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、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

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 *1*：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

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、合法的傍受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 *1 : Cisco Catalyst SD-WAN* での合法的傍受ワークフロー

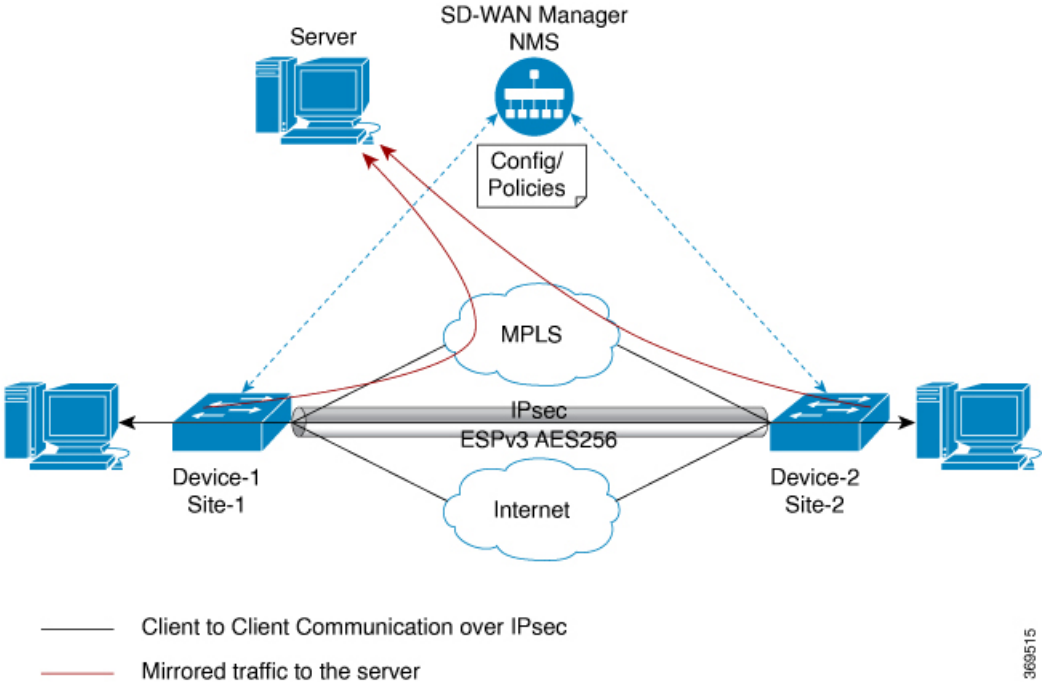
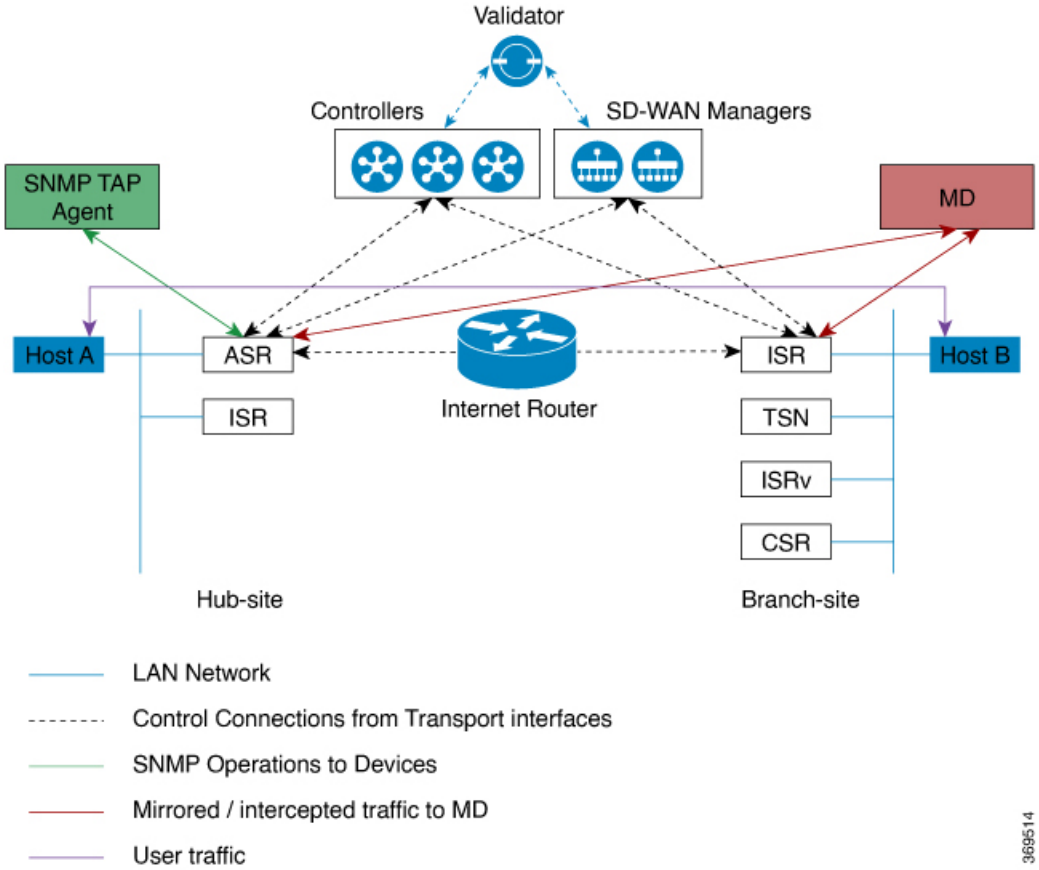


図 *2 : Cisco Catalyst SD-WAN* での合法的傍受プロセス



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:
Uwk3u4Vwkl8n632fKDIpKDEFkzfeJlhFQPOHopbvewmed0U83LQDgajO7GnmCIgA
```

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） リブ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。

メディエーションデバイスの IP アドレスが設定済みのメディエーション デバイス リストにない場合、そのメディエーション 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 LI MIB（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 bee 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 address
tunnel source GigabitEthernet1                      MD GW phy interface
tunnel mode ipsec ipv4
tunnel destination 10.74.5.213                       cEdge wan interface
tunnel protection ipsec profile ipsec_profile
!
```

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**

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。