目次

概要

リモートオフィスルータのセキュアおよび効率的な配備およびプロビジョニングするは（時々 Spokes と呼ばれる）難しい仕事である場合もあります。 リモートオフィスはそれがオンサイト ルータを設定してサービス 技術員にもらうチャレンジであるほとんどのエンジニアはコストおよび潜在的なセキュリティ リスクによる前もって構成されたスポークルータを送信 しないことを選択します場所にであるかもしれないし。 ゼロ タッチ配備（ZTD）オプションがそのような配備のための費用有効および拡張が容易なソリューションどのようにであるかこの資料に記述されています。

前提条件

要件

- USB フラッシュ ドライブをサポートする USBポートを備えている Cisco IOS® ルータ。 詳細については、USB および USB フラッシュ機能 サポートが eToken 参照して下さい。
- この機能はほとんど Cisco あらゆる 8xx プラットフォームで動作するために確認されます。詳細についてはデフォルトコンフィギュレーションファイル 白書（Cisco 800 シリーズ ISR の機能 サポート）を参照して下さい。
- 統合サービス ルータ（ISR）シリーズ G2 および 43xx/44xx のような USBポートを備えている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）

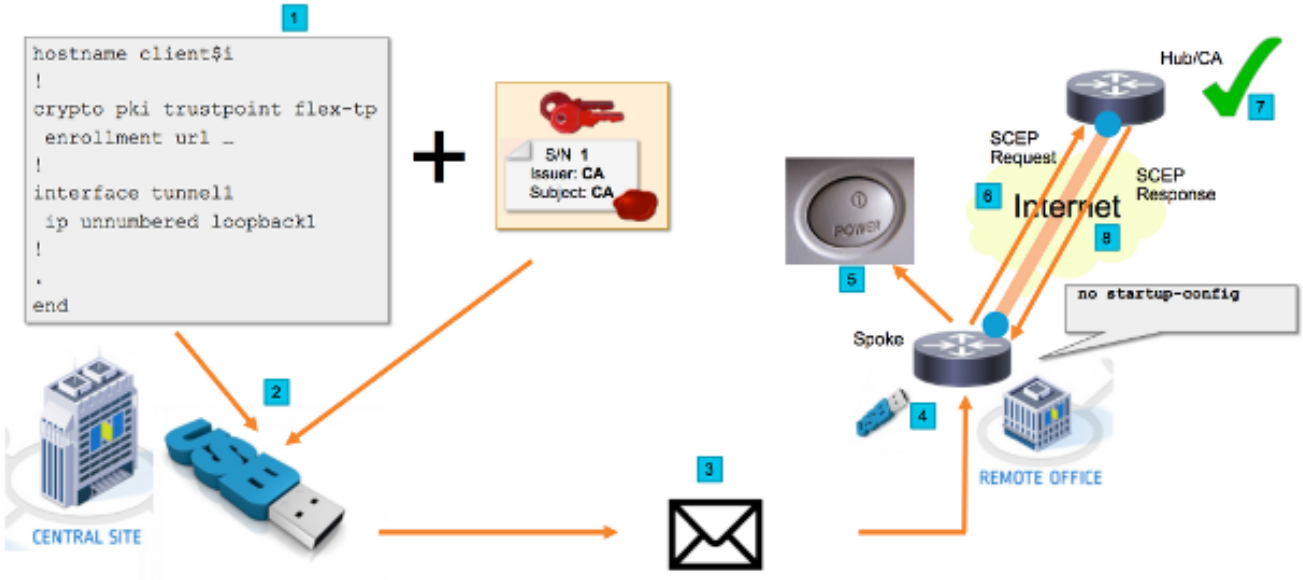
- USB によるゼロ タッチ配備
- DMVPN/FlexVPN/Site にサイト VPN

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 流 れ

1. セントラルサイト（会社の本部）でスポーク設定のテンプレートは作成されます。 テンプレートは VPN ハブルータの認証に署名した認証局 （CA） 認証が含まれています。
2. コンフィギュレーションテンプレートは ciscortr.cfg と呼ばれるファイルの USBキーでインスタンス化 されます。 このコンフィギュレーション ファイルは展開されるべきルータのためのスポーク特定の設定が含まれています。 **注** USB の設定は IP アドレスおよび CA 認証以外機密情報が含まれていません。 スポークまたは CA サーバのプライベートキーがありません。
3. USB フラッシュ ドライブはメールかパッケージ運送会社によってリモートオフィスに送信されます。
4. スポークルータはまた Cisco 製造からのリモートオフィスに直接送られます。
5. リモートオフィスでルータは動力を与えるために接続され、ネットワークに USB フラッシュ ドライブと含まれている手順で説明されているようにケーブル接続されます。 次に USB フラッシュ ドライブはルータに挿入されます。 **注** 少しはこのステップに関連する技術的なスキルへありません従ってあらゆるオフィス人員によって容易に実行されたことができます。

6. ルータが起動すれば usbflash0:/ciscortr.cfg からの設定を読みます。 ルータが CA サーバに Simple Certificate Enrollment Protocol （ SCEP ） 要求の上で送信 される動力を与えたらすぐ。
7. CA サーバ手動か自動許可で会社 セキュリティポリシーに基づいて設定することができます。 与える手動認証のために設定されたとき SCEP 要求のアウトオブバンド確認は実行された必要があります (配備を行う人員のための IP アドレス検証チェック、クレデンシャル検証、等)。 このステップは CA サーバ t 帽子に基づいて使用されます異なるかもしれません。
8. SCEP 応答が今有効な証明書を備えているスポークルータによって受け取られれば、IKE セッションは VPN ハブによって認証し、トンネルはうまく確立します。

コンフィギュレーション/テンプレート

usbflash0:/ciscortr.cfg ファイルにフラッシュ ドライブに置かれるこの出力例は模範的な FlexVPN リモートオフィス 設定を示します。

```
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。

トンネルが上がったかどうか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
```

認証が正しく登録されたかどうかまたスポークで確認できます:

```
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 バグ ID CSCuu93989 - G2 プラットフォームの構成ウィザード停止 PnP フローによりシステムは usbflash から設定をロードしますかもしれません: /ciscortr.cfg. その代りシステムは構成ウィザード 機能で停止するかもしれません:

```
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
```

使用をこの問題のための修正が含まれているバージョン約束して下さい。

USB による ZTD vs デフォルトコンフィギュレーションファイル

この資料が Cisco 800 シリーズ desribed **USB によってである**ゼロ接触 Deployement より別の機能 ISR 配置の外観で使用することデフォルトコンフィギュレーションファイルが特色になることに注目して下さい。

-	USB によってタッチ Deployement をゼロにして下さい	デフォルトコンフィギュレーションファ
サポート対象プラットフォーム	少数の 8xx ルータだけに制限される。詳細については、ISR 配置	すべての ISR G2、43xx および 44xx。

	の外観を Cisco 800 シリーズ参照して下さい	
ファイル名	*.cfg	ciscortr.cfg
ローカル フラッシュするで設定を保存します	はい、自動的に	いいえ、Embeded イベント マネージャ（EEM）必要となりました

より多くのプラットフォームが**デフォルトコンフィギュレーションファイル** 機能によってサポートされるので、このテクノロジーはこの技術情報で示されたソリューションのために選択されました。

要約

USB デフォルト 設定は（USB フラッシュ ドライブ**からの**ファイル名 **ciscortr.cfg** と）ネットワーク管理者に遠隔地のデバイスにログイン する必要なしでリモートオフィス スポークルータ VPN を（ちょうど VPN に制限されなくて）配置する機能を与えます。

関連情報

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