VPN リモート オフィス/スポークのゼロタッチ展開（ZTD）の設定例

目次

概要

リモート オフィス ルータ（スポークとも呼ばれます）をセキュアかつ効率的に導入してプロビジョニングするのは困難なタスクです。 リモート オフィスは、オンサイトでルータを設定するためにフィールド エンジニアを派遣するのが難しい場所にある場合があり、ほとんどのエンジニアは、コストと潜在的セキュリティ リスクを理由に、事前設定されたスポーク ルータを送らないことを選択します。 このドキュメントでは、そのような導入にはゼロ タッチ導入（ZTD）オプションがコスト効率の良いスケーラブルなソリューションでなる理由を説明します。

前提条件

要件

- USB フラッシュ ドライブをサポートする USB ポート搭載の Cisco IOS® ルータ。 詳細については、『USB eToken および USB フラッシュ機能のサポート』を参照してください。
- この機能は、ほぼすべての Cisco 8xx プラットフォームで有効であることが確認されています。 詳細については、デフォルト設定ファイルに関するホワイト ペーパー（Cisco 800 シリーズ ISR での機能サポート）を参照してください。
- サービス統合型ルータ（ISR）シリーズ G2 および 43xx/44xx など、USB ポートを備えたその他のプラットフォーム。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

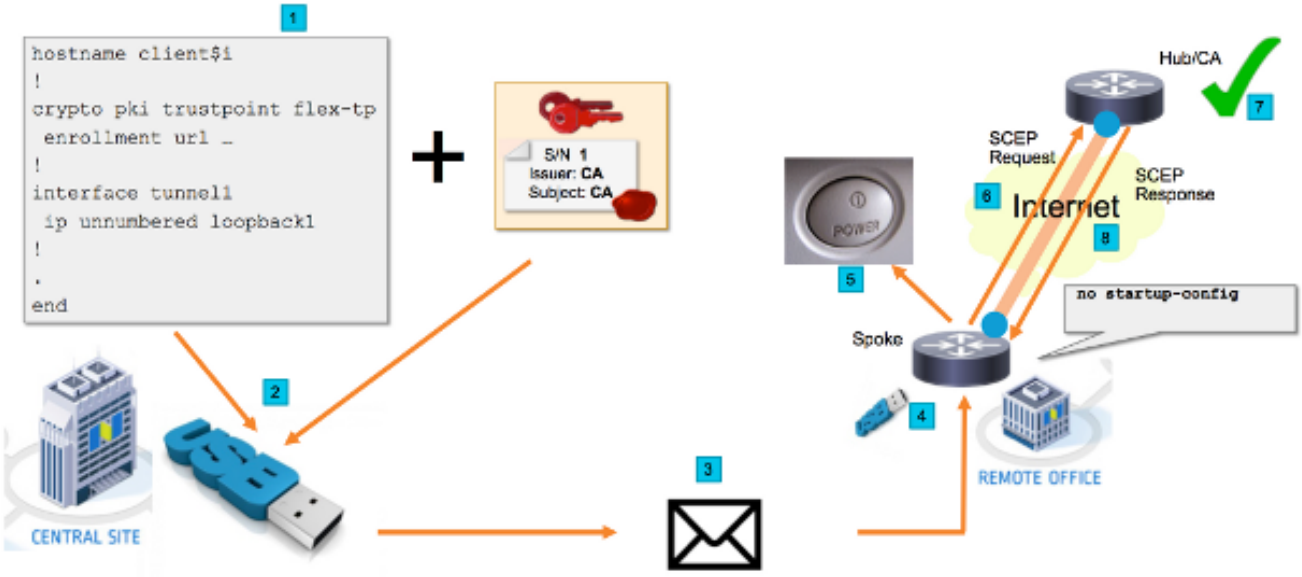
- Simple Certificate Enrollment Protocol（SCEP）
- USB によるゼロ タッチ導入
- DMVPN/FlexVPN/サイト間 VPN

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図



ネットワーク フロー

1. セントラル サイト（企業の本社）でスポーク設定テンプレートが作成されます。 テンプレートには、VPN ハブ ルータの証明書に署名した認証局（CA）の証明書が含まれています。
2. 設定テンプレートが、**ciscortr.cfg** というファイル内の USB キーでインスタンス化されます。 この設定ファイルには、導入対象のルータにスポーク固有の設定が含まれます。 **注:** USB での設定には、IP アドレスと CA 証明書以外の機密情報は含まれません。 スポークまたは CA サーバの秘密キーはありません。
3. USB フラッシュ ドライブがリモート オフィスにメールまたはパッケージ配送会社によって送られます。
4. スポーク ルータは、シスコの製造部門からリモート オフィスに直接配送されることもあります。
5. リモート オフィスで、USB フラッシュ ドライブと同梱されている説明に従って、ルータを電源に接続し、ネットワークにケーブル接続します。 次に、USB フラッシュ ドライブをル

ータに挿入します。 **注:** このステップには技術的スキルはほとんど、またはまったく必要ないため、任意の担当者が簡単に行うことができます。

6. ルータが起動すると、**usbflash0:/ciscortr.cfg** から設定が読み込まれます。 ルータの電源がオンになると同時に、Simple Certificate Enrollment Protocol（SCEP）要求が CA サーバに送信されます。
7. CA サーバ上には、企業のセキュリティ ポリシーに基づく手動または自動権限付与を設定できます。 証明書の手動権限付与を設定する場合は、SCEP 要求のアウトオブバンド検証を実行する必要があります（IP アドレスの有効性チェック、導入担当者のクレデンシャル検証など）。 このステップは、使用する CA サーバによって異なる場合があります。
8. 証明書が有効であることが確認されて、スポーク ルータが SCEP 応答を受信すると、IKE セッションで VPN ハブに対する認証が行われて、トンネルが正常に確立されます。

設定/テンプレート

以下の出力例に、フラッシュ ドライブの **usbflash0:/ciscortr.cfg** ファイルに格納された FlexVPN リモート オフィスの設定例を示します。

```
hostname client1
!
interface GigabitEthernet0
 ip address dhcp
!
crypto pki trustpoint client1
! CA Server's URL
 enrollment url http://10.122.162.242:80
! These fields needs to be filled, to avoid prompt while doing enroll
serial-number none
 ip-address none
 password
 subject-name cn=client1.cisco.com ou=cisco ou
!
crypto pki certificate chain client1
 certificate ca 01
 ! CA Certificate here
       quit
!
crypto ikev2 profile default
 match identity remote any
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint client1
 aaa authorization group cert list default default
!
interface Tunnel1
 ip unnumbered GigabitEthernet0
 tunnel source GigabitEthernet0
 tunnel mode ipsec ipv4
! Destination is Internet IP Address of VPN Hub
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default
!
event manager applet import-cert
! Start importing certificates only after 60s after bootup
! Just to give DHCP time to boot up
 event timer watchdog time 60
 action 1.0 cli command "enable"
 action 2.0 cli command "config terminal"
! Enroll spoke's certificate
```

```
 action 3.0 cli command "crypto pki enroll client1"
! After enrollement request is sent, remove that EEM script
 action 4.0 cli command "no event manager applet import-cert"
 action 5.0 cli command "exit"
event manager applet write-mem
 event syslog pattern "PKI-6-CERTRET"
 action 1.0 cli command "enable"
 action 2.0 cli command "write memory"
 action 3.0 syslog msg "Automatically saved configuration"
```

確認

ここでは、設定が正常に動作していることを確認します。

特定の show コマンドがアウトプット インタープリタ ツール (登録ユーザ専用) でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

トンネルが確立されたかどうかは、スポークで確認できます。

```
client1#show crypto session
Crypto session current status

Interface: Tunnel1
Profile: default
Session status: UP-ACTIVE
Peer: 172.16.0.2 port 500
 Session ID: 1
 IKEv2 SA: local 172.16.0.1/500 remote 172.16.0.2/500 Active
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map
```

また、証明書が正常に登録されているかどうかも、スポークで確認することができます。

```
client1#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
  Subject:
    Name: client1
    hostname=client1
    cn=client1.cisco.com ou=cisco ou
  Validity Date:
    start date: 01:34:34 PST Apr 26 2015
    end   date: 01:34:34 PST Apr 25 2016
  Associated Trustpoints: client1
  Storage: nvram:CA#6.cer

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=CA
 Subject:
   cn=CA
 Validity Date:
   start date: 01:04:46 PST Apr 26 2015
   end   date: 01:04:46 PST Apr 25 2018
```

```
 Associated Trustpoints: client1
 Storage: nvram:CA#1CA.cer
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

既知の注意事項と問題

Cisco Bug ID CSCuu93989 - G2 プラットフォームでの設定ウィザードの PnP 停止フローによって、usbflash: /ciscortr.cfg から設定がロードされない場合があります。 代わりに、次の設定ウィザード機能でシステムが停止します。

```
client1#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
  Subject:
    Name: client1
    hostname=client1
    cn=client1.cisco.com ou=cisco ou
  Validity Date:
    start date: 01:34:34 PST Apr 26 2015
    end   date: 01:34:34 PST Apr 25 2016
  Associated Trustpoints: client1
  Storage: nvram:CA#6.cer

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=CA
 Subject:
   cn=CA
 Validity Date:
   start date: 01:04:46 PST Apr 26 2015
   end   date: 01:04:46 PST Apr 25 2018
 Associated Trustpoints: client1
 Storage: nvram:CA#1CA.cer
```

必ず、この問題に対する修正が含まれるバージョンを使用してください。

USB による ZTD とデフォルト設定ファイルによる ZTD の違い

このドキュメントで使用した**デフォルト設定ファイル**機能は、**USB によるゼロ タッチ導入**（『Cisco 800 シリーズ ISR 導入の概要』を参照）とは異なる機能です。

-	**USB によるゼロ タッチ導入**	**デフォルト設定ファイル**
サポート対象プラットフォーム	少数の 8xx ルータのみに限定されます。詳細については、『Cisco 800 シリーズ ISR 導入の概要』を参照してください。	すべての ISR G2、43xx および 44xx。

ファイル名	*.cfg	ciscortr.cfg
ローカル フラッシュへの設定の保存	はい。自動的に保存されます。	いいえ。Embeded Event Manager（EEM）が必要です。

デフォルト設定ファイル機能はより多くのプラットフォームでサポートされているため、このドキュメントではこの手法をソリューションとして紹介しました。

要約

USB のデフォルト設定（USB フラッシュ ドライブからのファイル名 **ciscortr.cfg** で）を使用することで、ネットワーク管理者はリモートの場所にあるデバイスにログインすることなく、リモート オフィス スポーク ルータ VPN（ただし、VPN だけに限られません）を導入できます。

関連情報

- Simple Certificate Enrollment Protocol（SCEP）
- USB によるゼロ タッチ導入
- DMVPN/FlexVPN/サイト間 VPN
- テクニカルサポートとドキュメント - Cisco Systems