VPNリモートオフィス/スポークのゼロタッチ導入(ZTD)の設定

内容

概要

このドキュメントでは、ゼロタッチ導入(ZTD)オプションが導入のコスト効率と拡張性に優れたソリューションである仕組みについて説明します。

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。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 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、『Default Configuration Files White Paper（Cisco 800シリーズISR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いています。

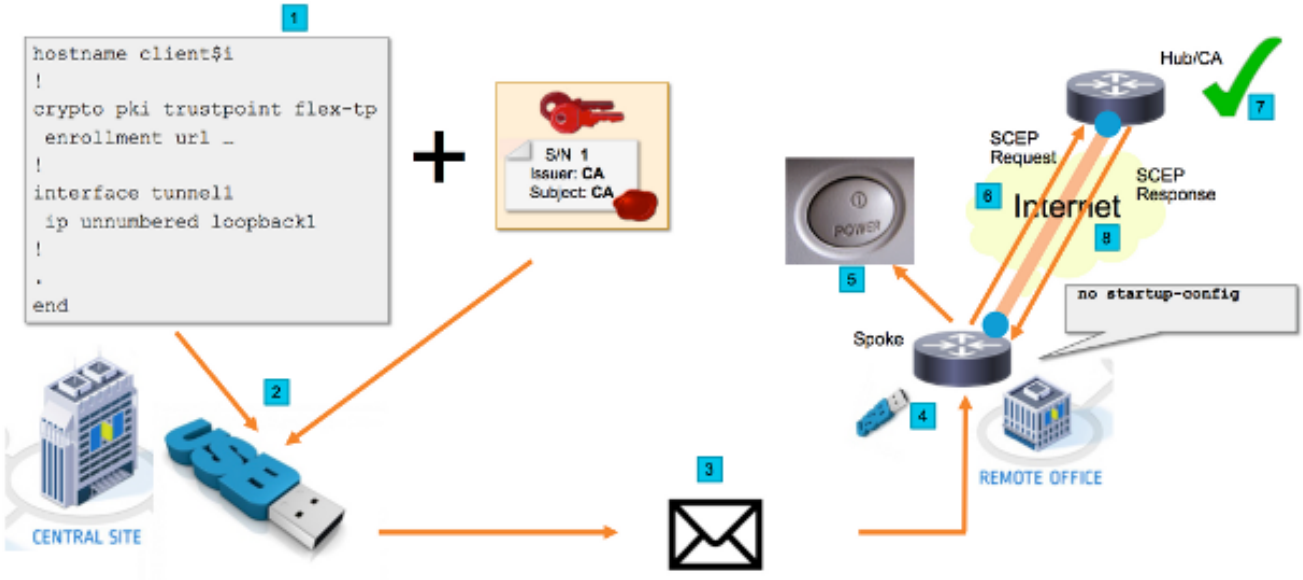
- Simple Certificate Enrollment Protocol（SCEP）
- USB によるゼロ タッチ導入
- DMVPN/FlexVPN/サイト間 VPN

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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るコマンドの詳細については、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（本社）に、スポーク設定の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は、ルータが電源に接続され、USBフラッシュドライブに付属の手順に従ってネットワークにケーブル接続されます。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**から設定が読み取られます。ルータの電源が入るとすぐに、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。手動証明書付与が設定されている場合、SCEP要求のアウトオブバンド検証（IPアドレス検証チェック、導入を実行する担当者のクレデンシャル検証など）を実行する必要があります。 この手順は、使用されているCAサーバによって異なる場合があります。
8. 有効な証明書を持つスポークルータがSCEP応答を受信すると、インターネットキー交換(IKE)セッションがVPNハブで認証され、トンネルが正常に確立されます。

SUDIベースの認可

ステップ7では、SCEPプロトコルを介して送信される証明書署名要求を手動で検証します。これは面倒で、技術者以外の担当者が実行するのが困難な場合があります。セキュリティを強化し、プロセスを自動化するために、Secure Unique Device Identification(SUDI)デバイス証明書を使用できます。SUDI証明書は、ISR 4Kデバイスに組み込まれている証明書です。これらの証明書はCisco CAによって署名されます。製造された各デバイスは異なる証明書で発行されており、デバイスのシリアル番号は証明書の共通名に含まれています。SUDI証明書、関連付けられたキーペア、および証明書チェーン全体が、不正開封防止型のトラストアンカーチップに保存されます。さらに、キーペアは特定のTrust Anchorチップに暗号的にバインドされ、秘密キーはエクスポートされません。この機能により、ID情報のクローニングやスプーフィングが事実上不可能になります。

SUDI秘密キーを使用して、ルータによって生成されたSCEP要求に署名できます。CAサーバは、署名を確認し、デバイスのSUDI証明書の内容を読み取ることができます。CAサーバは、SUDI証明書（シリアル番号など）から情報を抽出し、その情報に基づいて認証を実行できます。RADIUSサーバを使用して、このような許可要求に応答できます。

管理者は、スポークルータとそれに関連するシリアル番号のリストを作成します。シリアル番号は、技術者以外の担当者がルータのケースから読み取ることができます。これらのシリアル番号はRADIUSサーバデータベースに保存され、サーバはその情報に基づいてSCEP要求を承認し、証明書が自動的に付与されるようにします。シリアル番号は、シスコの署名付きSUDI証明書を使用して特定のデバイスに暗号的に結び付けられているため、偽造することはできません。

要約すると、CAサーバは、次の両方の条件を満たす要求を自動的に許可するように設定されます。

- Cisco SUDI CAによって署名された証明書に関連付けられた秘密キーで署名される
- SUDI証明書から取得したシリアル番号情報に基づいて、Radiusサーバによって認証さ

れます

導入シナリオ

CAサーバがインターネットに直接公開されている可能性があるため、トンネルを構築する前にクライアントが登録を実行できます。CAサーバは、VPNハブと同じルータに設定することもできます。このトポロジの利点はシンプルです。CAサーバがインターネット経由でさまざまな形式の攻撃に直接晒されるため、この欠点はセキュリティの低下です。

または、Registration Authorityサーバを設定してトポロジを拡張することもできます。Registration Authorityサーバの役割は、有効な証明書署名要求(CSR)を評価し、CAサーバに転送することです。RAサーバ自体にはCAの秘密キーが含まれていないため、自身で証明書を生成することはできません。このような導入では、CAサーバをインターネットに公開する必要がないため、全体的なセキュリティが向上します。

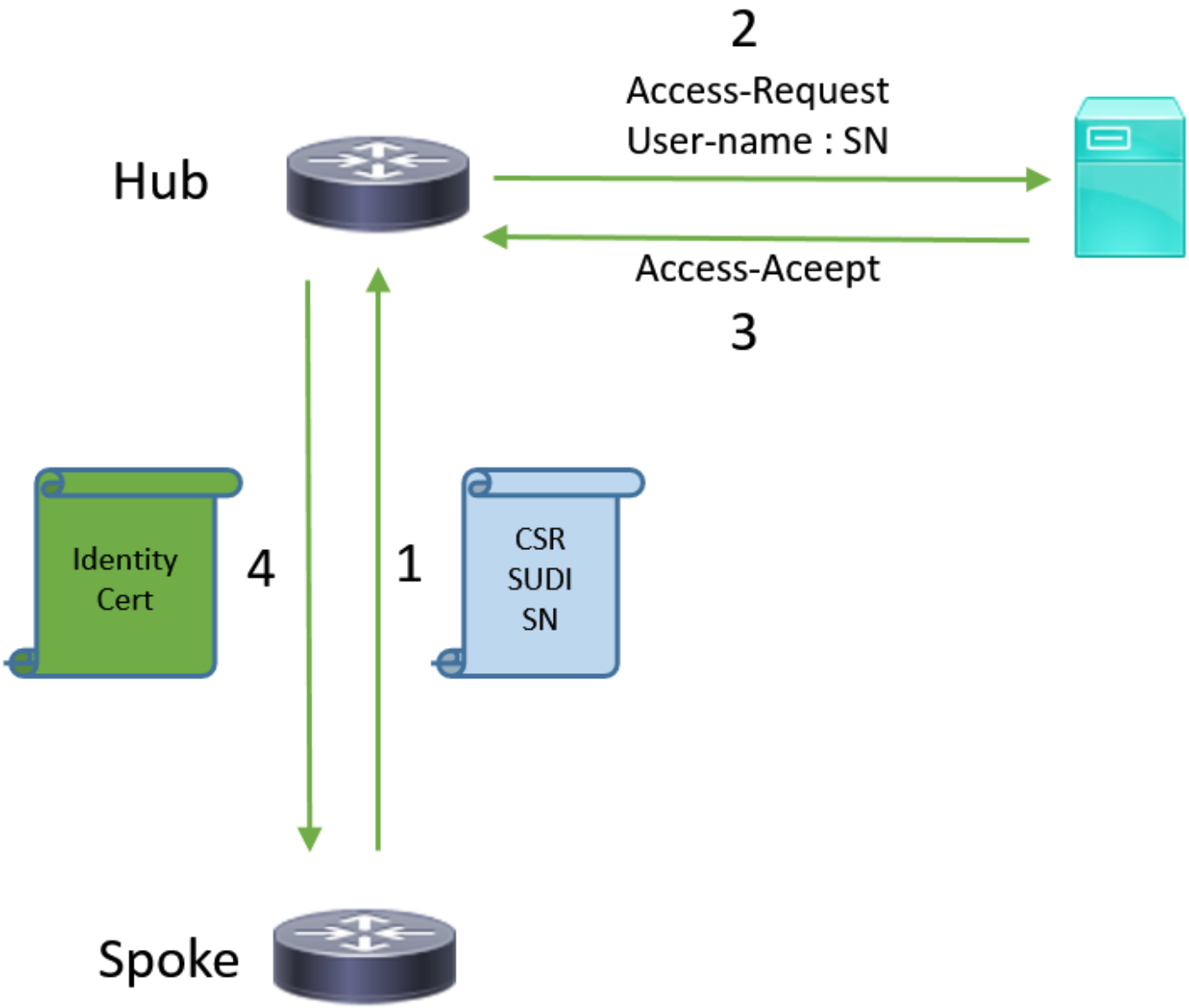
ネットワーク フロー

1.スポークルータはSCEP要求を作成し、SUDI証明書の秘密キーで署名し、CAサーバに送信します。

2.要求が正しく署名されていれば、RADIUS要求が生成されます。シリアル番号はユーザ名パラメータとして使用されます。

3. RADIUSサーバが要求を受け入れるか、拒否します。

4.要求が受け入れられると、CAサーバは要求を許可します。拒否された場合、CAサーバは「Pending」ステータスで応答し、フォールバックタイマーの期限が切れた後、クライアントは要求を再試行します。



CAのみの設定

```
!CA server

radius server RADSRV
address ipv4 10.10.20.30 auth-port 1812 acct-port 1813
key cisco123

aaa group server radius RADSRV
server name RADSRV

aaa authorization network SUDI group RADSRV

crypto pki server CA
! will grant certificate for requests signed by SUDI certificate automatically
grant auto trustpoint SUDI
issuer-name CN=ca.example.com
hash sha256
lifetime ca-certificate 7200
lifetime certificate 3600

crypto pki trustpoint CA
rsakeypair CA 2048
```

```
crypto pki trustpoint SUDI
! Need to import the SUDI CA certificate manually, for example with "crypto pki import" command
enrollment terminal
revocation-check none
! Authorize with Radius server
authorization list SUDI
! SN extracted from cert will be used as username in access-request
authorization username subjectname serialnumber
```

!CLIENT

```
crypto pki trustpoint FLEX
enrollment profile PROF
! Serial-number, fqdn and ip-address fields need to be defined, otherwise the interactive prompt
will prevent the process from starting automatically
serial-number none
fqdn none
ip-address none
! Password needs to be specified to automate the process. However, it will not be used by CA
server
password 7 110A1016141D5A5E57
subject-name CN=spoke.example.com
revocation-check none
rsakeypair FLEX 2048
auto-enroll 85 crypto pki profile enrollment PROF ! CA server address enrollment url
http://192.0.2.1 enrollment credential CISCO_IDEVID_SUDI ! By pre-importing CA cert you will
avoid “crypto pki authenticate” step. If auto-enroll is configured, enrollment will also start
automatically crypto pki certificate chain FLEX certificate ca 01 30820354 3082023C A0030201
02020101 300D0609 2A864886 F70D0101 04050030 3B310E30 0C060355 040A1305 43697363 6F310C30
0A060355 040B1303 54414331 ----- output truncated ---- quit
```

RADIUS server:

The Radius needs to return Access-Accept with the following Cisco AV Pair to enable certificate enrollment:

```
pki:cert-application=all
```

CAおよびRAによる設定

!CA server

```
crypto pki server CATEST
   issuer-name CN=CATEST.example.com,OU=TAC,O=Cisco
   ! will grant the requests coming from RA automatically
   grant ra-auto
crypto pki trustpoint CATEST
   revocation-check crl
   rsakeypair CATEST 2048
```

!RA server

```
radius server RADSRV
   address ipv4 10.10.20.30 auth-port 1812 acct-port 1813
   key cisco123

aaa group server radius RADSRV
   server name RADSRV
```

```
aaa authorization network SUDI group RADSRV

crypto pki server RA
   no database archive
   ! will forward certificate requests signed by SUDI certificate automatically
   grant auto trustpoint SUDI
   mode ra

crypto pki trustpoint RA
   ! CA server address
   enrollment url http://10.10.10.10
   serial-number none
   ip-address none
   subject-name CN=ra1.example.com, OU=ioscs RA, OU=TAC, O=Cisco
   revocation-check crl
   rsakeypair RA 2048

crypto pki trustpoint SUDI
   ! Need to import the SUDI CA certificate manually, for example with "crypto pki import"
command
   enrollment terminal
   revocation-check none
   ! Authorize with Radius server
   authorization list SUDI
   ! SN extracted from cert will be used as username in access-request
   authorization username subjectname serialnumber
```

!CLIENT

```
crypto pki trustpoint FLEX
   enrollment profile PROF
   ! Serial-number, fqdn and ip-address fields need to be defined, otherwise the interactive
prompt will prevent the process from starting automatically
   serial-number none
   fqdn none
   ip-address none
   ! Password needs to be specified to automate the process. However, it will not be used by CA
server
   password 7 110A1016141D5A5E57
   subject-name CN=spoke.example.com
   revocation-check none
   rsakeypair FLEX 2048
   auto-enroll 85

crypto pki profile enrollment PROF
   ! RA server address
   enrollment url  http://192.0.2.1
   enrollment credential CISCO_IDEVID_SUDI


! By pre-importing CA cert you will avoid “crypto pki authenticate” step. If auto-enroll is
configured, enrollment will also start automatically
crypto pki certificate chain FLEX
   certificate ca 01
  30820354 3082023C A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  3B310E30 0C060355 040A1305 43697363 6F310C30 0A060355 040B1303 54414331
 ----- output truncated ----
  quit
```

RADIUS server:

The Radius needs to return Access-Accept with the following Cisco AV Pair to enable certificate enrollment:

pki:cert-application=all

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
! This will differ if you use SUDI, please see above
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、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool 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
```

トラブルシュート

現在、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 :Config WizardがG2プラットフォームでPnPフローを停止すると、システムがusbflash:/ciscortr.cfgから設定をロードしなくなる可能性があります。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。

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

注：このバージョンの修正が含まれているバージョンを使用していることを不具合します。

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**するデフォルト設定ファイル**機能は、『Cisco 800シリーズISR導入の概要』で説明されているUSBによるゼロタッチ導入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**
対応プラットフォーム	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。
filename	*.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。Embedded 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
- シスコアンカーテクノロジー