トラフィックステアリング：</p> <ul style="list-style-type: none"> • トラフィックは送信元 (B1) から SC-HUB にステアリングされます。 • サービスチェーンの最初のサービスが実行されます。 • 最初のサービスから SC-HUB にトラフィックが戻ります。 • サービスチェーンの 2 番目のサービスが実行されます。 • 2 番目のサービスから SC-HUB にトラフィックが戻ります。 • トラフィックは宛先 (B2) に転送されます。

次の図は、サービス挿入の主要な要素を示しています。この図で、SC-HUB1 はサービスチェーンが接続されているルータです。

ヘアピンモデルでは、トラフィックは SC-HUB1 によってサービスチェーン内のサービスに送信され、サービスは SC-HUB1 にトラフィックを返します。SC-HUB1 は、トラフィックをサービスチェーン内の次のサービスに転送し、トラフィックがサービスチェーン内の最後のサービスから戻る場合は宛先に転送します。

Exit モデルでは、トラフィックは SC-HUB1 によってサービスチェーン内のサービスに送信され、サービスはトラフィックを宛先に転送します。トラフィックは宛先からサービスに戻り、SC-HUB1 に戻される場合があります。

図 20: サービス挿入の主要な要素



サービス挿入の制約事項

- サービスチェーンには、最大4つのサービスタイプを含めることができます。各サービスタイプは、機能によってロードバランシングされる高可用性ペアとして、またはサードパーティのロードバランサの背後で、サービスの複数のインスタンスを持つことができます。
- サービスチェーン内のサービスは、単一のVPNの中に存在する必要があります。
- サービスチェーンでデュアルスタックサービスを使用している場合は、そのサービスチェーンのすべてのサービスにデュアルスタック高可用性ペアが必要です。
- 特定のデバイスインターフェイスは、特定のサービスチェーン内の複数のサービスには使用しないでください。
- 特定のインターフェイスは、各サービスチェーンで同じサービスタイプに使用される場合にのみ、異なるサービスチェーンで使用できます。
- サービスチェーン内のサービスのインターフェイスとトンネルはすべて、サービスチェーンが定義されているVPNの一部である必要があります。
- 特定のインターフェイスに複数のトラッカーを関連付けることはできません。たとえば、エンドポイントトラッカー tracker1 が GigabitEthernet1 に関連付けられている場合、別のトラッカーを GigabitEthernet1 に関連付けることはできません。

サービス挿入の使用例

- 安全性の低いネットワーク領域からのトラフィックが、改ざんされていないことを確認するためにファイアウォールを通過する必要がある場合、サービスチェーンを使用できます。
- それぞれが異なる機能または組織を表す複数の VPN で構成されるネットワークでサービスチェーンを使用すると、VPN間のトラフィックがファイアウォールを通過することができます。たとえばキャンパス内では、部門間のトラフィックはファイアウォールを通過し、部門内のトラフィックは直接ルーティングされる場合があります。
- サービスチェーンを使用すると、PCI DSS（クレジットカードデータ保護基準）などの適合規格を順守できます。PCI DSS では、PCI トラフィックが集中型データセンターまたは地域ハブのファイアウォールを通過する必要があります。

サービス挿入の設定

Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、ワークフローライブラリを使用してサービス挿入を設定できます。ワークフローライブラリから、新しいサービスチェーンを作成したり、既存のサービスチェーンを変更したりすることができます。サービスチェーンには、最大 4 つのサービスタイプを含めることができます。

ワークフローでは、次のような複数の手順を設定できます。

- サービスチェーンの名前と説明を設定する
- サービスチェーン内のサービスとチェーン内のサービスの順序を指定する
- サービスチェーンをルータに接続するとき使用される、チェーン内のサービスの接続パラメータを指定する
- サービスタイプごとに、VPNを指定し、ロードバランシング、高可用性、トラッキングなどのオプションを設定する

サービスチェーンを作成または変更するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューで **[Workflows] > [Workflow Library]** を選択します。
2. **[Define and Configure Service Chain]** をクリックします。
3. ワークフローのプロンプトに従います。

トラッカーを定義していることを確認します。トラッカーの設定は、ブラックホールを回避するために非常に重要です。トラッカーを定義すると、サービスチェーンがアップ状態であると判断され、使用されます。サービスチェーンファイアウォールの IP アドレスが ICMP ベースのトラッカーで使用されている場合は、ファイアウォールが適切なインターフェイスで ICMP を許可していることを確認します。

サービスチェーンがリターントラフィックを Cisco Catalyst SD-WAN ファブリックにルーティングできることを確認します。これを行うには、サービスチェーンと Cisco Catalyst SD-WAN ルータ（サービスチェーンハブ）の間でダイナミック ルーティング プロトコルを使用するか、スタティックルートを使用します。

サービスチェーンを適切な Cisco Catalyst SD-WAN SC-Hub ルータに接続します。サービスチェーンをブランチルータに接続する必要はありません。

サービス挿入を設定した後、必要に応じて次のアクションを実行します。

- データポリシーのサービスチェーンアクションを設定して、サービスチェーンを介してトラフィックをルーティングします。「[データポリシーでのサービスチェーンアクションの設定](#)」を参照してください。
- 制御ポリシー、データポリシー、またはインターフェイスアクセス制御リストを使用して、トラフィックをサービスチェーンに転送します。「[サービスチェーンへのトラフィックステアリング](#)」を参照してください。
- TLOC 設定またはアフィニティ設定を構成して、サービスチェーンへのトラフィックの優先パスを選択します。「[パスの設定](#)」を参照してください。
- 送信トラフィックと受信トラフィックに別々のインターフェイスを設定します。「[送信トラフィックと受信トラフィックの別々のインターフェイス](#)」を参照してください。
- 信頼できるトラフィックが信頼できる高可用性ペアに流れるように設定します。「[信頼できるトラフィックと信頼できないトラフィックのサービスチェーン](#)」を参照してください。
- サービスチェーンを通過するトラフィックのフォールバックまたは制限動作を設定します。「[サービスチェーンを介したトラフィックのフォールバックおよび制限動作の設定](#)」を参照してください。

データポリシーでのサービスチェーンアクションの設定

Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、データポリシーのサービスチェーンアクションを設定することで、サービスチェーンを介してトラフィックをルーティングできます。

1. Cisco SD-WAN Manager メニューから、**[Configuration] > [Policies]** の順に選択します。
2. **[Custom Options]** をクリックしてから、**[Centralized Policy]** で **[Traffic Policy]** をクリックします。
3. **[Traffic Data]** タブをクリックします。
4. **[Add Policy]** をクリックし、**[Create New]** をクリックします。
5. **[Sequence Type]** をクリックし、**[Add Data Policy]** ダイアログボックスから **[Service Chaining]** を選択します。

6. [Actions] タブをクリックします。
7. [Service] をクリックします。
8. 次の表で説明するフィールドを設定します。

表 46: サービスチェーンアクションのフィールド

フィールド	説明
Service: Type	サービスチェーンのサービスタイプを選択します。
Service: VPN	サービスチェーンがホストされているVPN。 範囲: 0 ~ 65530
Service: TLOC IP	サービスチェーン内のサービスを適用するためのトランスポートロケータ (TLOC) のIPアドレスを入力します。
色	TLOC の色を選択します。
カプセル化	TLOC のカプセル化タイプを選択します。
Service: TLOC List	ブランチトラフィックにサービスを適用するために使用する定義済みの TLOC リストを選択します。
Local	サービスチェーンがローカルでホストされている場合は、[Local] チェックボックスをオンにします。 このチェックボックスをオンにしない場合、サービスチェーンはリモートでホストされます。
制限 (Restrict)	サービスチェーンがダウンした場合にパケットがドロップされるようにするには、このオプションをオンにします。[Local] オプションを使用してこのポリシーを設定すると、パケットはローカルでドロップされます。[Remote] オプションを使用してこのポリシーを設定すると、パケットはリモートホストでドロップされます。 このオプションは、デフォルトではオフになっています (トラフィックはルーティングにフォールバックします)。

サービスチェーンへのトラフィックステアリング

制御ポリシー、データポリシー、またはインターフェイスアクセス制御リストを使用して、トラフィックをサービスチェーンに転送できます。

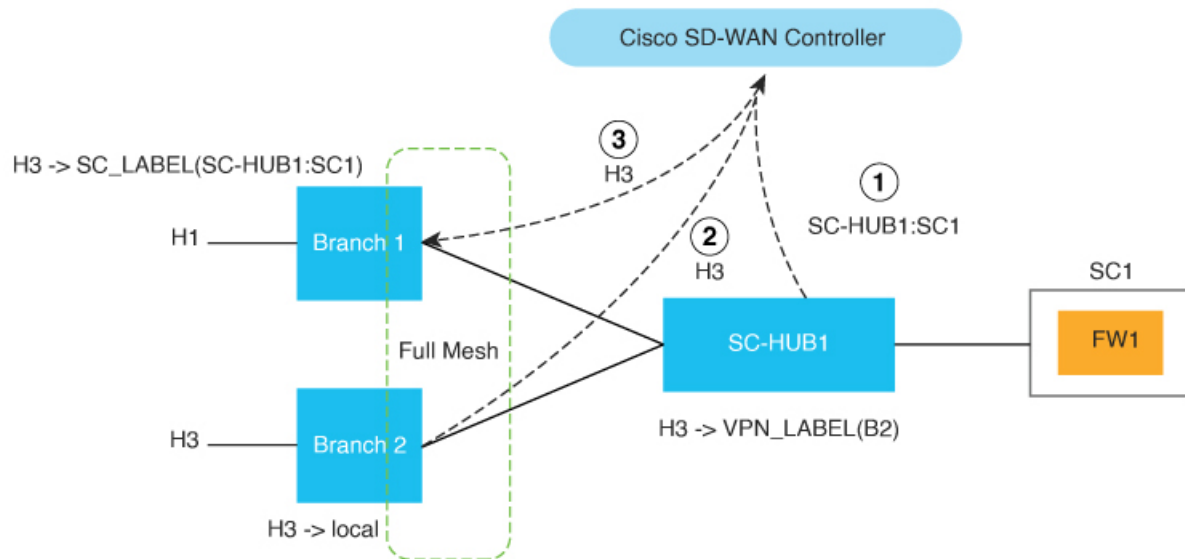
制御ポリシーを使用したトラフィックステアリング

制御ポリシーを使用してシスコのオーバーレイ管理ルート（vRoute と呼ばれる）を変更して、トラフィックを元の宛先ではなくサービスチェーンに転送できます。

次の図は、制御ポリシーを使用してトラフィックをサービスチェーンに転送する例を示しています。

この例では、ポリシーにより、H1（ホスト1）とH3（ホスト3）の間を流れるトラフィックにサービスチェーン1（SC1）が適用されます。このポリシーは、H1およびH3トラフィックルートのネクストホップとしてSC1を設定します。ポリシーが有効になる前は、トラフィックはB2（ブランチ2）からB1（ブランチ1）に流れます。ポリシーが有効になると、トラフィックはB2からSC-HUB1:SC1、それからB1に流れます。

図 21: 制御ポリシーを使用したトラフィックステアリング



1	SC-HUB1 は SC1 ルートをアドバタイズします。
2	B2 は H3 ルートを Cisco SD-WAN コントローラにアドバタイズします。

3	制御ポリシーにより、H3 ルートのネクストホップが SC1 にオーバーライドされ、Cisco SD-WAN コントローラは H3 ルートを B1 にアドバタイズします。
---	--

設定例：

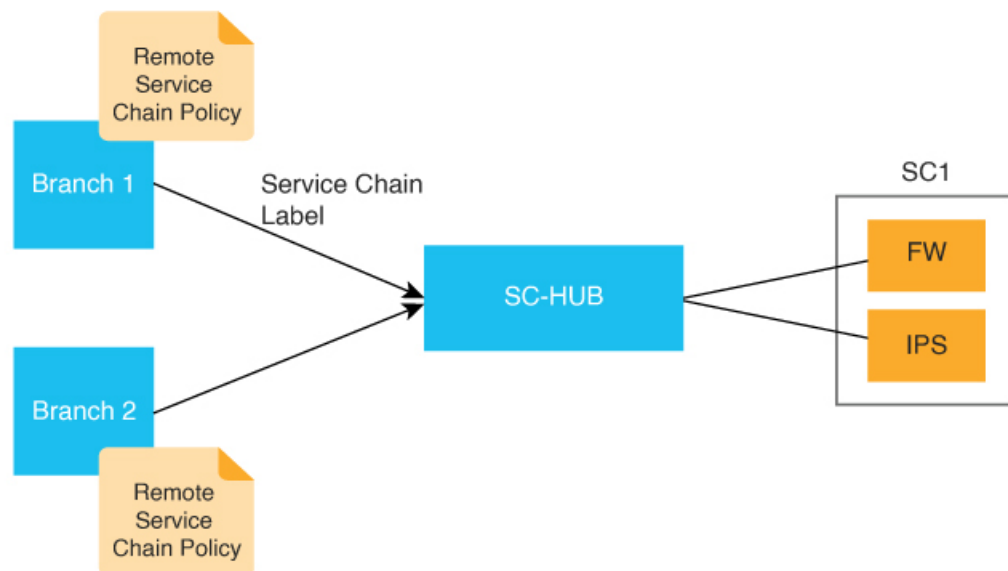
```
Control-policy name
  sequence number
  match route
  action accept
  set service-chain sc_name [tloc|tloc-list name] [vpn vpn]
  apply-policy site-list site_list control-policy name out
```

データポリシーを使用したトラフィックステアリング

データポリシーを使用してトラフィックを照合し、転送時に送信元 VPN のコンテキストで動作することができます。

次の図は、データポリシーを使用してリモートブランチでサービスチェーンインテントを指定する例を示しています。

図 22: リモートブランチでトラフィック サービス チェーン インテントが指定されたトラフィックステアリング



次に、リモートデバイスでトラフィックインテントが指定されている場合の、データポリシーを使用したトラフィックステアリングの設定例を示します。この例では、次のようになります。

- **match criteria** では、送信元と宛先の IP アドレスの組み合わせに一致するアプリケーションを指定します。
- **restrict|fallback** では、制限またはフォールバックを設定します。

- `tloc|tloc-list list` では、TLOC ランキングを使用してトラフィックパスの優先順位を指定します。

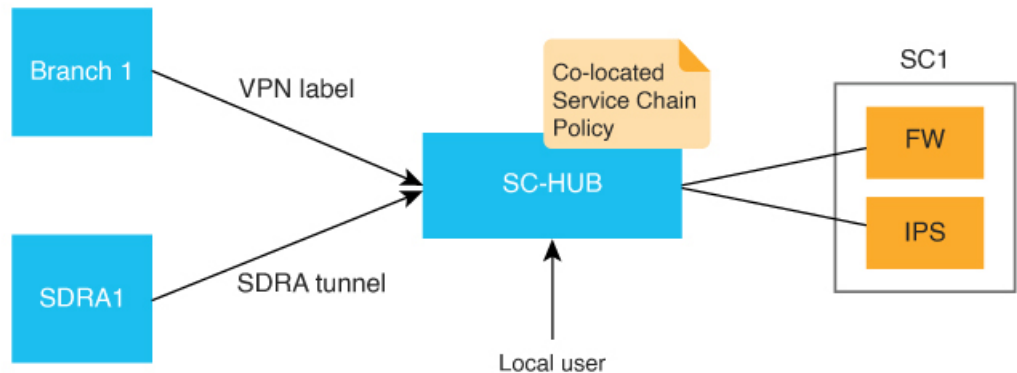


(注) `set attribute trust-posture` は、Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降で使用できます。

```
policy
data-policy name
vpn-list name
sequence 100
match criteria
action accept
set service-chain sc_name vpn vpn {restrict|fallback} [tloc|tloc-list list]
set attribute trust-posture {trusted | untrusted}
apply-policy site-list remote-sites data-policy name from-service
```

次の図は、データポリシーを使用して、サービスチェーンが接続されているデバイスでサービスチェーンインテントをローカルに指定する例を示しています。

図 23: ローカルデバイスでトラフィック サービス チェーンインテントが指定されたトラフィックステアリング



次に、ローカルデバイスでのサービスチェーンインテントの設定例を示します。この例で、`local` は、トラフィックをサービスチェーンにローカルに送信する必要があることを示します。

```
set service-chain SC1 [vpn vpn] local [restrict|fallback]
apply-policy site-list SC-HUB-sites data-policy policy {from-service|from-tunnel}|from-tunnel}
```

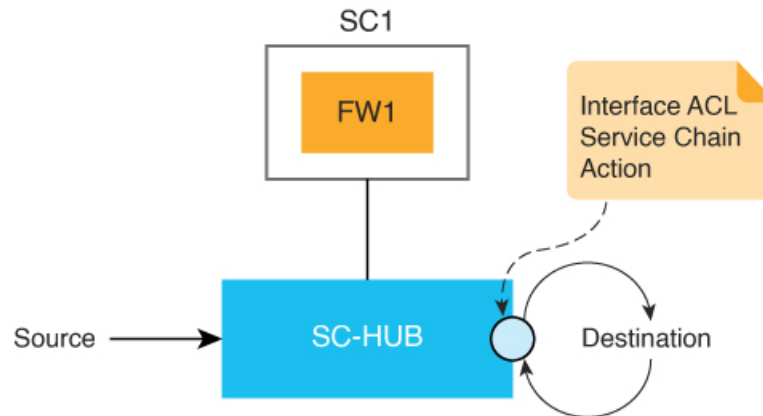
インターフェイスアクセス制御リストを使用したトラフィックステアリング

インターフェイスアクセス制御リスト（ACL）を使用して、指定したインターフェイスで着信または発信するトラフィックをサービスチェーン化できます。状況によっては、以前のルーティングルックアップまたはデータポリシーからトラフィック転送の決定を行う必要がある場合があります。

このアプローチは、インターフェイスからのすべてのトラフィックをサービスチェーン経由で送信する必要がある場合に役立ちます。

次の図は、ACLを使用して、サービスチェーンを介してトラフィックを転送する例を示しています。

図 24: ACL を使用したトラフィックステアリング



次に、ACL を使用したトラフィックステアリングの設定例を示します。

```
access-list list
  sequence number
  match criteria
  action accept
  set service-chain SC1 [vpn vpn] {restrict|fallback}
interface interface
  access-list list {in|out}
```

Path Preference

TLOC 設定またはアフィニティ設定を使用して、サービスチェーンへのトラフィックの優先パスを選択できます。

これを行うには、特定の TLOC 経由でのみトラフィックを転送するか、特定の TLOC を他の TLOC よりも優先するように TLOC リストを設定します。TLOC リストは、データポリシーまたは制御ポリシーのサービスチェーンアクションの一部として **tloc-list** で指定できます。

アフィニティ設定を構成するには、ブランチサイトで **affinity-group preference** を使用してブランチのアフィニティを設定し、サービスチェーンハブで **affinity-group** を使用して VPN のアフィニティを設定します。データポリシー **set service chain** アクションは、デフォルトでアフィニティに準拠しています。

次のコマンドを設定すると、データポリシーでのアフィニティの考慮を無効にすることができます。

data-policy-ignore-affinity-metric

TLOC 設定とアフィニティ設定の両方が設定されている場合、アフィニティ設定が最初に評価され、次に TLOC 設定が評価されます。

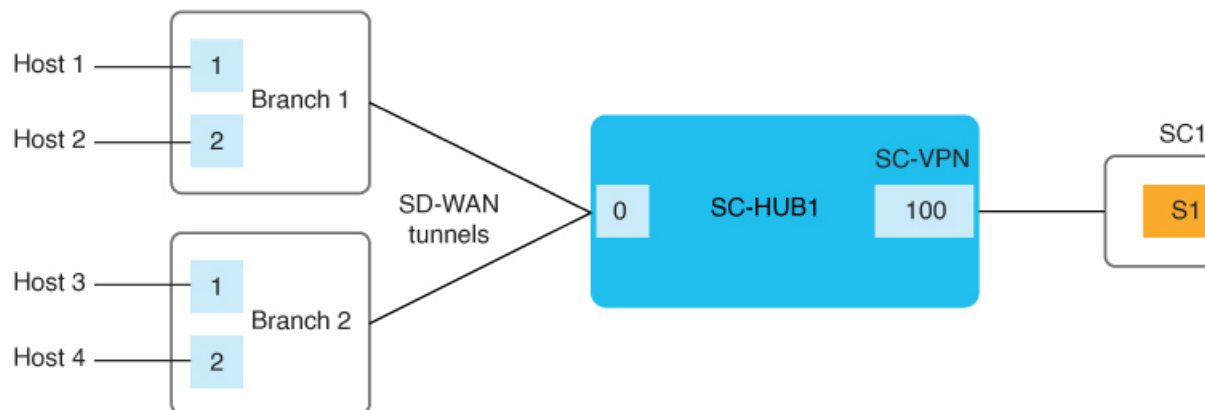
ユーザー VPN 間でのサービスチェーンの共有

サービスチェーン VPN は複数のユーザー VPN 間で共有でき、VPN 間のトラフィックは任意の VPN でサービスチェーン化できます。サービスチェーンの共有には、追加の設定は必要ありません。送信元と宛先の VPN が異なる場合は、送信元と宛先の VPN 間でルーティングが必要です。

次の図は、ユーザー VPN 間でのサービスチェーンの共有を示しています。この図では次のようになっています。

- VPN100 に接続されている SC1 (サービスチェーン 1) は、VPN1 (H1) および VPN2 (H4) のトラフィックで自動的に共有できます。
- VPN1 (H1) と VPN2 (H4) 間のトラフィックは、VPN1 または VPN2 あるいは共有サービスチェーン (VPN100) でサービスチェーン化できます。

図 25: VPN 間のサービスチェーン共有

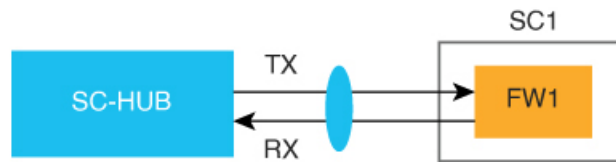


送信トラフィックと受信トラフィックの別々のインターフェイス

service コマンドを使用すると、サービスチェーンを介する送信トラフィックと受信トラフィックに別々のインターフェイスを設定できます。この場合、送信トラフィックと受信トラフィックは個別にトラッキングされます。詳細については、「[service](#)」を参照してください。

このアプローチを次の図に示します。

図 26: 送信トラフィックと受信トラフィックの別々のインターフェイス



信頼できるトラフィックと信頼できないトラフィックのサービスチェーン

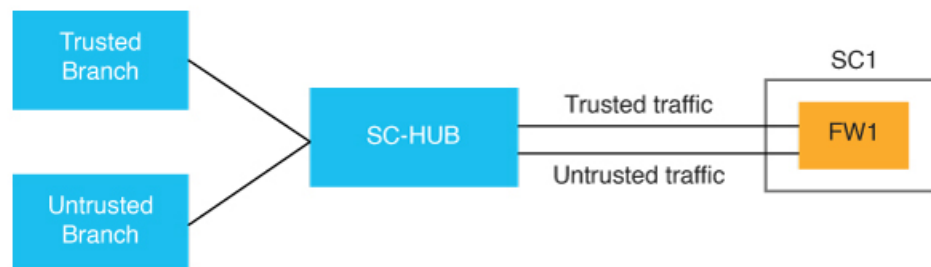
サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

信頼できるトラフィックが信頼できる高可用性ペアに流れるように設定できます。この場合、信頼できないトラフィックは信頼できない高可用性ペアに流れます。

データポリシーで **set attribute trust-posture untrusted action** を使用して、パケットを信頼できる (trusted) または信頼できない (untrusted) としてマークします。パケットのデフォルトの trust-posture は trusted です。

次の図は、信頼できるトラフィックと信頼できないトラフィックのフローを示しています。

図 27: 信頼できるトラフィックと信頼できないトラフィック



設定例：

```
service-chain SC1
  service netsvc1
    sequence 10
    service-transport-ha-pair 1
      attribute trust-posture {trusted|untrusted}
```

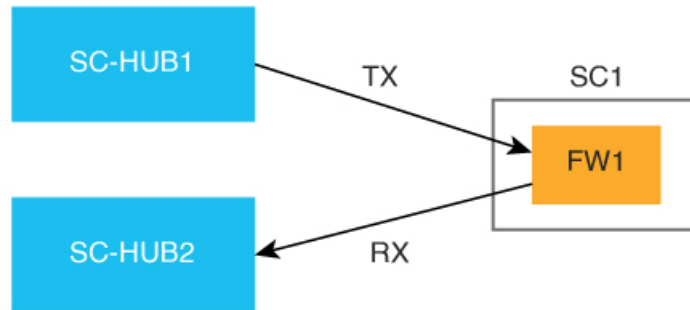
2つのルータ間のサービスチェーン

サービスチェーンにトラフィックを送信しているルータが、サービスチェーンからトラフィックを受信しているルータと異なる場合は、それぞれのデバイスで同じサービスチェーンを設定

します。サービスチェーンには1つのサービスのみを含めることができ、VPN内トラフィック専用です。

このアプローチを次の図に示します。

図 28: 2つのルータ間のサービスチェーン



サービスチェーンを介したトラフィックのフォールバックおよび制限動作の設定

サービスチェーンを通過するトラフィックのフォールバックまたは制限動作を設定できます。

set service-chain アクションで **fallback** が設定されていると、サービスチェーンがダウンした場合、またはポリシーで指定された TLOC が使用できない場合、トラフィックはルーティングにフォールバックします。

set service-chain アクションで **restrict** が設定されていると、サービスチェーンがダウンした場合、またはポリシーで指定された TLOC が使用できない場合、パケットはドロップされます。制限動作は、ファイアウォールなどのセキュリティサービスに適しています。

フォールバックおよび制限は、一元管理型データポリシー（リモートまたはコロケーション）およびインターフェイス ACL で指定できます。



(注) 出力 ACL を使用してトラフィックをサービスチェーンに転送する場合、制限動作が設定されていても、すべてのパケットは宛先に送信されます。これは、サービスチェーンの状態が検出される前に転送の決定が行われるためです。

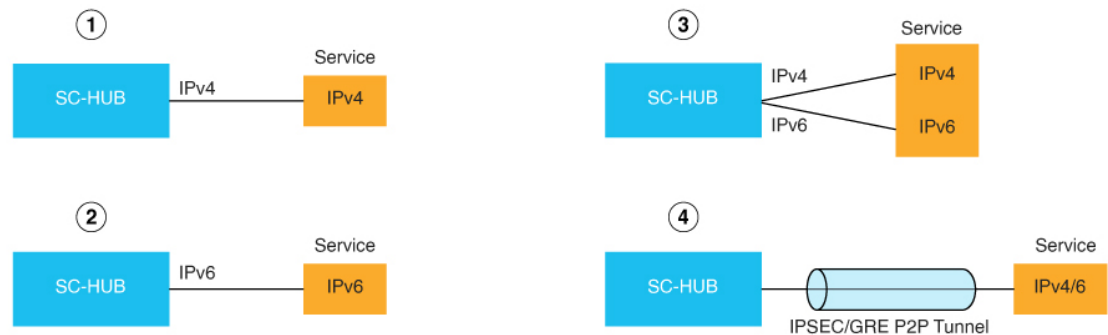
サービスチェーン内のサービスをルータに接続するためのインターフェイス

サービスチェーン内のサービスは、サービスチェーン VPN または SC-VPN と呼ばれる単一の VPN の中に存在する必要があります。

サービスチェーン内のサービスは、IPv4、IPv6、デュアルスタック、またはトンネルインターフェイスの任意の組み合わせを介して Cisco Catalyst SD-WAN ルータに接続できます。

次の図は、サービスチェーン内のサービスをルータに接続するためのインターフェイスを示しています。

図 29: サービスのルータへの接続



1	IPv4 接続
2	IPv6 接続
3	デュアルスタック接続
4	トンネル接続

Software Defined Cloud Interconnect Bring Your Own Service を使用したサービスチェーン

Software Defined Cloud Interconnect (SDCI) は、Megaport や Equinix などのネットワーク サービス プロバイダーを介して、ブランチサイトとクラウド間の接続を確立します。SDCI Bring Your Own Service (BYOS) 機能は、ミドルマイルネットワークに展開されている Cisco Catalyst 8000v Edge ソフトウェア (Catalyst 8000v) SDCI ゲートウェイにサービスチェーンを接続することで、サービス検査のための一元化された場所を確立します。BYOS を使用すると、外部サービスと SDCI インフラストラクチャのシームレスな統合が実現します。一元管理型データポリシーとも呼ばれる同じ場所に配置されたデータポリシーは、選択的なデータトラフィック検査のために、ミドルマイルネットワーク内のこれらのゲートウェイに適用されます。

このコンテキストでは、ブランチサイトがファーストマイルを表し、サービスプロバイダーがミドルマイルとして機能して、クラウドがラストマイルとして機能します。

SDCI の BYOS サービス検査では、次の状況でサービスチェーンを使用できます。

- C8000v SDCI ゲートウェイを使用して、ミドルマイルプロバイダーを介してブランチサイトをクラウドワークロードに接続する。

- Catalyst 8000v SDCI ゲートウェイを使用して、ミドルマイルプロバイダーを介してブランチサイトをインターコネクトする。
- Catalyst 8000v SDCI ゲートウェイを使用してミドルマイルプロバイダーによるインターネットクラウドトラフィック接続を促進する。

CLI テンプレートを使用したサービス挿入の設定

CLI テンプレートの使用の詳細については、[CLI アドオン機能テンプレート](#)および [CLI テンプレート](#)を参照してください。



- (注) デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

ここでは、サービス挿入の CLI 設定の例を示します。

1. サービスチェーンを作成します。

service-chain *chain-number*

2. サービスチェーンの説明を設定します。

service-chain-description *description*

3. サービスチェーン内のサービスを指定し、関連オプションを設定します。

service *service-type service-parameters*

4. (オプション、Cisco Catalyst SD-WAN Manager リリース 20.14.1 以降) サービスチェーン内のサービスの信頼ポスチャを設定します。

service *service-type service-transport-ha-pair value attribute trust-posture {trusted | untrusted}*

5. (オプション) すべての Cisco Catalyst SD-WAN Bidirectional Forwarding (BFD) セッションがダウンするように設定します。

service-chain-affect-bfd

6. サービスチェーン内のすべてのサービスをホストする VPN の名前を指定します。

service-chain-vrf *vrf*

7. (オプション、デフォルトで有効) サービスチェーン内のサービスのエンドポイントトラッキングを有効にします。

track-enable

8. (オプション、デフォルトで有効) サービスチェーンを有効にすることにより、デバイスでアクティブにします。

service-chain-enable



第 21 章

サービス チェーニング



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。



- (注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a および Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降、サービスチェーンの詳細については、「[サービス挿入](#)」を参照してください。

ネットワーク内のサービス

ファイアウォール、ロードバランサ、侵入検知と防御 (IDP) などのサービスは通常、仮想環境内で実行され、物理的に1か所に集中することもあれば、冗長性を確保するために数か所に分散されることもあります。サービスは、内部、クラウドベース、または外部のサブスクリプションの場合があります。ネットワークはこのようなサービスを介して、ネットワーク内の任意の場所からのトラフィックを再ルーティングできなければなりません。

お客様は、キャパシティ、冗長性、または単に最高水準の技術を選択するために、新しいサービスを要求に応じて社内に導入したり、社外にサブスクライブできるようにしたいと考えています。たとえば、ファイアウォールサイトがその容量を超えた場合、新しい場所で新しいファイアウォールサービスを生成できるなどです。この新しいファイアウォールをサポートするには、ポリシーベースで重み付けされた負荷分散を複数のファイアウォールに設定する必要があります。

サービスまたはサービスチェーンを介してトラフィックフローを再ルーティングする理由の一部を以下に示します。

- 安全性の低いネットワーク領域からのトラフィックフローは、改ざんされていないことを確認するために、ファイアウォールなどのサービスを通過するか、サービスチェーンを通過する必要があります。
- 複数のVPNで構成され、それぞれが機能または組織を代表するネットワークの場合、VPN間のトラフィックは、ファイアウォールなどのサービスまたはサービスチェーンを通過する必要があります。たとえばキャンパス内では、部門間のトラフィックはファイアウォールを通過し、部門内のトラフィックは直接ルーティングされる場合があります。
- 特定のトラフィックフローは、ロードバランサなどのサービスを通過する必要があります。

現在、トラフィックフローを再ルーティングする唯一の方法は、ポリシールートを使用して、送信元からサービスノード、サービスノードからその先のシステムにいたるまで、すべてのルーティングノードをプロビジョニングすることです。これは、オペレータが各ノードを手動で設定するか、オペレータに代わって各ノードの設定を実行するプロビジョニングツールを使用して行います。いずれの場合も、このプロセスのプロビジョニング、維持、およびトラブルシューティングは運用上複雑です。

Cisco Catalyst SD-WAN オーバーレイネットワークにおけるサービスのプロビジョニング

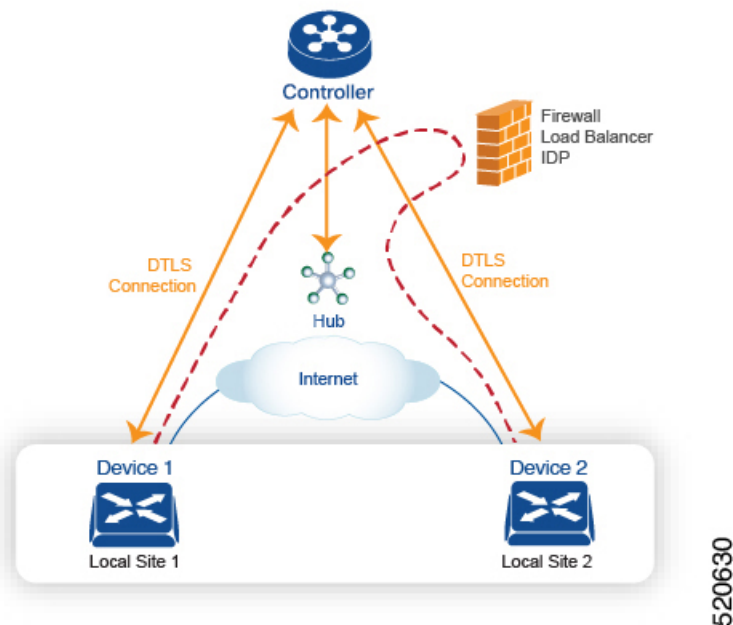
Cisco Catalyst SD-WAN ソリューションでは、ネットワークオペレータは、中央コントローラ、つまり Cisco SD-WAN コントローラ から、すべてのサービスチェーンを有効にしてオーケストレーションできます。設定やプロビジョニングはどのデバイスにも必要ありません。

Cisco Catalyst SD-WAN ネットワークにおけるサービスチェーンの一般的なフローは次のとおりです。

- デバイスは、ブランチまたはキャンパスで使用可能なサービス（ファイアウォール、IDS、IDP など）をドメイン内の Cisco SD-WAN コントローラ にアドバタイズします。複数のデバイスが同じサービスをアドバタイズできます。
- また、デバイスは OMP ルートと TLOC を Cisco SD-WAN コントローラ にアドバタイズします。
- サービスを必要とするトラフィックの場合、Cisco SD-WAN コントローラ のポリシーは、OMP ルートのネクストホップをサービス ランディングポイントに変更します。このようにして、トラフィックはサービスによって最初に処理されてから、最終的な宛先にルーティングされます。

次の図は、Cisco Catalyst SD-WAN ソリューションでサービスチェーンがどのように機能するかを示しています。図のネットワークでは、中央ハブルータが2つのブランチに接続され、それぞれにデバイスを備えています。標準的なネットワーク設計では、ブランチサイト1からブランチサイト2へのトラフィックはすべてハブルータを通過するような制御ポリシーが実装されています。ハブルータの背後には、ファイアウォールデバイスがあります。ここで、サイト1からサイト2へのすべてのトラフィックを、最初にファイアウォールで処理するとします。

サイト1のデバイスからのトラフィックは引き続きハブルータに流れますが、ハブルータはサイト2に直接送信する代わりに、トラフィックをファイアウォールデバイスにリダイレクトします。ファイアウォールが処理を完了すると、クリアされたすべてのトラフィックがハブに返され、このトラフィックはハブからサイト2のデバイスに渡されます。



サービスルート SAFI

ハブおよびローカルブランチデバイスは、サービスルートを使用して、ネットワークで使用可能なサービスをドメイン内の Cisco SD-WAN コントローラ にアドバタイズします。このサービスルートは、OMP/NLRI のサービスルート後続アドレスファミリー識別子 (SAFI) ビットを使用して OMP 経由で送信されます。Cisco SD-WAN コントローラ は RIB でサービスルートを維持し、これらのルートをデバイスには伝播しません。

各サービスルート SAFI には、次の属性があります。

- VPN ID (vpn-id) : サービスが属する VPN を識別します。
- サービス ID (svc-id) : サービスノードによってアドバタイズされているサービスを識別します。Cisco Catalyst SD-WAN ソフトウェアには、次の定義済みサービスがあります。
 - ファイアウォール用の FW (svc-id 1 にマッピング)
 - 侵入検知システム用の IDS (svc-id 2 にマッピング)
 - ID プロバイダー用の IDP (svc-id 3 にマッピング)
 - カスタムサービス用に予約されている netsvc1、netsvc2、netsvc3、netsvc4 (それぞれ svc-id 4、5、6、7 にマッピング)

- ラベル：サービスを通過する必要があるトラフィックの場合、Cisco SD-WAN コントローラはトラフィックをそのサービスに転送するために、OMP ルートのラベルをサービスラベルに置き換えます。
- 発信元 ID (originator-id)：サービスをアドバタイズしているサービスノードの IP アドレス。
- TLOC：サービスを「ホスティング」しているデバイスのトランスポート ロケーションアドレス。
- パス ID (path-id)：OMP パスの識別子。

サービスチェーンポリシー

サービスを介してトラフィックをルーティングするには、Cisco SD-WAN コントローラで制御ポリシーまたはデータポリシーをプロビジョニングします。一致基準が宛先プレフィックスまたはその属性のいずれかに基づいている場合は、制御ポリシーを使用します。一致基準にパケットまたはトラフィックフローの送信元アドレス、送信元ポート、DSCP 値、または宛先ポートが含まれている場合は、データポリシーを使用します。ポリシーは、CLI を使用して直接プロビジョニングすることも、Cisco SD-WAN Manager からプッシュすることもできます。

Cisco SD-WAN コントローラは、OMP ルート、TLOC ルート、サービスルートをルートテーブルに保持します。指定された OMP ルートは、TLOC とそれに関連付けられたラベルを伝送します。Cisco SD-WAN コントローラでは、TLOC とそれに関連付けられたラベルをサービスのラベルに変更するポリシーを適用できます。

サービスチェーンの正常性の追跡

Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降、Cisco Catalyst SD-WAN はネットワーク サービスを提供するデバイスを定期的にプローブして、それらが動作しているかどうかをテストします。サービスチェーン内のデバイスの可用性を追跡することは、ポリシーが使用できないサービスデバイスにトラフィックをルーティングする場合に発生し得る null ルートの回避に役立ちます。デフォルトでは、Cisco Catalyst SD-WAN はトラッキング結果をサービスログに書き込みますが、これは無効にすることができます。

制限事項

- トンネルインターフェイスを介したサービス挿入は、Cisco IOS XE Catalyst SD-WAN デバイスではサポートされていません。
- ローカルでホストされているサービスチェーンでの制御ポリシーベースのサービスチェーンアクションはサポートされていません。
- 同じデバイス上でのサービスチェーンと AppQoE の設定は、データポリシーまたは制御ポリシーベースのアクションに関係なくサポートされていません。
- [サービス チェーニングの設定 \(357 ページ\)](#)
- [サービスチェーン設定例 \(359 ページ\)](#)
- [サービスチェーンのモニター \(367 ページ\)](#)

サービス チェーニングの設定

Cisco Catalyst SD-WAN によって管理されるデバイスのサービスチェーンを設定するワークフローを次に示します。

1. サービスデバイスは、特定の VRF を介してアクセスされます。サービスデバイスの VRF に対応する VPN テンプレートで、サービスチェーンを設定し、サービスタイプとデバイスアドレスを指定します。デフォルトでは、トラッキング機能によって各サービスデバイスステータスの更新がサービスログに追加されます。VPN テンプレートでこれを無効にできます。
2. Cisco Catalyst SD-WAN によって管理されるデバイスのデバイステンプレートに VPN テンプレートをアタッチします。
3. デバイステンプレートをデバイスに適用します。

Cisco SD-WAN Manager を使用したサービスチェーンの設定

デバイスのサービスチェーンを設定します。

1. Cisco SD-WAN Manager で VPN テンプレートを作成します。
2. [サービス (Services)] をクリックします。
3. [サービス (Service)] セクションで [新規サービス (New Service)] をクリックし、以下を設定します。
 - **サービスタイプ (Service Type)** : サービスデバイスが提供するサービスのタイプを選択します。
 - **IP アドレス (IP Address)** : IP アドレスは唯一の有効なオプションです。
 - **IPv4 アドレス (IPv4 Address)** : デバイスのアドレスを 1 ~ 4 つ入力します。
 - **トラッキング (Tracking)** : サービスデバイスの定期的な正常性アップデートをシステムログに記録するかどうかを決定します。デフォルトは On です。



(注) サービスの最大数は 8 です。

4. [Add] をクリックします。設定されたサービスの表にサービスが表示されます。

Cisco IOS XE Catalyst SD-WAN デバイス における CLI での同等コマンド

次の表に、CLI によるサービスチェーンの設定が Cisco SD-WAN Manager の設定とどのように対応するかを示します。CLI 設定は、Cisco IOS XE Catalyst SD-WAN デバイス と Cisco vEdge デバイス で異なります。次の CLI の例は、Cisco IOS XE Catalyst SD-WAN デバイス の場合です。

CLI (Cisco IOS XE Catalyst SD-WAN デバイス)	Cisco SD-WAN Manager
service firewall vrf 10	Cisco SD-WAN Manager で、特定の VRF (この例では VRF 10) の VPN テンプレートにサービス挿入を設定します。 ドロップダウンリストから、サービスタイプを選択します (この例では firewall)。
no track-enable (注) デフォルト : enabled	VPN テンプレートの [サービス (サービス)] にサービスを追加する場合は、[トラッキング (Tracking)] で [オン (On)] または [オフ (Off)] を選択します。
ipv4 address 10.0.2.1 10.0.2.2	VRF テンプレートの [サービス (Service)] で、特定のサービスを提供するサービスデバイスの IP アドレスを 1 つ以上入力します。

CLI の例

```
sdwan
  service firewall vrf 10
  ipv4 address 10.0.2.1 10.0.2.2
commit
```

Cisco vEdge デバイス における CLI での同等コマンド

次の表に、CLI によるサービスチェーンの設定が Cisco SD-WAN Manager の設定とどのように対応するかを示します。CLI 設定は、Cisco IOS XE Catalyst SD-WAN デバイス と Cisco vEdge デバイス で異なります。次の CLI の例は、Cisco vEdge デバイス の場合です。

CLI (Cisco vEdge デバイス)	Cisco SD-WAN Manager
vpn 10	Cisco SD-WAN Manager で、VPN テンプレートにサービス挿入を設定します (この例では VPN 10)。 ドロップダウンリストから、サービスタイプを選択します (この例では firewall)。
service FW address 10.0.2.1	ドロップダウンリストから、サービスタイプを選択します (この例では firewall)。サービスデバイスのアドレスを 1 つ以上指定します。
no track-enable (注) デフォルト : enabled	VPN テンプレートの [サービス (サービス)] にサービスを追加する場合は、[トラッキング (Tracking)] で [オン (On)] または [オフ (Off)] を選択します。

CLI の例

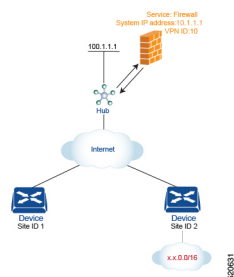
```
vpn 10
  service FW address 10.0.2.1
commit
```

サービスチェーン設定例

サービスチェーン制御ポリシーは、トラフィックが宛先に配信される前に、ネットワーク内のさまざまな場所に配置できるサービス側デバイスにデータトラフィックを転送するものです。サービスチェーンを機能させるには、Cisco SD-WAN コントローラで一元管理型制御ポリシーを設定し、そのデバイスと同じサイトに配置されたデバイス上でサービスデバイス自体を設定します。サービスが Cisco SD-WAN コントローラにアドバタイズされるようにするには、サービス側デバイスの IP アドレスをローカルで解決する必要があります。

このトピックでは、サービスチェーン設定の例を示します。

サービスを介したサイト間トラフィックのルーティング



簡単な例として、サービスを介して1つのサイトから別のサイトに移動するデータトラフィックのルーティングについて説明します。この例では、サイト1のデバイスからサイト2のデバイスに移動するすべてのトラフィックを、ハブ（システム IP アドレスは 100.1.1.1）の背後にあるファイアウォールサービスを介してルーティングします。簡単にするために、すべてのデバイスが同じ VPN 内にあることにします。

このシナリオの場合、次のように設定します。

- ハブルータで、ファイアウォールデバイスの IP アドレスを設定します。
- Cisco SD-WAN コントローラで、ファイアウォールサービスを介してサイト1からサイト2に向かうトラフィックをリダイレクトする制御ポリシーを設定します。
- Cisco SD-WAN コントローラで、サイト1に制御ポリシーを適用します。

設定手順を以下に示します。

1. ハブルータで、ファイアウォールデバイスの IP アドレスを指定して、ファイアウォールサービスをプロビジョニングします。この設定では、ハブルータの OMP が Cisco SD-WAN コントローラに1つのサービスルートをアドバタイズします。サービスルートには、ハブルータの TLOC や、サービスタイプをファイアウォールとして識別する svc-id-1 のサービスラベルなど、ファイアウォールの場所を識別する多数のプロパティが含まれています。（前述のように、ルートをアドバタイズする前に、デバイスでファイアウォールの IP アドレスがローカルで解決できるようにしておきます）。

```
sdwan
service firewall vrf 10
  ipv4 address 10.1.1.1
```

2. Cisco SD-WAN コントローラ で、ファイアウォールを介してサイト 1 からサイト 2 に移動するデータトラフィックをリダイレクトする制御ポリシーを設定します。次に、Cisco SD-WAN コントローラ で、このポリシーをサイト 1 に適用します。

```

policy
  lists
    site-list firewall-sites
      site-id 1
  control-policy firewall-service
    sequence 10
    match route
      site-id 2
    action accept
      set service FW vpn 10
    default-action accept
  apply-policy
    site-list firewall-sites control-policy firewall-service out

```

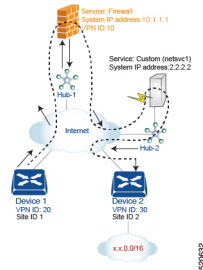
このポリシー設定によって次のことが行われます。

- **apply-policy** コマンドで参照され、このポリシーが適用されるすべてのサイトを列挙する **firewall-sites** というサイトリストを作成する。後でこのポリシーを拡張して、他のサイトからサイト 2 に向かうすべてのトラフィックも最初にこのファイアウォールを通過するようにする場合は、追加のサイト ID を **firewall-sites** サイトリストに追加するだけです。設定の **control-policy firewall-service** 部分を変更する必要はありません。
- **firewall-service** という名前の制御ポリシーを定義する。このポリシーには、1つのシーケンス要素と次の条件が備わっています。
 - サイト 2 宛てのルートを照合する。
 - マッチした場合は、ルートを受け入れ、VPN 10 にあるハブルータによって提供されるファイアウォールサービスにリダイレクトする。
 - マッチしないすべてのトラフィックを受け入れる。つまり、サイト 2 宛てではないすべてのトラフィックを受け入れる。
- **firewall-list** にリストされているサイト、つまりサイト 1 にポリシーを適用する。Cisco SD-WAN Validator は、アウトバウンド方向、つまりサイト 1 に再配布するルートにポリシーを適用します。これらのルートでは次の変更が起こります。
 - TLOC が、サイト 2 の TLOC からハブ 1 ルータの TLOC に変更される。これは、Cisco SD-WAN コントローラ がハブルータから受信したサービスルートを通じて学習した TLOC です。サイト 2 宛てのトラフィックがハブルータに送信される TLOC の変更が起こったからである。
 - ラベルが **svc-id-1** (ファイアウォールサービスを識別するもの) に変更される。このラベルにより、ハブルータはトラフィックをファイアウォールデバイスに転送する。

ハブルータはトラフィックを受信すると、ファイアウォールのシステム IP アドレス、10.1.1.1 に転送します。トラフィック処理を完了させたファイアウォールは、トラフィッ

クをハブルータに戻し、このルータがそのトラフィックを最終的な宛先であるサイト 2 に転送します。

ノードごとに1つのサービスを使用するサービスチェーンを介したVPN間トラフィックのルーティング



サービスチェーンを使用すると、トラフィックは宛先に到達する前に2つ以上のサービスを通り抜けます。ここでは、3番目のVPNにあるサービスを介して、あるVPNから別のVPNにトラフィックをルーティングする例を紹介합니다。サービスは、それぞれ異なるハブルータの背後にあります。具体的には、VPN 20 のデバイス 1 からデバイス 2 のVPN 30 のプレフィックス x.x.0.0/16 宛てのすべてのトラフィックが、まずハブ 1 の背後にあるファイアウォールを通過し、次にハブ 2 の背後にあるカスタムサービス netsvc1 を通過してから最終的な宛先に送信されるようにするとします。

このポリシーを機能させる必須条件を以下に示します。

- VPN 10、VPN 20、およびVPN 30 は、必ずインターネットなどのエクストラネットで接続する。
- VPN 10 は、必ずVPN 20 およびVPN 30 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。
- VPN 20 は、必ずVPN 30 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。
- VPN 30 は、必ずVPN 20 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。

このシナリオの場合、次の4つの設定を行います。

- ハブ 1 ルータでファイアウォールデバイスの IP アドレスを設定します。
- ハブ 2 ルータでカスタムのサービス側デバイスの IP アドレスを設定します。
- Cisco SD-WAN コントローラ で、ファイアウォールデバイスを介してサイト 1 からサイト 2 に向かうトラフィックをリダイレクトする制御ポリシーを設定します。
- Cisco SD-WAN コントローラ で、トラフィックをカスタムのサービス側デバイスにリダイレクトする 2 番目の制御ポリシーを設定します。

設定手順を以下に示します。

1. ハブ 1 でファイアウォールサービスを設定します。この設定では、ハブ 1 ルータの OMP が Cisco SD-WAN コントローラにサービスルートをアドバタイズします。サービスルートには、ハブルータの TLOC や、サービスタイプをファイアウォールとして識別する `svc-id-1` のサービスラベルなど、ファイアウォールの場所を識別する多数のプロパティが含まれています。

```
sdwan
service firewall vrf 10
  ipv4 address 10.1.1.1
```

2. ハブ 2 でカスタムサービス `netstvcl` を設定します。この設定では、ハブ 2 ルータの OMP が Cisco SD-WAN コントローラにサービスルートをアドバタイズします。サービスルートには、ハブ 2 の TLOC と、カスタムサービスを識別する `svc-id-4` のサービスラベルが含まれています。

```
sdwan
service netstvcl vrf 10
  ipv4 address 2.2.2.2
```

3. サービスチェーンの 1 番目のサービス（ファイアウォール）用に Cisco SD-WAN コントローラで制御ポリシーを作成し、デバイス 1 ルータの場所であるサイト 1 に適用します。

```
policy
  lists
    site-list firewall-custom-service-sites
      site-id 1
    control-policy firewall-service
      sequence 10
      match route
        vpn 30
        site-id 2
      action accept
        set service FW
      default-action accept
  apply-policy
    site-list firewall-custom-service-sites control-policy firewall-service out
```

このポリシー設定によって次のことが行われます。

- **apply-policy** コマンドで参照され、このポリシーが適用されるすべてのサイトを列挙する **firewall-custom-service-sites** というサイトリストを作成する。
- 1 つのシーケンス要素と次の条件を備えた **firewall-service** という名前の制御ポリシーを定義する。
 - VPN 30 とサイト 2 の両方を宛先とするルートを照合する。
 - マッチした場合は、ルートを受け入れ、ファイアウォールサービスへリダイレクトする。
 - マッチしない場合は、トラフィックを受け入れる。
- **firewall-custom-service-sites** サイトリスト、つまりサイト 1 内のサイトにポリシーを適用する。Cisco SD-WAN コントローラは、アウトバウンド方向、つまりサイト 1 に再配布するルートにこのポリシーを適用します。これらのルートでは次の変更が起こります。

- TLOC が、サイト 2 の TLOC からハブ 1 ルータに変更される。これは、Cisco SD-WAN コントローラ がハブから受信したサービスルートを通じて学習した TLOC です。サイト 2 宛てのトラフィックがハブ 1 ルータに送信される TLOC の変更が起こったからだ。
- ラベルが `svc-id-1` (ファイアウォールサービスを識別するもの) に変更される。このラベルにより、ハブ 1 ルータはトラフィックをファイアウォールデバイスに転送する。

ハブ 1 ルータはトラフィックを受信すると、ファイアウォールのシステム IP アドレス、10.1.1.1 に転送します。トラフィックの処理を完了させたファイアウォールは、トラフィックをハブ 1 ルータに返します。ハブ 1 ルータは、次の手順で定義されたポリシーにより、トラフィックをハブ 2 ルータに転送します。

4. サービスチェーン内の 2 番目のサービス (カスタムサービス) 用に Cisco SD-WAN コントローラ で制御ポリシーを作成し、ハブ 1 ルータのサイトに適用します。

```
policy
  site-list custom-service
    site-id 3
  control-policy netsvc1-service
    sequence 10
      match route
        vpn 30
        site-id 2
      action accept
        set service netsvc1
    default-action accept
apply-policy
  site-list custom-service control-policy netsvc1-service out
```

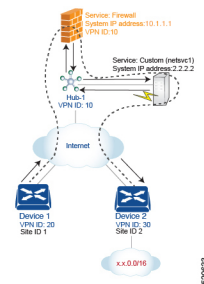
このポリシー設定によって次のことが行われます。

- **apply-policy** コマンドで参照され、このポリシーが適用されるすべてのサイトを列挙する **custom-service** というサイトリストを作成する。
- 1 つのシーケンス要素と次の条件を備えた **netsvc1-service** という名前の制御ポリシーを定義する。
 - VPN 30 とサイト 2 の両方を宛先とするルートを照合する。
 - マッチした場合は、ルートを受け入れ、カスタムサービスへリダイレクトする。
 - マッチしない場合は、トラフィックを受け入れる。
- **custom-service** リスト、つまりサイト 3 内のサイトにポリシーを適用する。Cisco SD-WAN コントローラ は、アウトバウンド方向、つまりサイト 3 に再配布するルートにこのポリシーを適用します。これらのルートでは次の変更が起こります。
 - TLOC が、サイト 2 の TLOC からハブ 2 ルータの TLOC に変更される。これは、Cisco SD-WAN コントローラ がハブ 2 ルータから受信したサービスルートを通じて学習した TLOC です。サイト 2 宛てのトラフィックがハブ 2 ルータに送信される TLOC の変更が起こったからです。

- ラベルが **svc-id-4** (ファイアウォールサービスを識別するもの) に変更される。このラベルにより、ハブ 2 は、カスタムサービスをホストしているデバイスにトラフィックを転送します。

ハブ 2 ルータはトラフィックを受信すると、カスタムサービスをホストしているデバイスのシステム IP アドレス、2.2.2.2 に転送します。トラフィックは処理された後、ハブ 2 ルータに戻され、最終的な宛先であるサイト 2 に転送されます。

ノードごとに複数のサービスがあるサービスチェーンを介したVPN間トラフィックのルーティング



サービスチェーンに同じノードに接続されているサービスが複数ある場合、つまり両方のサービスが同じデバイスの背後にある場合は、制御ポリシーとデータポリシーを組み合わせることで目的のサービスチェーンを作成します。この例は、前のセクションの例に似ていますが、単一のハブルータの背後にファイアウォールとカスタムサービス (netvc-1) がある点が異なります。ここでは、VPN 20 のデバイス 1 から VPN 30 のデバイス 2 のプレフィックス x.x.0.0/16 宛てのすべてのデータトラフィックが、最初にハブ 1 のファイアウォールを通過し、その後同じハブ 1 にあるカスタムサービス netvc1 を通過してから最終的な宛先に送信されるようにします。

このポリシーを機能させる必須条件を以下に示します。

- VPN 10、VPN 20、および VPN 30 は、必ずインターネットなどのエクストラネットで接続する。
- VPN 10 は、必ず VPN 20 および VPN 30 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。
- VPN 20 は、必ず VPN 30 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。
- VPN 30 は、必ず VPN 20 からルートをインポートする。ルートは必要に応じて選択的にインポート可能。

このシナリオの場合、次のように設定します。

- ハブルータで、ファイアウォールとカスタムサービスを設定します。
- Cisco SD-WAN コントローラで、ファイアウォールを介してサイト 1 からサイト 2 に向かうデータトラフィックをリダイレクトする制御ポリシーを設定します。

- Cisco SD-WAN コントローラ で、データトラフィックをカスタムサービスにリダイレクトするデータポリシーを設定します。

設定手順を以下に示します。

1. ハブルータで、ファイアウォールとカスタムサービスを設定します。

```
sdwan
service firewall vrf 10
  ipv4 address 10.1.1.1
service netsvc1 vrf 10
  ipv4 address 2.2.2.2
```

この設定では、ハブルータの OMP が 2 つのサービスルートで Cisco SD-WAN コントローラにアダプタイズします。1 つはファイアウォール用、もう 1 つはカスタムサービス netsvc1 用です。どちらのサービスルートにも、ハブ 1 ルータの TLOC と、サービスのタイプを識別するサービスラベルが含まれています。ファイアウォールサービスの場合のサービスラベルは svc-id-1 で、カスタムサービスの場合は svc-id-4 となります。

2. Cisco SD-WAN コントローラ で、VPN 30 (サイト 2) 宛てのトラフィックをハブ 1 (サイト 3) に接続されているファイアウォールサービスに再ルーティングするように制御ポリシーコントローラを設定し、このポリシーを次のようにサイト 1 に適用します。

```
policy
  lists
    site-list device-1
    site-id 1
  control-policy firewall-service
  sequence 10
  match route
    vpn 30
  action accept
  set service FW
apply-policy
  site-list device-1 control-policy firewall-service out
```

3. Cisco SD-WAN コントローラ で、ファイアウォールデバイスから受信したデータトラフィックをカスタムサービス netsvc1 にリダイレクトまたはチェーンするデータポリシーを設定します。次に、このポリシーをハブ 1 に適用します。このデータポリシーは、ネットワーク x.x.0.0/16 の宛先に向かうパケットを IP アドレス 2.2.2.2 というカスタムサービスをホストしているデバイスのシステム IP アドレスにルーティングするためのものです。

```
policy
  lists
    site-list device-2
    site-id 2
    site-list Hub-1
    site-id 3
    prefix-list svc-chain
    ip-prefix x.x.0.0/16
    vpn-list vpn-10
    vpn 10
  data-policy netsvc1-policy
  vpn-list vpn-10
  sequence 1
  match
    ip-destination x.x.0.0/16
  action accept
  set next-hop 2.2.2.2
```

```

apply-policy
  site-list Hub-1 data-policy netsvc1-policy from-service

```

サービスチェーンを使用したアクティブシナリオまたはバックアップシナリオ

set service アクションを使用して、サービスチェーン用にアクティブまたはバックアップ制御ポリシーを設定する場合に、使用可能なパスの合計数（アクティブパスとスタンバイパスの合計）が設定された **send-path-limit** を超えるようなら、ルートへの直接的な基本設定はしないでください。基本設定を行う場合は、**set tloc-list** アクションと **set service** アクションを併用するようにしてください。そうしないと、アクティブパスのみ、またはバックアップパスのみが特定のスポークルータにアドバタイズされることがあります。

たとえば、Cisco SD-WAN コントローラ OMP テーブルには、8つのアクティブパスとバックアップパスがあります。ベストパスの計算に基づいて、パスは次の順序でソートされます。

backup1、backup2、backup3、backup4、active1、active2、active3、active4

send-path-limit 4 が設定されている場合、1番目のポリシーを適用すると、4つのバックアップパスのみが送信されます。2番目のポリシーを適用すると、2つのアクティブパスと2つのバックアップパスが送信されます。

send-path-limit がアクティブパスとバックアップパスの合計数よりも小さい場合に障害が発生しやすいポリシーの例を以下に示します。

```

control-policy SET_SERVICE_ACTIVE-BACKUP
  sequence 10
    match route
      prefix-list _AnyIpv4PrefixList
      site-list HUBS_PRIMARY
      tloc-list INTERNET_TLOCS
    !
    action accept
      set
        preference 200
        service FW vpn 10
      !
    !
  !
  sequence 20
    match route
      prefix-list _AnyIpv4PrefixList
      site-list HUBS_SECONDARY
      tloc-list INTERNET_TLOCS
    !
    action accept
      set
        preference 100
        service FW vpn 10
      !
    !
  !
  default-action accept
  !
  !

```

ポリシー同じですが、推奨事項に従って修正した例を以下に示します。

```

policy
lists

```

```
tloc-list HUBS_PRIMARY_INTERNET_TLOCS
 tloc 10.0.0.0 color biz-internet encaps ipsec preference 200
 tloc 10.0.0.1 color biz-internet encaps ipsec preference 200
 !
tloc-list HUBS_SECONDARY_INTERNET_TLOCS
 tloc 10.255.255.254 color biz-internet encaps ipsec preference 100
 tloc 10.255.255.255 color biz-internet encaps ipsec preference 100
 !
!
control-policy SET_SERVICE_ACTIVE-BACKUP_FIXED
 sequence 10
  match route
   prefix-list _AnyIpv4PrefixList
   site-list HUBS_PRIMARY
   tloc-list INTERNET_TLOCS
  !
  action accept
   set
    service FW vpn 10 tloc-list HUBS_PRIMARY_INTERNET_TLOCS
  !
 !
 !
 sequence 20
  match route
   prefix-list _AnyIpv4PrefixList
   site-list HUBS_SECONDARY
   tloc-list INTERNET_TLOCS
  !
  action accept
   set
    service FW vpn 10 tloc-list HUBS_SECONDARY_INTERNET_TLOCS
  !
 !
 !
 default-action accept
 !
 !
```

サービスチェーンのモニター

ハブアンドスポークデバイスで、サービスチェーンのさまざまな側面をモニタリングできます。



(注) サービスデバイスをサービスチェーンの一部として動作するように設定することを、サービスの挿入と呼びます。

• ハブデバイスで、設定されたサービスを表示します。

• Cisco SD-WAN Manager のメニューから、次の手順を実行します。

[リアルタイムモニタリング (Real Time monitoring)] ページで、設定されたサービスを表示します ([モニター (Monitor)] > [デバイス (Devices)] > [ハブデバイス (hub-device)] > [リアルタイム (Real Time)])。[デバイスオプション (Device Options)] で、[OMPサービス (OMP Services)] を選択します。

Cisco vManage リリース 20.6.x 以前 : [リアルタイムモニタリング (Real Time monitoring)] ページで、設定されたサービスを表示します ([モニター (Monitor)] > [ネットワーク (Network)] > [ハブデバイス (hub-device)] > [リアルタイム (Real Time)])。 [デバイスオプション (Device Options)] で、 [OMPサービス (OMP Services)] を選択します。

- スポークデバイスで、サービスチェーンパスの詳細を表示します。

- **Cisco SD-WAN Manager** を使用 :

[トレースルート (Traceroute)] ページでサービスチェーンパスを表示します ([モニター (Monitor)] > [デバイス (Devices)] > [スポークデバイス (spoke-device)] > [トラブルシューティング (Troubleshooting)] > [接続 (Connectivity)] > [トレースルート (Trace Route)])。 目的のパスの宛先 IP、VPN、および送信元インターフェイスを入力します。

Cisco vManage リリース 20.6.x 以前 : [トレースルート (Traceroute)] ページでサービスチェーンパスを表示します ([モニター (Monitor)] > [ネットワーク (Network)] > [スポークデバイス (spoke-device)] > [トラブルシューティング (Troubleshooting)] > [接続 (Connectivity)] > [トレースルート (Trace Route)])。 目的のパスの宛先 IP、VPN、および送信元インターフェイスを入力します。

- **CLI** を使用 :

traceroute コマンドを使用します。詳細については、 [『Cisco Catalyst SD-WAN Command Reference』](#) を参照してください。

例 : 2つのスポークデバイス間のサービスチェーンパスを表示する

次の例は、Cisco SD-WAN Manager または CLI を使用して、2つのスポーク間にサービスチェーンを追加する前と後に、スポーク間のパスを表示する方法を示しています。

わかりやすくするために、この例では、2つのスポークデバイス、ハブデバイス、およびファイアウォールサービスを提供するサービスデバイスのシナリオを示し、ファイアウォールサービスチェーンを設定する方法を示します。

シナリオの各デバイスの詳細は次のとおりです。

デバイス	アドレス
ハブ、インターフェイス ge0/4 経由	10.20.24.15
スポーク 1	10.0.3.1
スポーク 2	10.0.4.1
サービスデバイス (ファイアウォールサービス)	10.20.24.17

3つのデバイスの設定 :

```
Hub
====
vm5# show running-config vpn 1
vpn 1
  name ospf_and_bgp_configs
  service FW
  address 10.20.24.17
  exit
  router
    ospf
      router-id 10.100.0.1
      timers spf 200 1000 10000
      redistribute static
      redistribute omp
      area 0
        interface ge0/4
          exit
        exit
      !
    !
  interface ge0/4
    ip address 10.20.24.15/24
    no shutdown
  !
  interface ge0/5
    ip address 10.30.24.15/24
    no shutdown
  !
  !
```

```
Spoke 1
=====
vpn 1
  name ospf_and_bgp_configs
  interface ge0/1
    ip address 10.0.3.1/24
    no shutdown
  !
  !
```

```
Spoke2
=====
vpn 1
  interface ge0/1
    ip address 10.0.4.1/24
    no shutdown
  !
  !
```

1. サービス挿入なし：

この時点ではサービス挿入ポリシーは設定されていないため、スポーク 1 で **traceroute** を実行してスポーク 2 (10.0.4.1) へのパスの詳細を表示すると、スポーク 2 への単純なパスが表示されます。

→ スポーク 2 (10.0.4.1)

```
vm4# traceroute vpn 1 10.0.4.1
Traceroute 10.0.4.1 in VPN 1
traceroute to 10.0.4.1 (10.0.4.1), 30 hops max, 60 byte packets
 1 10.0.4.1 (10.0.4.1) 7.447 ms 8.097 ms 8.127 ms
```

同様に、Cisco SD-WAN Manager で [トレースルート (Traceroute)] ページを表示すると、スポーク 1 からスポーク 2 への単純なパスが表示されます。

2. サービス挿入あり :

次の Cisco SD-WAN コントローラ のポリシーは、前述のファイアウォール サービス デバイスを使用して、ファイアウォールサービスのサービス挿入を設定します。

```
vm9# show running-config policy
policy
  lists
    site-list firewall-sites
      site-id 400
    !
  !
  control-policy firewall-services
    sequence 10
    match route
      site-id 600
    !
    action accept
    set
      service FW vpn 1
    !
  !
  !
  default-action accept
  !
!
vm9# show running-config apply-policy
apply-policy
  site-list firewall-sites
  control-policy firewall-services out
  !
!
```

サービス挿入を設定した後、スポーク 1 (10.0.3.1) で **traceroute** を実行してスポーク 2 (10.0.4.1) へのパスの詳細を表示すると、次のパスが表示されます。

→ ハブ (10.20.24.15) → ファイアウォール サービス デバイス (10.20.24.17) → ハブ (10.20.24.15) → スポーク 2 (10.0.4.1)

```
Traceroute -m 15 -w 1 -s 10.0.3.1 10.0.4.1 in VPN 1
traceroute to 10.0.4.1 (10.0.4.1), 15 hops max, 60 byte packets
 1 10.20.24.15 (10.20.24.15) 2.187 ms 2.175 ms 2.240 ms
 2 10.20.24.17 (10.20.24.17) 2.244 ms 2.868 ms 2.873 ms
 3 10.20.24.15 (10.20.24.15) 2.959 ms 4.910 ms 4.996 ms
 4 10.0.4.1 (10.0.4.1) 5.045 ms 5.213 ms 5.247 ms
```

同様に、Cisco SD-WAN Manager で [トレースルート (Traceroute)] ページを表示すると、ハブおよびファイアウォール サービス デバイスを経由するスポーク 1 からスポーク 2 へのパスの各手順が表示されます。



第 22 章

合法的傍受



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

合法的傍受機能は、法執行機関（LEA）の要件を満たす際にサービスプロバイダーをサポートし、管轄または行政命令によって承認されている電子サーベイランスを提供します。サーベイランスは、エッジルータを通過する Voice over Internet Protocol (VoIP) またはデータトラフィックを傍受するため、盗聴を利用して実行されます。LEA は、ターゲットのサービスプロバイダーに盗聴を要求します。サービスプロバイダーには、IP セッションを使用してその個人が送受信するデータ通信を傍受する責任があります。ユーザーセッションは、送信元および宛先 IP アドレス、または VRF 名のいずれかを使用してタップされ、ルータ内で vrf-tableid 値に変換されます。

表 47: 機能の履歴

機能名	リリース情報	説明
合法的傍受メッセージの暗号化	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	この機能は、静的トンネル情報を使用して、Cisco IOS XE Catalyst SD-WAN デバイス とメディアデバイス間の合法的傍受メッセージを暗号化します。

- [合法的傍受に関する情報 \(372 ページ\)](#)
- [合法的傍受の前提条件 \(375 ページ\)](#)
- [Cisco Catalyst SD-WAN Manager を使用した合法的傍受のインストール \(376 ページ\)](#)

- [合法的傍受 MIB \(377 ページ\)](#)
- [信頼できるホストへのアクセス制限 \(暗号化なし\) \(378 ページ\)](#)
- [信頼できるメディエーションデバイスの制限 \(378 ページ\)](#)
- [合法的傍受の設定 \(379 ページ\)](#)
- [CLI を使用した、合法的傍受の設定 \(379 ページ\)](#)
- [合法的傍受トラフィックの暗号化 \(380 ページ\)](#)
- [メディア デバイス ゲートウェイとの静的トンネルの確認 \(382 ページ\)](#)

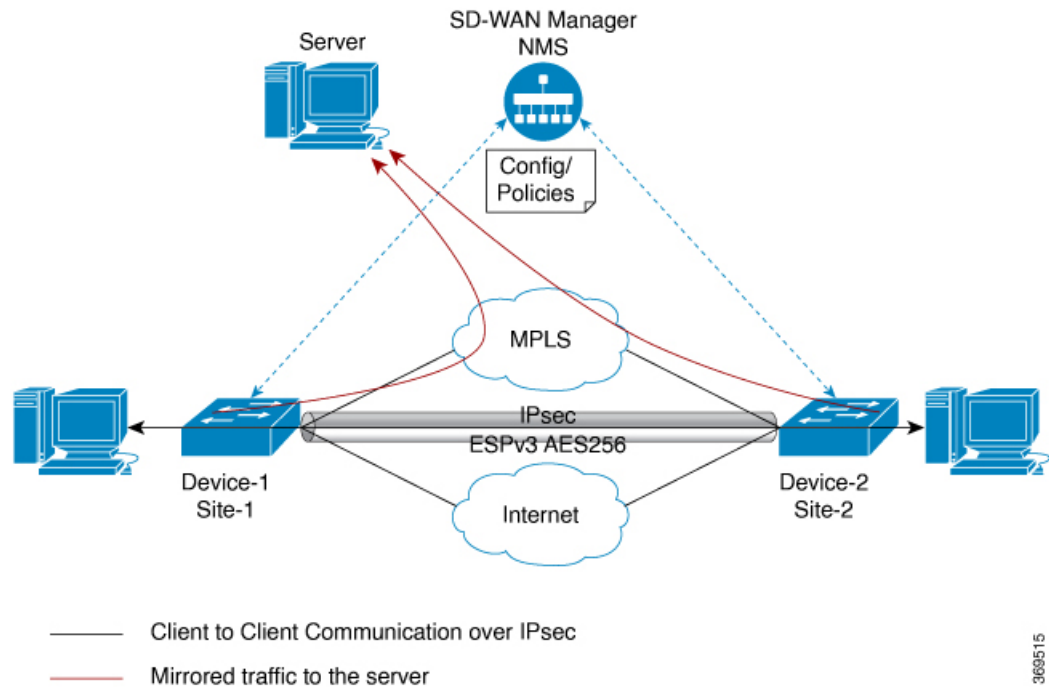
合法的傍受に関する情報

合法的傍受は、裁判所または行政機関による命令を根拠として、司法当局 (LEA) が個人 (ターゲット) に対して電子監視を実施できるようにするプロセスです。合法的傍受プロセスを容易にするために、特定の法律および規制によって、サービスプロバイダー (SP) およびインターネットサービスプロバイダー (ISP) に対して、認可された電子監視を明示的にサポートするようにネットワークを実装することが定められています。

合法的傍受プロセス

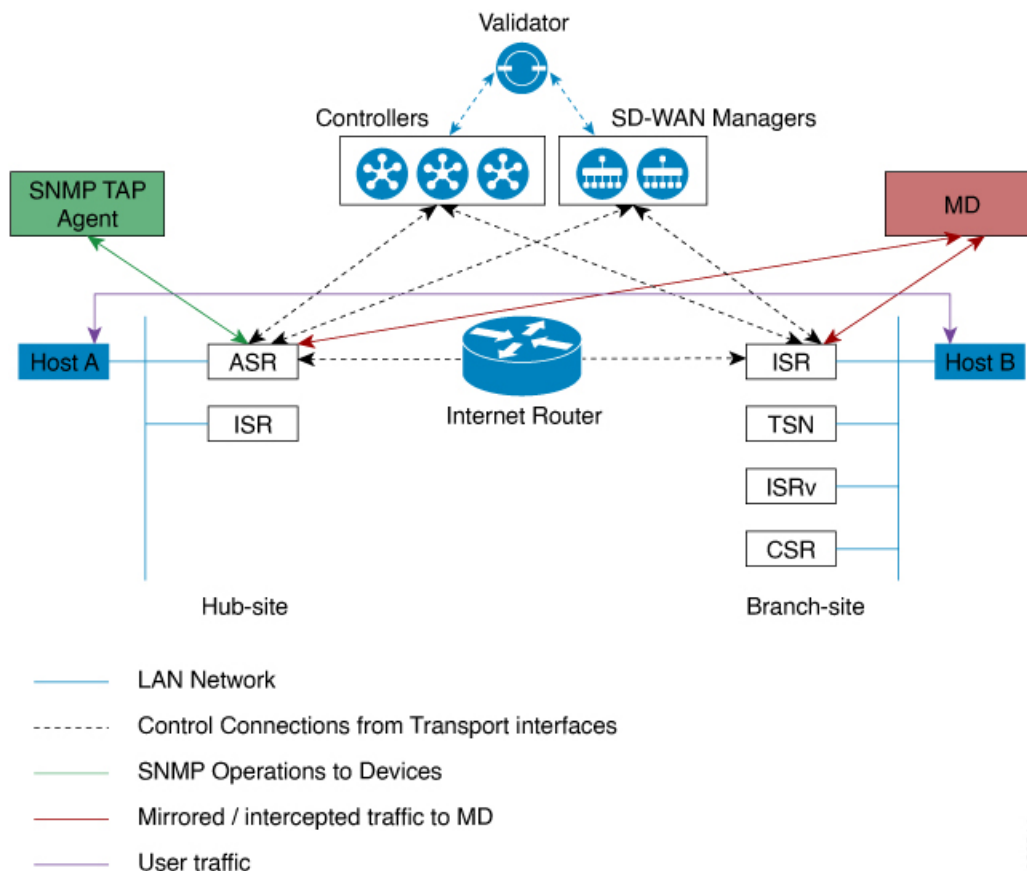
サイト A からサイト B への通信の合法的傍受をトリガーすると、エッジプラットフォームはトラフィックを複製し、トラフィックの暗号化されていないコピーをターゲットサーバーに送信します。これはお客様のネットワークでホストされ、合法的傍用に設計されたサーバーです。Cisco SD-WAN Manager により、サイト A とサイト B にアクセスして情報を取得できる Cisco SD-WAN Manager ユーザー (非合法的傍受ユーザー) は、情報の重複したフローに気付かないようになります。

図 30 : Cisco Catalyst SD-WAN での合法的傍受ワークフロー



368515

図 31 : Cisco Catalyst SD-WAN での合法的傍受プロセス



369514

ライセンスベースの合法的傍受

Cisco Catalyst SD-WAN ソリューションは、期間ベースのライセンス機能です。この機能ライセンスは、Cisco Catalyst SD-WAN ソリューションの Cisco SD-WAN Manager コンポーネントを有効にし、お客様が合法的傍受機能にアクセスできるようにします。ソリューションで合法的傍受ライセンスが有効になると、Cisco SD-WAN Manager は Cisco SD-WAN Manager UI の [ユーザーの管理 (Manage Users)] メニューに新しい権限を提供します。デフォルトでは、この権限はすべての管理者ユーザーが使用できます。さらに、管理者は他のユーザーに合法的傍受権限を割り当てることができます。

合法的傍受権限を持つユーザーであれば、WAN ネットワーク内のエッジデバイスで合法的傍受機能を有効にできます。ユーザーが合法的傍受機能を使用して行ったすべての変更は監査ログに記録され、システム内の他のユーザーが行ったあらゆる変更と同じように記録されます。

合法的傍受の権限を持つすべてのユーザーは、監視を実行する裁判所命令または令状を取得した後、令状があるサイトで合法的傍受に関連する変更を加えることができます。

1. Cisco SD-WAN Manager に合法的傍受のライセンスをインストールします。
2. Cisco SD-WAN Manager で合法的傍受管理者 (liadmin) ユーザーを作成します。liadmin ユーザーは、ユーザーグループ (Basic) に関連付けられている必要があります。

3. **liadmin** ユーザーとして Cisco SD-WAN Manager にログインし、合法的傍受固有のテンプレートを設定します。
4. Cisco SD-WAN Manager は、合法的傍受に対応したイメージを含むすべての Cisco IOS XE Catalyst SD-WAN デバイスにテンプレートを自動的にプッシュします。
5. 設定は、Cisco SD-WAN Manager から次の方法でデバイスにプッシュされます。
 1. SNMP、TAP、MIB 設定
 2. SNMP アクセスリスト (li-acl キーワード)
 3. MD リスト
6. SNMP SET は、次の目的を達成するためにデバイスに送信されます。
 1. Cisco IOS XE Catalyst SD-WAN デバイスで MD エントリを設定してアクティブにします。
 2. 傍受するストリームを設定してアクティブにします。
 3. 傍受をアクティブ化または非アクティブ化します。
7. メディエーションデバイスは、傍受またはミラーリングされたトラフィックを受信します。

VRF 対応の合法的傍受

VRF 対応の合法的傍受は、特定の VPN 内における IPv4 データの合法的傍受盗聴をプロビジョニングする機能です。この機能により、LEA は、その VPN 内のターゲットデータを合法的に傍受できます。VRF ベースの合法的傍受タップを受けるのは、その VPN 内の IPv4 データのみです。

VPN ベースの IPv4 タップをプロビジョニングするために、LI 管理機能 (メディエーションデバイスで動作します) は、CISCO-IP-TAP-MIB を使用して、ターゲットの VPN が使用している VRF テーブルの名前を特定します。VRF 名は、タップを実行するために LI をイネーブルにする VPN インターフェイスを選択するのに使用します。デバイスは、傍受するトラフィックと、傍受したパケットを送信するメディエーションデバイスを、VRF 名 (および送信元アドレス、宛先アドレス、送信元ポート、宛先ポート、プロトコル) に基づいて決定します。

合法的傍受の前提条件

シスコによる合法的傍受 MIB ビューへのアクセスは、メディエーションデバイス、およびルータでの合法的傍受について知る必要があるシステム管理者だけに制限する必要があります。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

ルータがメディエーションデバイスと通信して合法的傍受を実行するには、次の構成要件が満たされている必要があります。

- ルータとメディエーションデバイスの両方のドメイン名が、ドメイン ネーム システム (DNS) に登録されている必要があります。DNSで、ルータのIPアドレスは、通常はルータ上の FastEthernet0/0/0 インターフェイスのアドレスです。
- メディエーションデバイスに Access Function (AF) および Access Function Provisioning Interface (AFPI) が必要です。
- メディエーションデバイスを、CISCO-TAP2-MIB ビューにアクセスできるシンプル ネットワーク管理プロトコル (SNMP) ユーザグループに追加する必要があります。グループに追加するユーザとして、メディエーションデバイスのユーザ名を指定します。
 - メディエーションデバイスを CISCO-TAP2-MIB ユーザとして追加するときに、必要に応じてメディエーションデバイスの認可パスワードを指定できます。パスワードの長さは、最低 8 文字である必要があります。
- 機能テンプレートの [VPN インターフェイス イーサネット (VPN Interface Ethernet)] ページを使用して Cisco SD-WAN Manager で SNMP サービスを設定する必要があります。「テンプレート」トピックの「VPN インターフェイス イーサネット」セクションを参照してください。

Cisco Catalyst SD-WAN Manager を使用した合法的傍受のインストール



(注) 次のプロセスは、すべての Cisco SD-WAN Manager ノードで繰り返す必要があります。

1. Cisco SD-WAN Manager デバイスに管理者として接続する
2. ツールライセンスを要求する

```
vm12# tools license request
Your org-name is: XYZ Inc
Your license-request challenge is:
Uwk3u4Vwk18n632fKDIpKDEFkzfeJlhFQP0Hopbvewmed0U83LQDgaj07GnmCIgA
```

3. ステップ 2 の出力を使用してライセンスを生成するには、シスコサポートにお問い合わせください。
4. install file コマンドを実行し、再起動します。

```
vm12# tools license install file license.lic
License installed. Please reboot to activate.
vm12# reboot
Are you sure you want to reboot? [yes,no] yes
```

```
Broadcast message from root@vm12 (somewhere) (Tue Jan 22 17:07:47 2019):
Tue Jan 22 17:07:47 UTC 2019: The system is going down for reboot NOW!
Connection to 10.0.1.32 closed.
tester@vip-vmanage-dev-109:~$
```

5. 次のコマンドを使用して、合法的傍受ライセンスが正常にインストールされていることを確認します。

```
vm12# show system status
LI License Enabled True
```

6. Cisco SD-WAN Manager を使用して合法的傍受管理者ユーザーを作成します。
7. 合法的傍受の管理者ログイン情報を使用して Cisco SD-WAN Manager にログインします。



- (注) リポート後にすべてのライセンスを削除するには、**tools license remove-all** コマンドを使用します。以前のライセンスを再インストールすることはできません。

合法的傍受 MIB

機密に関係するため、シスコによる合法的傍受 MIB は合法的傍受機能をサポートするソフトウェアイメージだけで使用できます。

これらの MIB には、Network Management Software MIBs [Support ページ](#)からはアクセスできません。

合法的傍受 MIB へのアクセスの制限

合法的傍受 MIB へのアクセスは、必ずメディエーションデバイスおよび合法的傍受について知る必要があるユーザーに限ってください。こうした MIB へのアクセスを制限するには、次の作業を実行する必要があります。

1. シスコによる合法的傍受 MIB を含むビューを作成します。
2. このビューへの読み取りおよび書き込みアクセス権を持つ SNMP ユーザグループを作成します。このユーザグループに割り当てられたユーザだけが、MIB の情報にアクセスできます。
3. ユーザをシスコ LI ユーザグループに追加し、合法的傍受に関連する MIB および情報にアクセスできるユーザを定義します。このグループのユーザとして、メディエーションデバイスを追加してください。追加しないと、ルータで合法的傍受を実行できません。



- (注) MD5 認証キー生成アルゴリズムの詳細は、<https://tools.ietf.org/html/rfc3414#appendix-A.2.1> で定義されています。

信頼できるホストへのアクセス制限（暗号化なし）

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方をサポートします。セキュリティ モデルは、ユーザおよびユーザに属するグループに合わせて設定される認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットを処理するときに適用されるセキュリティ メカニズムが決定されます。

さらに、名前付きアクセスリストに対応した SNMP 機能により、いくつかの SNMP コマンドで、標準の名前付きアクセスコントロールリスト（ACL）のサポートが追加されます。

新しい SNMP グループ、つまり SNMP ユーザーを SNMP ビューにマッピングするテーブルを設定するには、グローバル コンフィギュレーション モードで `snmp-server` コマンドを使用します。

以下は、99 という名前のアクセスリストで、10.1.1.1 からの SNMP トラフィックのみを Cisco IOS XE Catalyst SD-WAN デバイスにアクセスできるようにする例です。このアクセスリストは、この後 SNMP ユーザーである `testuser` に適用されます。

```
access-list 99 permit ip host 10.1.1.1
snmp-server user testuser INTERCEPT_GROUP v3 encrypted auth sha
testPassword1 priv aes testPassword2 access 99
```

許可されているのは、WAN インターフェイス（`gigabitEthernet 1`）からの SNMP トラフィックのみです。

```
control-plane host
management-interface gigabitEthernet 1 allow snmp
```

信頼できるメディアエーションデバイスの制限

以下は、`md-list` コマンドを使用して、サブネット 10.3.3.0/24 での SNMP 要求 `config MD` を許可する例です。

Cisco IOS XE Catalyst SD-WAN デバイスはメディアエーションデバイスを作成する SNMP 要求を受信すると、まずメディアエーションデバイス リストの設定情報を確認します。

メディアエーションデバイスの IP アドレスが設定済みのメディアエーションデバイス リストにならない場合、そのメディアエーションデバイス エントリはアクティブになっていません。

```
md-list 10.3.3.0 255.255.255.0
```



(注) メディアエーションデバイス リストのサブネットは最大 8 つまで設定できます。

合法的傍受の設定

Cisco SD-WAN Manager の合法的傍受設定のための 2 つのコンポーネントを次に示します。

- 合法的傍受の SNMP テンプレート：このテンプレートは、次の設定を規定します。
 - 合法的傍受用の SNMPv3 グループ：デフォルトのグループ名は INTERCEPT_GROUP です。
 - 合法的傍受用の SNMPv3 ユーザー：デフォルトでは、すべてのユーザーがアクセスリストによって制限されます。
 - SNMPv3 ビューはデフォルトで設定されています。ビューには Cisco TAP MIB が含まれます。
 - 次の TAP MIB が設定されています。
 - ciscoIpTapMIB
 - ciscoTap2MIB
 - ifIndex
 - ifDescr
- 合法的傍受アクセスリストテンプレート：このアクセスリストテンプレートは、次の設定を提供します。
 - 仲介デバイスリストの設定：最大 8 つのサブネットを設定するオプションを提供します。
 - SNMP アクセスリスト：最大 8 つのサブネットまたはホストアドレス、およびワイルドカードマスクを設定するオプションを提供します。

CLI を使用した、合法的傍受の設定

```
control-plane host
management-interface GigabitEthernet0/0/0 allow ftp ssh snmp
management-interface GigabitEthernet0/0/1 allow ftp ssh snmp
!
!
md-list 10.101.0.0 255.255.255.0
md-list 10.102.0.10 255.255.255.255
md-list 10.103.0.0 255.255.255.0
md-list 10.104.0.4 255.255.255.255
md-list 10.105.0.0 255.255.255.0
md-list 10.106.0.0 255.255.255.0
md-list 10.107.0.7 255.255.255.255
md-list 10.108.0.0 255.255.0.0
!
ip access-list standard li-acl
permit 174.16.50.254
```

例：メディエーション デバイス アクセスの合法的傍受 MIB の有効化

次に、メディエーション デバイスが合法的傍受 MIB にアクセスできるようにする例を示します。この例では、4つのLMIB（CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、CISCO-802-TAP-MIB、CISCO-USER-CONNECTION-TAP-MIB）を含む SNMP ビュー（tapV）を作成します。また、tapV ビュー内の MIB に読み込み、書き込み、通知アクセス可能なユーザ グループも作成します。

```
snmp-server enable trap
snmp-server engineID local 766D616E6167652Dac10ff31
snmp-server group INTERCEPT_GROUP v3 noauth read INTERCEPT_VIEW write INTERCEPT_VIEW
notify SNG_VIEW
snmp-server user UItestuser1 INTERCEPT_GROUP v3 encrypted auth md5
DA:B2:36:03:6A:5C:D0:6D:F6:D8:9C:5E:56:77:AD:43 priv aes 128
DA:B2:36:03:6A:5C:D0:6D:F6:D8:9C:5E:56:77:AD:43 access li-acl
snmp-server user UItestuser2 INTERCEPT_GROUP v3 encrypted auth md5
D2:01:1E:47:D8:9E:3E:B5:58:CD:90:0F:49:FC:36:56 priv aes 128
CF:32:C4:3E:34:27:3F:4A:D8:18:A7:19:E5:04:A7:DF access li-acl
!
snmp-server engineID local 766D616E6167652DAC10FF31
snmp-server group INTERCEPT_GROUP v3 noauth read INTERCEPT_VIEW write INTERCEPT_VIEW
notify SNG_VIEW
snmp-server view INTERCEPT_VIEW ciscoIpTapMIB included
snmp-server view INTERCEPT_VIEW ciscoTap2MIB included
snmp-server view INTERCEPT_VIEW ifIndex included
snmp-server view INTERCEPT_VIEW ifDescr included
```

合法的傍受トラフィックの暗号化

ルータ（コンテンツ傍受アクセスポイント（IAP））と仲介デバイス（MD）間で傍受されたトラフィックを暗号化することを推奨します。

必要な設定は次のとおりです。

- ルータで暗号化を設定し、MD内の暗号化クライアントまたはMDに関連するルータでトラフィックを復号します。
- 信頼できるホストへのアクセスを制限します。
- VPN クライアントを設定します。

デバイスでの暗号化の設定

暗号化を設定するには、認証、許可、およびアカウントティング（AAA）パラメータを設定します。次に、パラメータを設定する例を示します。

```
aaa authentication login userauthen local
username <username> password 0 <password>
```

CISCO-TAP2-MIB では、送信元インターフェイスは Cisco IOS XE Catalyst SD-WAN デバイスのトンネルインターフェイスである必要があり、宛先アドレスは仲介デバイスの IP アドレスである必要があります。

CLI を使用した、合法的傍受の暗号化設定

以下は、Cisco IOS XE Catalyst SD-WAN デバイス とメディア デバイス ゲートウェイの間に IPSec トンネルを設定する場合の例です。メディア デバイス ゲートウェイは、IPSec トンネルを終端し、IPSec トンネルを介してメディアデバイスリストにルートを追加します。

CISCO-TAP2-MIB では、送信元インターフェイスは Cisco IOS XE Catalyst SD-WAN デバイスのトンネルインターフェイスで、宛先アドレスは、メディアデバイスの IP アドレスです。

```
crypto ikev2 diagnose error 1000
crypto ikev2 keyring ikev2_keyring
peer mypeer
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123                                □ pre-shared key should be same on media
deviec gateway
!
crypto ikev2 profile ikev2_profile
authentication local pre-share
authentication remote pre-share
dpd 10 3 on-demand
lifetime 14400
keyring local ikev2_keyring
match identity remote address 0.0.0.0 0.0.0.0
!
crypto ikev2 proposal default
encryption aes-cbc-256
group 14 16 19 2 20 21
integrity sha256 sha384 sha512
!
crypto ipsec profile ipsec_profile
set ikev2-profile ikev2_profile
set pfs group16
set transform-set tfs
set security-association lifetime seconds 7200
set security-association replay window-size 256
!
crypto ipsec transform-set tfs esp-gcm 256
mode tunnel
!
interface Tunnel100
no shutdown
ip address 10.2.2.1 255.255.255.0                        □ tunnel address
tunnel source GigabitEthernet1                        □ Cisco XE SD-WAN WAN interface
tunnel destination 10.124.19.57                       □ Media Device Gateway address
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec_profile

ip route 10.3.3.0 255.255.255.0 Tunnel100 □ route MD list traffic through IPSec Tunnel
```

IPSec トンネルを終端するようにメディアゲートウェイを設定するには、次の設定を使用します。

```
crypto ikev2 proposal default
encryption aes-cbc-256
integrity sha384 sha512 sha256
group 20 16 19 14 21 2
!
crypto ikev2 keyring ikev2_keyring
peer mypeer
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123                                □ pre-shared key, should be same on cEdge
!
```

```
crypto ikev2 profile ikev2-profile
match identity remote address 0.0.0.0 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local ikev2_keyring
lifetime 14400
dpd 10 3 on-demand
crypto ipsec transform-set tfs esp-gcm 256
mode tunnel
crypto ipsec profile ipsec_profile
set security-association lifetime seconds 7200
set security-association replay window-size 256
set transform-set tfs
set pfs group16
set ikev2-profile ikev2_profile
!
interface Tunnel100
ip address 10.2.2.2 255.255.255.0
tunnel source GigabitEthernet1
tunnel mode ipsec ipv4
tunnel destination 10.74.5.213
tunnel protection ipsec profile ipsec_profile
!
```

Tunnel address
 MD GW phy interface
 cEdge wan interface

メディア デバイス ゲートウェイとの静的トンネルの確認

Cisco IOS XE Catalyst SD-WAN デバイス とメディア デバイス ゲートウェイ間の IPSec トンネルは静的であり、常にアップ状態です。

メディア デバイス ゲートウェイの静的トンネル設定を確認するには、次のコマンドを使用します。

- **show crypto session detail**
- **show crypto ipsec sa**



第 23 章

合法的傍受 2.0



- (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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

表 48: 機能の履歴

機能名	リリース情報	説明
合法的傍受 2.0	Cisco vManage リリース 20.9.1	これは、合法的傍受バージョン 2.0 を導入する機能です。合法的傍受 2.0 の機能では、マネージドサービスプロバイダー (MSP) によってキャプチャされた Cisco Catalyst SD-WAN IPsec トラフィックを復号できるように、キー情報が Cisco Catalyst SD-WAN ルータおよび制御コンポーネントによって法執行機関 (LEA) に提供されます。これは、LEA が暗号化されたネットワークトラフィック情報を復号するのに役立ちます。合法的傍受 1.0 の詳細については、Cisco Catalyst SD-WAN の『ポリシー設定ガイド』の「合法的傍受」の章を参照してください。

機能名	リリース情報	説明
合法的傍受 2.0 の拡張機能	Cisco vManage リリース 20.10.1	<p>これは、Cisco Catalyst SD-WAN の合法的傍受機能で使用可能な Cisco SD-WAN Manager GUI およびトラブルシューティング オプションを強化する機能です。</p> <ul style="list-style-type: none"> • Cisco SD-WAN Manager GUI 拡張機能は次のとおりです。 <ul style="list-style-type: none"> • Cisco SD-WAN コントローラ で新たに設定された傍受設定を同期するための [vSmart に同期 (Sync to vSmart)] ボタン。 • 傍受設定を有効または無効にするトグルボタン。 • 同期とアクティブ化のステータスを表示する進行状況ページ。 • 新しい合法的傍受タスクを示す、Cisco SD-WAN Manager ツールバーのタスクリストアイコンの赤い点。 • アクティブおよび完了した合法的傍受タスクのリストを表示するタスクリストペイン。 • Cisco SD-WAN コントローラ からキー情報または傍受関連情報 (IRI) を取得するための傍受取得オプション Get IRI。 • デバッグログと管理技術ファイルを使用して、Cisco SD-WAN コントローラ および Cisco SD-WAN Manager をトラブルシューティングする機能。
合法的傍受 2.0 の拡張機能	Cisco Catalyst SD-WAN Manager リ リース 20.12.1	<p>これは、合法的傍受をマルチテナントモードに拡張し、Cisco SD-WAN Manager クラスタのサポートを行えるようにする機能です。Cisco SD-WAN Manager クラスタの詳細については、「クラスタの管理」を参照してください。</p>

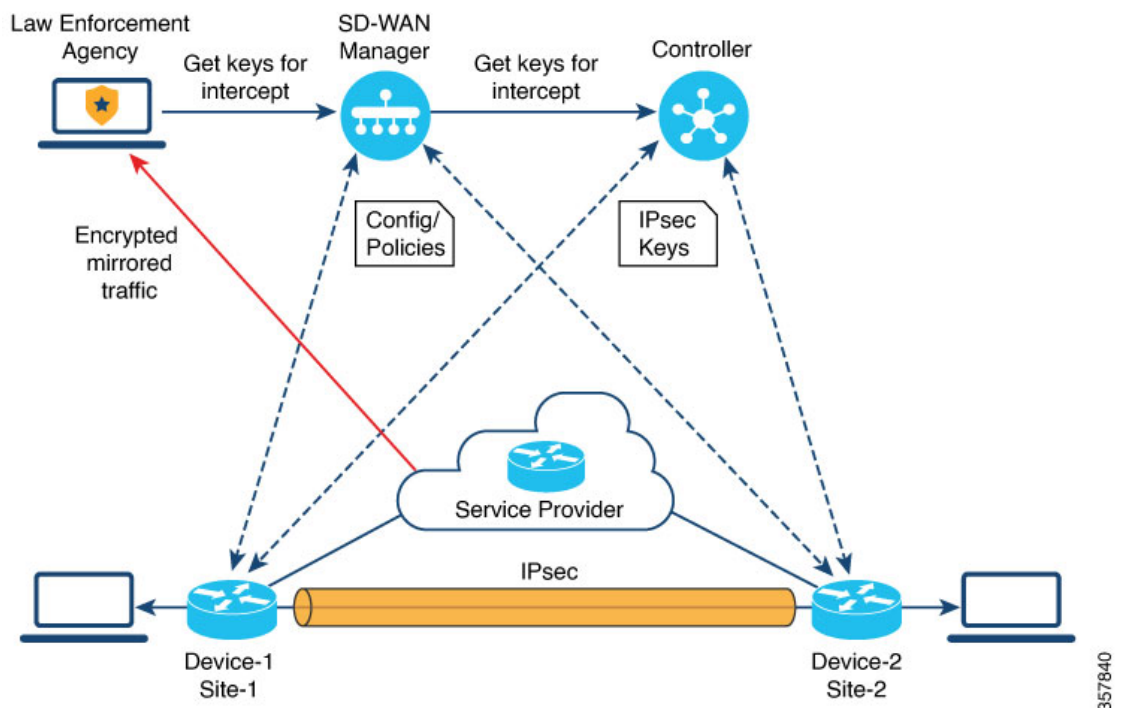
- [合法的傍受 2.0 について \(385 ページ\)](#)
- [Cisco Catalyst SD-WAN の合法的傍受 2.0 の前提条件 \(386 ページ\)](#)
- [Cisco Catalyst SD-WAN の合法的傍受 2.0 の利点 \(386 ページ\)](#)
- [合法的傍受 2.0 のワークフローの設定 \(386 ページ\)](#)
- [合法的傍受管理者の作成 \(387 ページ\)](#)
- [合法的傍受 API ユーザーの作成 \(387 ページ\)](#)
- [傍受案件の作成 \(388 ページ\)](#)
- [傍受内容の回収 \(390 ページ\)](#)
- [Cisco SD-WAN Manager による合法的傍受のための Cisco SD-WAN コントローラ トラブルシューティング \(391 ページ\)](#)

合法的傍受 2.0 について

Cisco Catalyst SD-WAN の合法的傍受機能により、LEA は分析または証拠のためにネットワークトラフィックのコピーを取得できます。これは、トラフィックミラーリングとも呼ばれます。Cisco Catalyst SD-WAN の『Policies Configuration Guide』の「合法的傍受」の章を参照してください。

Cisco vManage リリース 20.9.1 以降、Cisco Catalyst SD-WAN は次の図に示すように、合法的傍受の新しいアーキテクチャを実装します。

図 32:合法的傍受 2.0 アーキテクチャ



新しいアーキテクチャには次のような特長があります。

- トラフィックミラーリングはCisco Catalyst SD-WAN の範囲外です。LEA は、対応するサービスプロバイダーと連携して、ミラーリング用のネットワークトラフィックをキャプチャします。



(注) 上の図では、サービスプロバイダーはアンダーレイ接続で、IPsec トンネルはオーバーレイ接続です。

- キャプチャされたネットワークトラフィックは暗号化されているため、Cisco SD-WAN Manager と Cisco SD-WAN コントローラ は LEA にキー情報を提供します。

- LEA は Cisco SD-WAN Manager からキーを取得して、Cisco Catalyst SD-WAN IPsec トラフィックを復号します。LEA は、各キー再生成期間中にキー情報が取得されるようにします。キー再生成期間は、サービスプロバイダーによって提供されます。キーの取得の詳細については、[傍受内容の回収 \(390 ページ\)](#) を参照してください。キー再生成期間の詳細については、「[Configure Data Plane Security Parameters](#)」を参照してください。

合法的傍受管理者は、傍受を設定し、合法的傍受を実行する合法的傍受 API ユーザーを作成する全責任を負います。Cisco SD-WAN Manager 管理者は、合法的傍受管理者のアカウントを作成できます。管理者は、**li-admin** グループのメンバーである必要があります。合法的傍受管理者のアカウント作成の詳細については、「[合法的傍受管理者の作成 \(Create Lawful Intercept Administrator\)](#)」を参照してください。

Cisco Catalyst SD-WAN の合法的傍受 2.0 の前提条件

- Cisco SD-WAN コントローラを Manager モードに設定する必要があります。
- Cisco Catalyst SD-WAN での IPsec トラフィックの復号の詳細については、シスコサポートまたはシスコの営業チームにお問い合わせください。

Cisco Catalyst SD-WAN の合法的傍受 2.0 の利点

- 合法的傍受用にエッジデバイスを設定する必要はありません。



(注) 傍受を設定するには、管理者が傍受に含める必要があるエッジデバイスを選択する必要があります。これが必要なのは、Cisco SD-WAN Manager から取得されるキー情報には、選択したデバイスのキーも含まれるためです。

- サービスプロバイダーは、傍受のためにデータトラフィックをキャプチャします。トラフィックはエッジデバイスからは傍受されません。

合法的傍受 2.0 のワークフローの設定



(注) 合法的傍受機能は、Cisco SD-WAN Manager を通してのみ設定でき、CLI では設定できません。

Cisco SD-WAN Manager で合法的傍受を設定するには、次の手順を実行します。

1. [合法的傍受管理者の作成](#)

- 合法的傍受 API ユーザーの作成
- 傍受案件の作成

合法的傍受管理者の作成

Cisco SD-WAN Manager の管理者アカウントを使用して、合法的傍受管理者のアカウントを作成します。

- Cisco SD-WAN Manager メニューから、[管理 (Administration)] > [合法的傍受 (Lawful Intercept)] の順に選択します。
- [ユーザーの追加 (Add User)] をクリックして、合法的傍受管理者ユーザーアカウントを作成します。
- [氏名 (Full Name)] フィールドに、合法的傍受管理者の氏名を入力します。
- [ユーザー名 (User Name)] フィールドに、合法的傍受管理者のユーザー名を入力します。ユーザー名の先頭には「li-」が付きます。
- [パスワード (Password)] フィールドに、合法的傍受管理者のパスワードを入力します。
- [パスワードの確認 (Confirm password)] フィールドで、パスワードを確認します。
- [ユーザーグループ (User Group)] ドロップダウンリストから [li-admin] を選択し、[追加 (Add)] をクリックします。

新しく作成された合法的傍受管理者ユーザーアカウントが [ユーザー (Users)] ウィンドウに表示されます。

合法的傍受 API ユーザーの作成

合法的傍受 API ユーザーアカウントは、ログインし、Cisco SD-WAN Manager の REST API を使用してキー情報を取得する LEA のユーザー用です。Cisco Catalyst SD-WAN IPsec トラフィックの合法的傍受を実行するユーザーです。

LEA では

`https://{vmanage_ip}/dataservice/li/intercept/retrieve/<intercept_id>` を使用して、キー情報を取得します。

合法的傍受 API ユーザーを作成するには、次の手順を実行します。

- 合法的傍受管理者として Cisco SD-WAN Manager にログインします。



(注) 合法的傍受管理者が Cisco SD-WAN Manager にログインすると、Cisco SD-WAN Manager メニューで使用できるのは[モニター (Monitor)] オプションと[管理 (Administration)] オプションのみです。

2. Cisco SD-WAN Manager メニューから、[管理 (Administration)] > [合法的傍受 (Lawful Intercept)] の順に選択します。
3. [ユーザーの追加 (Add User)] をクリックして、合法的傍受 API ユーザーアカウントを作成します。
4. [氏名 (Full Name)] フィールドに、合法的傍受 API ユーザー氏名を入力します。
5. [ユーザー名 (UserName)] フィールドに、合法的傍受 API ユーザー名を入力します。ユーザー名の先頭には「li-」が付きます。
6. [パスワード (Password)] フィールドに、合法的傍受 API ユーザーのパスワードを入力します。
7. [パスワードの確認 (Confirm password)] フィールドで、パスワードを確認します。
8. [ユーザーグループ (User Group)] ドロップダウンリストから [li-api] を選択し、[追加 (Add)] をクリックします。

新しく作成された合法的傍受 API ユーザーアカウントが [ユーザー (Users)] ウィンドウに表示されます。LEA は、合法的傍受 API ユーザーアカウントを使用して Cisco SD-WAN Manager にログインし、キー情報を取得できます。

傍受案件の作成

サポート対象の最小リリース : Cisco vManage リリース 20.9.1 および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.9.1

傍受データを収集するために傍受案件を設定します。傍受案件を設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、[管理 (Administration)] > [合法的傍受 (Lawful Intercept)] の順に選択します。
2. [傍受案件 (Intercepts)] タブをクリックし、[傍受案件の追加 (Add Intercepts)] をクリックします。
3. Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降のリリース :
Tenant ドロップダウンリストから、テナントを選択します。テナントの追加に関する詳細は、「[新しいテナントの追加](#)」を参照してください。
4. [傍受案件 ID (Intercept ID)] フィールドに、番号を入力します。最小 2 桁、最大 25 桁を入力します。

5. [説明 (Description)] フィールドに、傍受案件の説明を入力します。
6. [有効化 (Enable)] トグルボタンは、デフォルトで有効になっています。ただし、傍受案件は作成後も非アクティブ状態のままです。
7. [Next] をクリックします。

シングルテナントモードでは、[エッジデバイスの追加 (Add Edge Devices)] ポップアップウィンドウに Cisco Catalyst SD-WAN ネットワーク内のすべてのエッジデバイスが表示されます。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降のリリース :

マルチテナントモードでは、[エッジデバイスの追加 (Add Edge Devices)] ポップアップウィンドウに、選択したテナントに関連付けられているすべてのシングルテナントエッジデバイスが表示されます。

8. 傍受案件に追加する1つ以上のエッジデバイス名をクリックし、[次へ (Next)] をクリックします。

ここで、Cisco SD-WAN Manager から、選択したエッジデバイスのキーが提供されます。



- (注) 傍受案件に追加したすべてのエッジデバイスに対して傍受令状を指定します。

傍受のためにエッジデバイスが追加されると、同じネットワークに接続されているすべてのピアデバイスも合法的傍受に使用できます。

9. [LI APIユーザーの追加 (Add LI API users)] ページには、合法的傍受管理者によって作成されたすべての LI-API ユーザーが表示されます。
10. 1つ以上のユーザー名をクリックして傍受案件に追加します。ここで選択したユーザーは、傍受に必要なキー情報を Cisco SD-WAN Manager から取得できます。傍受案件用にキーを取得する方法については、[傍受内容の回収](#)を参照してください。
11. [サマリー (Summary)] をクリックします。
傍受案件の概要が表示されます。
12. [Submit] をクリックします。`[傍受案件 (Intercepts)]` ページに、設定した傍受案件が表示されます。
13. [vSmart に同期 (Sync to vSmart)] をクリックして、Cisco SD-WAN Manager で設定された傍受案件設定を Cisco SD-WAN コントローラ と同期します。
進行状況ページに、同期とアクティブ化のステータスが表示されます。同期が成功すると、[アクティブ状態 (Activate State)] フィールドに緑色のチェックマークが表示されます。



- (注) [Activate State] フィールドには、Cisco SD-WAN コントローラが **Manager** モードに設定されている場合にのみ、緑色のチェックマークのステータスが表示されます。

追加の合法的傍受タスクがある場合は、Cisco SD-WAN Manager ツールバーのタスクリストアイコンに赤い点が表示されます。タスクリストアイコンをクリックすると、アクティブな状態になっている完了したすべての合法的傍受タスクのリストが表示されます。合法的傍受タスクは、最新 500 件まで表示できます。

傍受案件が変更されると、[vSmart に同期 (Sync to vSmart)] ボタンが有効になります。[vSmart に同期 (Sync to vSmart)] をクリックして、Cisco SD-WAN Manager の傍受案件設定を Cisco SD-WAN コントローラ と同期します。



- (注) [vSmart に同期 (Sync to vSmart)] ボタンは、新しい傍受案件が作成された場合、または傍受案件が編集または削除された場合にのみ有効になります。

傍受に必要なキー情報を取得するには、[...] をクリックし、[IRI の取得 (Get IRI)] をクリックします。IRI は Cisco SD-WAN コントローラ から取得され、Cisco SD-WAN Manager に表示されます。

傍受内容の回収

こうした情報は、MSP によってキャプチャされたトラフィックを復号するために必要であるため、LEA は定期的にキー情報を取得する必要があります。

LEA は、[Cisco Catalyst SD-WAN Manager REST API](#) を使用してキー情報を取得できます。

1. LEA は、合法的傍受 API ユーザーとして Cisco SD-WAN Manager にログインします。
2. 合法的傍受 API ユーザーが認証されると、LEA はキー情報を取得する傍受 ID を指定する Cisco SD-WAN Manager REST API を使用して、リクエストを送信します。
3. LEA からのリクエストを Cisco SD-WAN Manager が受信すると、Cisco SD-WAN Manager は、傍受設定がされている Cisco SD-WAN コントローラ に要求を転送します。
4. Cisco SD-WAN コントローラ は次に、指定された傍受案件 ID のキー情報を取得し、キー情報を JSON 形式で Cisco SD-WAN Manager に返します。

Cisco SD-WAN Manager による合法的傍受のための Cisco SD-WAN コントローラ トラブルシューティング

サポート対象の最小リリース : Cisco vManage リリース 20.10.1 および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

Cisco SD-WAN Manager では、デバッグログと admin-tech ファイルを提供して、Cisco SD-WAN コントローラ および Cisco SD-WAN Manager のいかなる問題もトラブルシューティングできるようにしています。

デバッグ ログ

Cisco SD-WAN Manager の Cisco SD-WAN コントローラ をトラブルシューティングするために、デバッグログを使用します。

Cisco SD-WAN Manager でデバッグログを表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、[管理 (Administration)] > [合法的傍受 (Lawful Intercept)] の順に選択します。
2. [Devices] タブをクリックします。
3. デバッグログを表示するデバイスの横にある [...] をクリックし、[デバッグログ (Debug Log)] を選択します。
4. [ログファイル (Log Files)] ドロップダウンリストで、ログファイル名を選択します。ウィンドウの下部にログ情報が表示されます。

Admin-tech ファイル

Cisco SD-WAN Manager の Cisco SD-WAN Manager および Cisco SD-WAN コントローラ をトラブルシューティングするために、デバッグログと admin-tech ファイルを使用します。Admin-tech ファイルの生成に関する詳細については、「[Admin-tech ファイルの生成](#)」を参照してください。



第 24 章

Cisco Catalyst SD-WAN のポリシーに関する トラブルシューティング



(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、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** 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。

- [概要 \(393 ページ\)](#)
- [サポート記事 \(394 ページ\)](#)
- [フィードバックのリクエスト \(395 ページ\)](#)
- [免責事項と注意事項 \(395 ページ\)](#)

概要

この章では、シスコの主題専門家 (SME) が作成したドキュメントへのリンクを提供します。サポートチケットを必要とせずに技術的な問題を解決できるようにすることを目的としています。これらのドキュメントで問題を解決できない場合は、該当する [シスココミュニティ](#) にアクセスすることをお勧めします。この問題をすでに経験し、解決策を提供している可能性のある他のシスコのお客様からは、豊富な情報とアドバイスを入手できます。コミュニティで解決策が見つからない場合は、[シスコサポート](#) でサポートチケットを提出するのが最善の方法です。サポートチケットを発行する必要がある場合、これらのドキュメントは、収集してサポートチケットに追加する必要があるデータに関するガイダンスを提供します。参照したサポートドキュメントを指定すると、TAC はドキュメントの所有者と改善要求を作成できます。

サポート記事

このセクションのドキュメントは、各記事の「使用するコンポーネント」セクションにリストされている特定のソフトウェアとハードウェアを使用して作成されています。ただし、これは、それらが使用されるコンポーネントにリストされているものに限定されるという意味ではなく、通常、ソフトウェアおよびハードウェアの新しいバージョンに関連し続けます。ソフトウェアまたはハードウェアに変更があり、コマンドが動作しなくなったり、構文が変更されたり、GUI や CLI がリリースごとに異なって見える可能性があることに注意してください。

このテクノロジーに関連するサポート記事は次のとおりです。

マニュアル	説明
Cisco Catalyst SD-WAN - Configure Route Leaking	このビデオでは、Cisco Catalyst SD-WAN でルートリークを設定する方法を示します。
Collect an Admin-Tech in Cisco Catalyst SD-WAN Environment and Upload to TAC Case	Cisco Catalyst SD-WAN 環境で admin-tech を開始する方法について説明します。
Configure AAR Policy on Cisco Catalyst SD-WAN	このビデオでは、Cisco Catalyst SD-WAN でアプリケーション認識型ルーティングポリシーを設定する方法を示します。
Configure Cisco Catalyst SD-WAN Router to Restrict SSH Access	Cisco Catalyst SD-WAN ルータへの SSH 接続を制限するプロセスについて説明します。
Configure a Control Policy for Region Topology	このビデオでは、リージョントポロジの制御ポリシーを設定し、異なるリージョンのサイトが最も近い DC を介してインターネットに到達できるようにする方法について説明します。
Configure Active/Standby Hub and Spoke Topology on Cisco Catalyst SD-WAN	このドキュメントでは、Cisco Catalyst SD-WAN でアクティブスタンバイハブアンドスポークトポロジを設定および検証する手順について説明します。
Configure a Data Policy to Overwrite a Control Policy	このビデオでは、次のタスクを完了するためにデータポリシーを設定する方法を示します：リージョン 1 のサイトのユーザーはリージョン 2 の DC を介して AWS ネットワークにアクセスする必要があります。その他はすべて、リージョン 1 の DC 経由で流れる必要があります。
Determine Policy Drops on cEdge with FIA Trace	このビデオでは、FIA トレースを使用して cEdge でのポリシートラフィックのドロップを確認する方法を示します。

マニュアル	説明
Troubleshoot Cisco Catalyst Controller Policy Push Activation Errors	Cisco Catalyst SD-WAN オーバーレイネットワークで Cisco SD-WAN Manager からの Cisco SD-WAN コントローラポリシーのアクティブ化で発生する一般的なエラーについて説明します。
Understand BFD Protocol Relationship with App-Aware Routing	このドキュメントでは、BFD Hello パケットとアプリケーション認識型ルーティングトンネル統計情報の間に存在する関係について説明します。

フィードバックのリクエスト

ユーザー入力役立ちます。これらのサポートドキュメントを改善するための重要な側面は、お客様からのフィードバックです。これらのドキュメントは、シスコ内の複数のチームによって所有および管理されていることに注意してください。ドキュメントに固有の問題（不明瞭、混乱、情報不足など）を見つけた場合：

- 対応する記事の右側のパネルにある [Feedback] ボタンを使用して、フィードバックを提供します。ドキュメントの所有者に通知され、記事が更新されるか、削除のフラグが付けられます。
- ドキュメントのセクション、領域、または問題に関する情報と、改善できる点を含めてください。できるだけ詳細に記述してください。

免責事項と注意事項

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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。