



リバースプロキシ

- [リバースプロキシ \(1 ページ\)](#)
- [リバースプロキシについて \(1 ページ\)](#)
- [リバースプロキシに関する制約事項 \(4 ページ\)](#)
- [リバースプロキシでの証明書のプロビジョニング \(5 ページ\)](#)
- [Cisco SD-WAN Manager を使用したリバースプロキシの設定 \(6 ページ\)](#)
- [CLI を使用したリバースプロキシの監視 \(8 ページ\)](#)
- [CLI を使用したリバースプロキシの監視 \(12 ページ\)](#)

リバースプロキシ

表 1: 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN および Cisco Catalyst SD-WAN のマルチテナント機能を使用したリバースプロキシのサポート	Cisco IOS XE リリース 17.6.1a Cisco SD-WAN リリース 20.6.1 Cisco vManage リリース 20.6.1	この機能を使用すると、Cisco IOS XE Catalyst SD-WAN デバイス と Cisco SD-WAN Manager と Cisco SD-WAN コントローラ の間のオーバーレイネットワークにリバースプロキシを展開できます。また、この機能を使用すると、Cisco vEdge デバイス または Cisco IOS XE Catalyst SD-WAN デバイス を含むシングルテナント展開とマルチテナント展開の両方にリバースプロキシを展開できます。マルチテナント展開では、サービスプロバイダーがリバースプロキシおよび関連する設定を管理します。

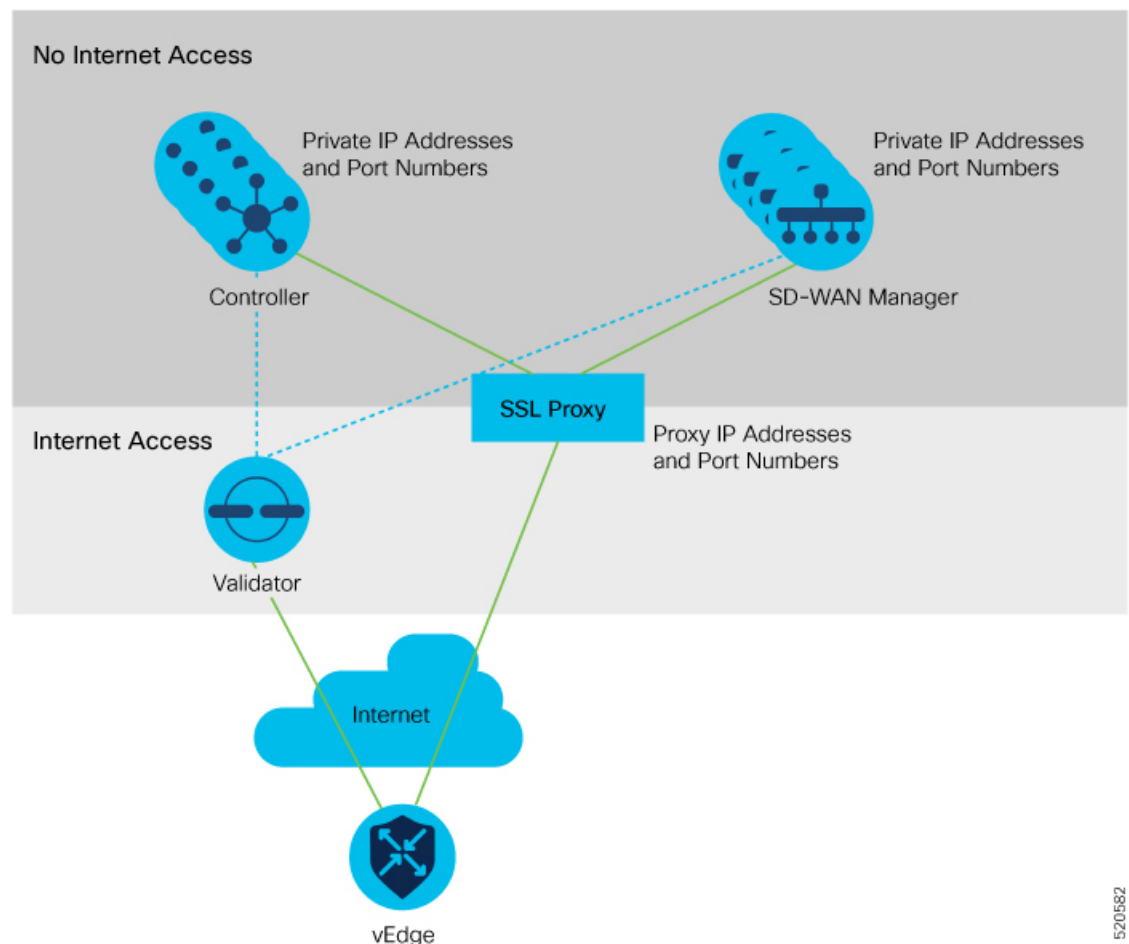
リバースプロキシについて

標準のオーバーレイネットワークでは、Cisco Catalyst SD-WAN エッジデバイスが Cisco SD-WAN 制御コンポーネント（Cisco SD-WAN Manager および Cisco SD-WAN コントローラ）への直接

接続を開始し、これらの接続を介してコントロールプレーン情報を交換します。WAN エッジデバイスは通常、ブランチサイトに配置され、インターネット経由で Cisco SD-WAN コントローラに接続します。その結果、Cisco SD-WAN Manager および Cisco SD-WAN コントローラもインターネットに直接接続されます。

セキュリティまたはその他の理由から、Cisco SD-WAN コントローラに直接インターネット接続をさせたくない場合があります。このようなシナリオでは、Cisco SD-WAN コントローラと WAN エッジデバイスの間にリバースプロキシを展開できます。リバースプロキシは、Cisco SD-WAN コントローラと WAN エッジデバイスの間で制御トラフィックを渡す仲介役として機能します。WAN エッジデバイスは、Cisco SD-WAN Manager および Cisco SD-WAN コントローラと直接通信するのではなくリバースプロキシと通信し、リバースプロキシは Cisco SD-WAN Manager および Cisco SD-WAN コントローラとの間のトラフィックをリレーします。

次の図は、WAN エッジデバイスと Cisco SD-WAN Manager および Cisco SD-WAN コントローラとの間に展開されたリバースプロキシを示しています。



Cisco Catalyst SD-WAN のシングルテナント展開とマルチテナント展開の両方でリバースプロキシを展開できます。TLOC は、パブリックまたはプライベート TLOC に関係なく、パブリック IP アドレスとポートでリバースプロキシと通信します。

プライベートネットワークとパブリックインターネット接続の両方によるデバイスのサポート

次の複数の TLOC を持つデバイスを含む Cisco Catalyst SD-WAN ネットワークでは、リバースプロキシを使用できます。

- インターネットアクセスなしで内部のプライベートネットワークに接続する TLOC、および
- パブリックインターネットに接続する TLOC

このシナリオには、各 Cisco SD-WAN コントローラ の TLOC カラーを設定するための特定の要件があります。次の表では、この特殊なケースについて説明します。比較のために、TLOC が1つのみのデバイスと、プライベートネットワーク用とパブリックインターネット用に個別の TLOC があるデバイスの例を示しています。

表 2: TLOC カラーの要件

デバイス	TLOC	TLOC 接続	この TLOC カラーの設定	この Cisco SD-WAN Validator へのデバイスの接続	接続先 : Cisco SD-WAN コントローラ、および Cisco SD-WAN Manager	特定の TLOC カラー要件
A	1	内部プライベートネットワーク	プライベートの色 例 : private1	プライベートネットワークを介して到達可能な Cisco SD-WAN Validator	プライベートネットワークを介した直接接続	なし
B	1	パブリックインターネット	パブリックの色 例 : custom1	パブリックインターネットを介して到達可能な Cisco SD-WAN Validator	リバースプロキシを介した接続	なし

デバイス	TLOC	TLOC 接続	この TLOC カラーの設定	この Cisco SD-WAN Validator へのデバイスの接続	接続先 : Cisco SD-WAN コントローラ、および Cisco SD-WAN Manager	特定の TLOC カラー要件
C	1	内部プライベートネットワーク	プライベートネットワークの色 例 : private1	プライベートネットワークを介して到達可能な Cisco SD-WAN Validator	プライベートネットワークを介した直接接続	ここに示すように複数の TLOC を持つデバイスを含むネットワークには、次の特定の要件があります。 プライベートネットワークに使用しているプライベートの色を使用して、各 Cisco SD-WAN コントローラの TLOC を設定する。TLOC カラーをデフォルトのままにしない。 Cisco SD-WAN コントローラの TLOC カラーをデフォルトの色のままにすると次の問題が発生します : デバイス C などの内部プライベートネットワークに接続する TLOC を持つデバイスが Cisco SD-WAN コントローラに接続できない。
	2	パブリックインターネット	パブリックの色 例 : custom1	パブリックインターネットを介して到達可能な Cisco SD-WAN Validator	リバースプロキシを介した接続	

リバースプロキシに関する制約事項

• マルチテナントのシナリオ

マルチテナント Cisco Catalyst SD-WAN オーバーレイネットワークでは、3 ノード Cisco SD-WAN Manager クラスタのみでリバースプロキシデバイスを展開できます。

- TLS ベースのコントロールプレーン

リバースプロキシの展開は、Cisco SD-WAN Manager および Cisco SD-WAN コントローラの TLS ベースのコントロールプレーンでのみサポートされます。

- Cisco vEdge 5000 ルータの制限

Cisco vEdge 5000 ルータではリバースプロキシを展開できません。

- IPv6

IPv6 制御接続ではリバースプロキシを展開できません。

- プライベート WAN 用の TLOC を備えたデバイス

次の制限は、(a) 1 つ以上のデバイスがプライベート WAN に接続するための TLOC を持ち、(b) 1 つ以上の Cisco SD-WAN Validator がリバースプロキシに到達できないシナリオで、エッジデバイスに適用されます。

このシナリオでは、ゼロタッチプロビジョニング (ZTP) オンボーディングは、デフォルトの TLOC カラーを使用した TLOC での Cisco IOS XE Catalyst SD-WAN デバイスのオンボーディングをサポートしていません。デフォルト以外の TLOC カラーを設定する最小限の設定でデバイスをブートストラップします。

リバースプロキシでの証明書のプロビジョニング

トラフィックを交換する前に、リバースプロキシと WAN エッジデバイスの相互認証が必要です。

リバースプロキシでは、Cisco SD-WAN コントローラの証明書に署名した CA によって署名された証明書をプロビジョニングする必要があります。この証明書は、WAN エッジデバイスを検証するためにリバースプロキシによって使用されます。

リバースプロキシの証明書署名要求 (CSR) を生成し、シスコが署名するようにするには、次の手順を実行します。

1. リバースプロキシで次のコマンドを実行します。

```
proxy$ openssl req -new -days 365 -newkey rsa:2048 -nodes -keyout Proxy.key -out Proxy.csr
```

プロンプトが表示されたら、次の表に示されている値を入力します。

プロパティ	説明
Country Name (2 letter code)	任意の国コード。 例：US
State or Province Name	任意の州または都道府県。 例：CA

プロパティ	説明
Locality Name	任意の地域。 例：San Jose
Organization Name	「vIPTela Inc」または「Viptela LLC」のいずれかを使用してください。 Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a から、エンタープライズ証明書の組織名として「Cisco Systems」文字列を使用できます。 Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降、ブートストラップ設定ファイルの [Organization Name] フィールドにカンマを含めることはできません。 例：Viptela LLC
Organizational Unit Name	オーバーレイで設定した「組織」の名前を使用します。 例：cisco-sdwan-12345
Common Name	「.viptela.com」で終わるホスト名。 例：proxy.viptela.com
Email Address	任意の有効な電子メールアドレスを使用します。 例：someone@example.com

2. CSR がシスコによって署名されます。

- Cisco SD-WAN コントローラの CA として Symantec/Digicert を使用する場合は、Cisco TAC で CSR の署名のためのケースを開きます。
- Cisco SD-WAN コントローラの CA として Cisco Public Key Infrastructure (PKI) を使用する場合は、Cisco ネットワーク プラグ アンド プレイ (PnP) アプリケーションで CSR を送信し、署名付き証明書を取得します。

Cisco SD-WAN Manager を使用したリバースプロキシの設定

リバースプロキシの設定

1. Cisco SD-WAN Manager のメニューで、**[Administration] > [Settings]** の順に選択します。
2. **[Reverse Proxy]** 設定で、**[Edit]** をクリックします。

3. [Enable Reverse Proxy] で、[Enabled] をクリックします。
4. [Save] をクリックします。

Cisco SD-WAN コントローラでのリバースプロキシの設定

1. Cisco SD-WAN Manager のメニューから、[Configure] > [Devices] の順に選択します。
2. [Controllers] をクリックします。



(注) Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降、Cisco Catalyst SD-WAN のブランド変更との一貫性を保つために、[Controllers] タブの名前が [Control Components] タブに変更されました。

3. 目的の Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ で [...] をクリックして、[Add Reverse Proxy] をクリックします。

[Add Reverse Proxy] ダイアログボックスが表示されます。

4. プライベート IP アドレスとポート番号をプロキシ IP アドレスとポート番号にマッピングするには、次の手順を実行します。
 1. [Add Reverse Proxy] をクリックします。
 2. 次の詳細を入力します。

プライベート IP	プライベート IP アドレスは、VPN0 のトランスポートインターフェイスの IP アドレスです。
プライベートポート	これは、オーバーレイネットワークでトラフィックの制御と処理を行う接続を確立するために使用されるポートです。デフォルトポート番号は、12346 です。
プロキシ IP	プライベート IP アドレスをマップする必要があるプロキシ IP アドレス。
プロキシポート	プライベートポートをマップする必要があるプロキシポート。

3. Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ に複数のコアがある場合は、コアごとに手順 4a と手順 4b を繰り返します。
5. プライベート IP アドレスとポート番号からプロキシ IP アドレスとポート番号へのマッピングを削除するには、マッピングを探してごみ箱アイコンをクリックします。
6. リバースプロキシ設定を保存するには、[Add] をクリックします。
設定を破棄するには、[Cancel] をクリックします。

7. Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ にアタッチされたセキュリティ機能テンプレートで、トランスポートプロトコルとして TLS を選択します。

Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ でリバースプロキシを設定すると、オーバーレイネットワーク内の WAN エッジデバイスは、リバースプロキシでの認証用の証明書を使用してプロビジョニングされます。

1. リバースプロキシが展開されると、Cisco SD-WAN Validator はリバースプロキシの詳細を WAN エッジデバイスと共有します。
2. リバースプロキシについて学習した WAN エッジデバイスは、Cisco SD-WAN Manager から署名付き証明書のインストールを開始します。
3. 証明書がインストールされると、WAN エッジデバイスはその証明書を使用してリバースプロキシを認証し、リバースプロキシに接続します。

リバースプロキシの無効化



(注) リバースプロキシを無効にする前に、Cisco SD-WAN Manager インスタンスおよび Cisco SD-WAN コントローラ に対して設定したプライベート IP アドレスとポート番号からプロキシ IP アドレスとポート番号へのマッピングを削除します。マッピングの削除については、「Configure Reverse Proxy Settings on Cisco Catalyst SD-WAN Controllers」を参照してください。

1. Cisco SD-WAN Manager のメニューで、[Administration] > [Settings] の順に選択します。
2. [Reverse Proxy] 設定で、[Edit] をクリックします。
3. [Enable Reverse Proxy] で、[Disabled] をクリックします。
4. [Save] をクリックします。

CLI を使用したリバースプロキシの監視

Cisco SD-WAN コントローラでの WAN エッジデバイスのプライベートおよびプロキシ IP アドレスとポート番号の監視

次に、Cisco SD-WAN コントローラ での **show control connections** コマンドの出力例を示します。WAN エッジデバイスの場合、コマンド出力の [PEER PRIVATE IP] および [PEER PRIVATE PORT] 列のエントリは、設定された TLOC IP アドレスと WAN エッジインターフェイスのポート番号です。[PEER PUBLIC IP] および [PEER PUBLIC PORT] 列のエントリは、リバースプロキシインターフェイスの対応する IP アドレスとポート番号です。同じコマンドを Cisco SD-WAN Manager インスタンスで実行した場合も、同様の出力が得られます。


```
vsmart1# show control connections
```

PEER								PEER	
PUB	PEER	PEER	PEER	SITE	DOMAIN	PEER	PRIV	PEER	
INDEX	TYPE	PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	
PORT	ORGANIZATION	REMOTE	COLOR	STATE	UPTIME		PORT	PUBLIC	
								IP	
0	vbond	dtls	172.16.1.2	0		0	10.1.1.2	12346	
12346	EXAMPLE-ORG	default		up	53:08:18:50			10.1.1.2	
0	vmanage	tls	172.16.1.6	1		0	10.2.100.6	45689	
45689	EXAMPLE-ORG	default		up	53:08:18:32			10.2.100.6	
1	vedge	tls	1.1.100.1	100		1	10.3.1.2	57853	
53624	EXAMPLE-ORG	biz-internet		up	53:08:18:44			10.2.100.1	
1	vedge	tls	1.1.101.1	101		1	10.4.1.2	55411	
53622	EXAMPLE-ORG	biz-internet		up	53:08:18:48			10.2.100.1	
1	vbond	dtls	172.16.1.2	0		0	10.1.1.2	12346	
12346	EXAMPLE-ORG	default		up	53:08:18:51			10.1.1.2	

SD-WAN コントローラのプライベート IP アドレスとポート番号から Cisco SD-WAN Validator のプロキシ IP アドレスとポート番号へのマッピングの表示

次に、Cisco SD-WAN Validator での **show orchestrator reverse-proxy-mapping** コマンドの出力例を示します。コマンド出力の [PROXY IP] 列と [PROXY PORT] 列のエントリは、プロキシの IP アドレスとポート番号です。[PRIVATE IP] 列と [PRIVATE PORT] 列のエントリは、VPN 0 のトランスポートインターフェイスのプライベート IP アドレスとポート番号です。

```
vbond# show orchestrator reverse-proxy-mapping
```

	PRIVATE			PROXY
UUID	PRIVATE IP	PORT	PROXY IP	PORT

14c35ae4-69e3-41c5-a62f-725c839d25df	10.2.100.4	23456	10.2.1.10	23458
14c35ae4-69e3-41c5-a62f-725c839d25df	10.2.100.4	23556	10.2.1.10	23558
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23456	10.2.1.10	23457
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23556	10.2.1.10	23557
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23656	10.2.1.10	23657
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23756	10.2.1.10	23757
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23856	10.2.1.10	23857
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23956	10.2.1.10	23957
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	24056	10.2.1.10	24057
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	24156	10.2.1.10	24157
vbond#				

例：SD-WAN コントローラのプライベート IP アドレスとポート番号から WAN エッジデバイスのプロキシ IP アドレスとポート番号へのマッピングを表示する

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan control connections** コマンドの出力例を示します。コマンド出力で、Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ の [PROXY] 列のエントリを確認します。エントリが [Yes] の場合、[PEER PUBLIC IP] および [PEER PUBLIC PORT] のエントリはプロキシ IP アドレスとポート番号です。

Device# **show sdwan control connections**

				CONTROLLER		PEER		PEER	
PEER	PEER	PEER		SITE	DOMAIN	PEER	PRIV	PEER	PUB
				GROUP					
TYPE	PROT	SYSTEM IP	ID	ID	PRIVATE	IP	PORT	PUBLIC IP	PORT
ORGANIZATION		LOCAL COLOR	PROXY	STATE	UPTIME	ID			
vsmart	tls	172.16.1.4	1	1	10.2.100.4	23558	10.2.1.10	23558	
EXAMPLE-ORG		biz-internet	Yes	up	52:08:44:25 0				
vbond	dtls	0.0.0.0	0	0	10.1.1.2	12346	10.1.1.2	12346	
EXAMPLE-ORG		biz-internet	-	up	52:08:50:47 0				
vmanage	tls	172.16.1.6	1	0	10.2.100.6	23957	10.2.1.10	23957	
EXAMPLE-ORG		biz-internet	Yes	up	66:03:04:50 0				

Device#

Cisco vEdge デバイス では、**show control connections** コマンドを実行して同様の出力を取得できます。

リバースプロキシとの認証のために WAN エッジデバイスにインストールされた署名付き証明書の表示

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan certificate reverse-proxy** コマンドの出力例を示します。

Device# **show sdwan certificate reverse-proxy**

Reverse proxy certificate

Certificate:

Data:

Version: 1 (0x0)

```
Serial Number: 1 (0x1)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = US, CN = 6c63e80a-8175-47de-a455-53a127ee70bd, O = Viptela

Validity

    Not Before: Jun  2 19:31:08 2021 GMT

    Not After : May 27 19:31:08 2051 GMT

Subject: C = US, ST = California, CN = C8K-9AE4A5A8-4EB0-E6C1-1761-6E54E4985F78,
O = ViptelaClient
Subject Public Key Info:

    Public Key Algorithm: rsaEncryption

        RSA Public-Key: (2048 bit)

        Modulus:

            00:e2:45:49:53:3a:56:d4:b8:70:59:90:01:fb:b1:
            44:e3:73:17:97:a3:e9:b7:55:44:d4:2d:dd:13:4a:
            a8:ef:78:14:9d:bd:b5:69:de:c9:31:29:bd:8e:57:
            09:f2:02:f8:3d:1d:1e:cb:a3:2e:94:c7:2e:61:ea:
            e9:94:3b:28:8d:f7:06:12:56:f3:24:56:8c:4a:e7:
            01:b1:2b:1b:cd:85:4f:8d:34:78:78:a1:26:17:2b:
            a5:1b:2a:b6:dd:50:51:f8:2b:13:93:cd:a6:fd:f8:
            71:95:c4:db:fc:a7:83:05:23:68:61:15:05:cc:aa:
            60:af:09:ef:3e:ce:70:4d:dd:50:84:3c:9a:57:ce:
            cb:15:84:3e:cd:b2:b6:30:ab:86:68:17:94:fa:9c:
            1a:ab:28:96:68:8c:ef:c8:f7:00:8a:7a:01:ca:58:
            84:b0:87:af:9a:f6:13:0f:aa:42:db:8b:cc:6e:ba:
            c8:c1:48:d2:f4:d8:08:b1:b5:15:ca:36:80:98:47:
            32:3a:df:54:35:fe:75:32:23:9f:b5:ed:65:41:99:
            50:b9:0f:7a:a2:10:59:12:d8:3e:45:78:cb:dc:2a:
            95:f2:72:02:1a:a6:75:06:87:52:4d:01:17:f2:62:
            8c:40:ad:29:e4:75:17:04:65:a9:b9:6a:dd:30:95:
            34:9b

        Exponent: 65537 (0x10001)

Signature Algorithm: sha256WithRSAEncryption

99:40:af:23:bb:cf:7d:59:e9:a5:83:78:37:02:76:83:79:02:
```

```

b3:5c:56:e8:c3:aa:fc:78:ef:07:23:f8:14:19:9c:a4:5d:88:

07:4d:6e:b8:0d:b5:af:fa:5c:f9:55:d0:60:94:d9:24:99:5e:
33:06:83:03:c3:73:c1:38:48:45:ba:6a:35:e6:e1:51:0e:92:

c3:a2:4a:a2:e1:2b:da:cd:0c:c3:17:ef:35:52:e1:6a:23:20:

af:99:95:a2:cb:99:a7:94:03:f3:78:99:bc:76:a3:0f:de:04:

7d:35:e1:dc:4d:47:79:f4:c8:4c:19:df:80:4c:4f:15:ab:f1:

61:a2:78:7a:2b:6e:98:f6:7b:8f:d6:55:44:16:79:e3:cd:51:

0e:27:fc:e6:4c:ff:bb:8f:2d:b0:ee:ed:98:63:e9:c9:cf:5f:

d7:b1:dd:7b:19:32:22:94:77:d5:bc:51:85:65:f3:e0:93:c7:

3c:79:fc:34:c7:9f:40:dc:b1:fc:6c:e5:3d:af:2d:77:b7:c3:

88:b3:89:7c:a6:1f:56:35:3b:35:66:0c:c8:05:b5:28:0b:98:

19:c7:b0:8e:dc:b7:3f:9d:c1:bb:69:f0:7d:20:95:b5:d1:f0:

06:35:b7:c4:64:ba:c4:95:31:4a:97:03:0f:04:54:6d:cb:50:

2f:31:02:59

```

Device#

Cisco vEdge デバイス では、**show certificate reverse-proxy** コマンドを実行して同様の出力を取得できます。

CLI を使用したリバースプロキシの監視

Cisco SD-WAN コントローラでの WAN エッジデバイスのプライベートおよびプロキシ IP アドレスとポート番号の監視

次に、Cisco SD-WAN コントローラ での **show control connections** コマンドの出力例を示します。WAN エッジデバイスの場合、コマンド出力の [PEER PRIVATE IP] および [PEER PRIV PORT] 列のエントリは、設定された TLOC IP アドレスと WAN エッジインターフェイスのポート番号です。[PEER PUBLIC IP] および [PEER PUB PORT] 列のエントリは、リバース プロキシ インターフェイスの対応する IP アドレスとポート番号です。同じコマンドを Cisco SD-WAN Manager インスタンスで実行した場合も、同様の出力が得られます。

vsmart1# **show control connections**

										PEER
PEER	PEER	PEER	PEER		SITE	DOMAIN	PEER	PRIV	PEER	
PUB										
INDEX	TYPE	PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	PORT	PUBLIC
PORT	ORGANIZATION		REMOTE	COLOR	STATE	UPTIME				IP
0	vbond	dtls	172.16.1.2		0	0	10.1.1.2	12346	10.1.1.2	
12346	EXAMPLE-ORG		default		up	53:08:18:50				

```

0      vmanage tls 172.16.1.6      1      0      10.2.100.6 45689 10.2.100.6
45689  EXAMPLE-ORG default      up      53:08:18:32
1      vedge  tls 1.1.100.1      100    1      10.3.1.2 57853 10.2.100.1
53624  EXAMPLE-ORG biz-internet up      53:08:18:44
1      vedge  tls 1.1.101.1      101    1      10.4.1.2 55411 10.2.100.1
53622  EXAMPLE-ORG biz-internet up      53:08:18:48
1      vbond  dtls 172.16.1.2      0      0      10.1.1.2 12346 10.1.1.2
12346  EXAMPLE-ORG default      up      53:08:18:51

vsmart1#

```

SD-WAN コントローラのプライベート IP アドレスとポート番号から Cisco SD-WAN Validator のプロキシ IP アドレスとポート番号へのマッピングの表示

次に、Cisco SD-WAN Validator での **show orchestrator reverse-proxy-mapping** コマンドの出力例を示します。コマンド出力の [PROXY IP] 列と [PROXY PORT] 列のエントリは、プロキシの IP アドレスとポート番号です。[PRIVATE IP] 列と [PRIVATE PORT] 列のエントリは、VPN 0 のトランスポート インターフェイスのプライベート IP アドレスとポート番号です。

```
vbond# show orchestrator reverse-proxy-mapping
```

	PRIVATE		PROXY	
UUID	PRIVATE IP	PORT	PROXY IP	PORT

14c35ae4-69e3-41c5-a62f-725c839d25df	10.2.100.4	23456	10.2.1.10	23458
14c35ae4-69e3-41c5-a62f-725c839d25df	10.2.100.4	23556	10.2.1.10	23558
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23456	10.2.1.10	23457
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23556	10.2.1.10	23557
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23656	10.2.1.10	23657
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23756	10.2.1.10	23757
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23856	10.2.1.10	23857
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	23956	10.2.1.10	23957
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	24056	10.2.1.10	24057
6c63e80a-8175-47de-a455-53a127ee70bd	10.2.100.6	24156	10.2.1.10	24157

```
vbond#
```

例：SD-WAN コントローラのプライベート IP アドレスとポート番号から WAN エッジデバイスのプロキシ IP アドレスとポート番号へのマッピングを表示する

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan control connections** コマンドの出力例を示します。コマンド出力で、Cisco SD-WAN Manager インスタンスまたは Cisco SD-WAN コントローラ の [PROXY] 列のエントリを確認します。エントリが [Yes] の場

合、[PEER PUBLIC IP] および [PEER PUBLIC PORT] のエントリはプロキシ IP アドレスとポート番号です。

Device# **show sdwan control connections**

				CONTROLLER		PEER		PEER	
PEER	PEER	PEER		SITE	DOMAIN	PEER	PRIV	PEER	PUB
				GROUP					
TYPE	PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	PORT	PUBLIC
ORGANIZATION		LOCAL	COLOR	PROXY	STATE	UPTIME	ID		IP
vsmart	tls	172.16.1.4		1	1	10.2.100.4		23558	10.2.1.10
EXAMPLE-ORG		biz-internet		Yes	up	52:08:44:25	0		23558
vbond	dtls	0.0.0.0		0	0	10.1.1.2		12346	10.1.1.2
EXAMPLE-ORG		biz-internet		-	up	52:08:50:47	0		12346
vmanage	tls	172.16.1.6		1	0	10.2.100.6		23957	10.2.1.10
EXAMPLE-ORG		biz-internet		Yes	up	66:03:04:50	0		23957

Device#

Cisco vEdge デバイス では、**show control connections** コマンドを実行して同様の出力を取得できます。

リバースプロキシとの認証のために **WAN** エッジデバイスにインストールされた署名付き証明書の表示

次に、Cisco IOS XE Catalyst SD-WAN デバイス での **show sdwan certificate reverse-proxy** コマンドの出力例を示します。

Device# **show sdwan certificate reverse-proxy**

Reverse proxy certificate

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 1 (0x1)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = US, CN = 6c63e80a-8175-47de-a455-53a127ee70bd, O = Viptela

Validity

```
Not Before: Jun  2 19:31:08 2021 GMT
Not After  : May 27 19:31:08 2051 GMT

Subject: C = US, ST = California, CN = C8K-9AE4A5A8-4EB0-E6C1-1761-6E54E4985F78,
O = ViptelaClient
Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

    00:e2:45:49:53:3a:56:d4:b8:70:59:90:01:fb:b1:
    44:e3:73:17:97:a3:e9:b7:55:44:d4:2d:dd:13:4a:
    a8:ef:78:14:9d:bd:b5:69:de:c9:31:29:bd:8e:57:
    09:f2:02:f8:3d:1d:1e:cb:a3:2e:94:c7:2e:61:ea:
    e9:94:3b:28:8d:f7:06:12:56:f3:24:56:8c:4a:e7:
    01:b1:2b:1b:cd:85:4f:8d:34:78:78:a1:26:17:2b:
    a5:1b:2a:b6:dd:50:51:f8:2b:13:93:cd:a6:fd:f8:
    71:95:c4:db:fc:a7:83:05:23:68:61:15:05:cc:aa:
    60:af:09:ef:3e:ce:70:4d:dd:50:84:3c:9a:57:ce:
    cb:15:84:3e:cd:b2:b6:30:ab:86:68:17:94:fa:9c:
    1a:ab:28:96:68:8c:ef:c8:f7:00:8a:7a:01:ca:58:
    84:b0:87:af:9a:f6:13:0f:aa:42:db:8b:cc:6e:ba:
    c8:c1:48:d2:f4:d8:08:b1:b5:15:ca:36:80:98:47:
    32:3a:df:54:35:fe:75:32:23:9f:b5:ed:65:41:99:
    50:b9:0f:7a:a2:10:59:12:d8:3e:45:78:cb:dc:2a:
    95:f2:72:02:1a:a6:75:06:87:52:4d:01:17:f2:62:
    8c:40:ad:29:e4:75:17:04:65:a9:b9:6a:dd:30:95:
    34:9b

Exponent: 65537 (0x10001)

Signature Algorithm: sha256WithRSAEncryption

    99:40:af:23:bb:cf:7d:59:e9:a5:83:78:37:02:76:83:79:02:
    b3:5c:56:e8:c3:aa:fc:78:ef:07:23:f8:14:19:9c:a4:5d:88:
    07:4d:6e:b8:0d:b5:af:fa:5c:f9:55:d0:60:94:d9:24:99:5e:
    33:06:83:03:c3:73:c1:38:48:45:ba:6a:35:e6:e1:51:0e:92:
    c3:a2:4a:a2:e1:2b:da:cd:0c:c3:17:ef:35:52:e1:6a:23:20:
```

```
af:99:95:a2:cb:99:a7:94:03:f3:78:99:bc:76:a3:0f:de:04:
7d:35:e1:dc:4d:47:79:f4:c8:4c:19:df:80:4c:4f:15:ab:f1:
61:a2:78:7a:2b:6e:98:f6:7b:8f:d6:55:44:16:79:e3:cd:51:
0e:27:fc:e6:4c:ff:bb:8f:2d:b0:ee:ed:98:63:e9:c9:cf:5f:
d7:b1:dd:7b:19:32:22:94:77:d5:bc:51:85:65:f3:e0:93:c7:
3c:79:fc:34:c7:9f:40:dc:b1:fc:6c:e5:3d:af:2d:77:b7:c3:
88:b3:89:7c:a6:1f:56:35:3b:35:66:0c:c8:05:b5:28:0b:98:
19:c7:b0:8e:dc:b7:3f:9d:c1:bb:69:f0:7d:20:95:b5:d1:f0:
06:35:b7:c4:64:ba:c4:95:31:4a:97:03:0f:04:54:6d:cb:50:
2f:31:02:59
```

Device#

Cisco vEdge デバイス では、**show certificate reverse-proxy** コマンドを実行して同様の出力を取得できます。

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。