تكوين النشر دون لمس (ZTD) للمكاتب/الفروع البعيدة لشبكة VPN

المحتويات

المقدمة

يوضح هذا المستند كيفية النشر دون لمس (ZTD) يعد الحل الموفر للتكلفة والقابل للتطوير لعمليات النشر.

قد يكون من الصعب تنفيذ عملية نشر تتسم بالأمان والفاعلية وتوفير موجهات المكاتب البعيدة (والتي تسمى أحيانًا الفروع). قد تكون المكاتب البعيدة في مواقع حيث يكون من الصعب وجود مهندس ميداني يقوم بتكوين الموجه في الموقع، ويختار معظم المهندسين عدم إرسال موجهات تم تكوينها مسبقًا بسبب التكلفة والمخاطر الأمنية المحتملة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- أي موجه Cisco IOS® به منفذ USB يدعم محركات أقراص USB المحمولة. للحصول على تفاصيل، راجع دعم ميزات USB EToken و USB Flash.

- أكدت اذه سمة أن يعمل على تقريبا أي cisco 8xx منصة. للحصول على تفاصيل، راجع التقرير الرسمي لملفات التكوين الافتراضية (ميزات دعم على موجه خدمات مدمجة Cisco 800 Series ISR).
- أنظمة أساسية أخرى تحتوي على منافذ USB مثل موجه الخدمة المتكاملة (ISR) من الجيل الثاني و 43xx/44xx.

المكونات المستخدمة

تستند المعلومات الواردة في اذه المستند إلى إصدارات البرامج والمكونات المادية التالية:

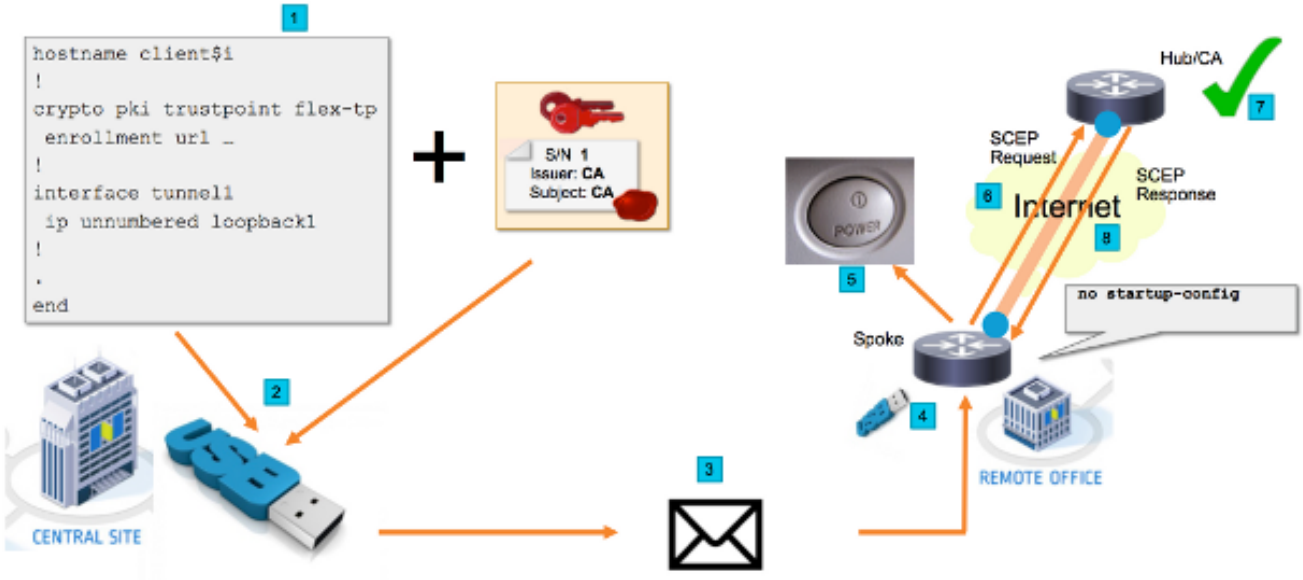
- بروتوكول تسجيل الشهادة البسيط (SCEP)
- النشر دون لمس عبر منفذ USB
- شبكات VPN/FlexVPN/من موقع إلى موقع

تم إنشاء المعلومات الواردة في اذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في اذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

> **ملاحظة**: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في اذه القسم.

الرسم التخطيطي للشبكة



تدفق الشبكة

1. في الموقع المركزي (مقر الشركة الرئيسي)، يتم إنشاء قالب تكوين Talk. يحتوي القالب على شهادة المرجع المصدق (CA) التي وقعت على شهادة موجه موزع شبكات VPN.
2. تم إنشاء مثيل لقالب التكوين على مفتاح USB في ملف يسمى **ciscortr.cfg**.

يحتوي ملف التكوين هذا على التكوين الخاص بالموجه الذي سيتم نشره.
ملاحظة: لا يحتوي التكوين على USB على أي معلومات حساسة بخلاف عناوين IP ومشهادة CA. لا يوجد مفتاح خاص لخادم TALK أو CA.

3. يتم إرسال محرك أقراص USB المحمول إلى المكتب البعيد عبر شركة البريد أو توصيل الحزم.
4. يتم إرسال الموجه الذي يتم التحدث به أيضا إلى المكتب البعيد مباشرة من شركة Cisco Manufacturing.
5. في المكتب البعيد، يتم توصيل الموجه بالطاقة وتوصيله بكابل بالشبكة USB. بعد ذلك، يتم كما هو موضح في التعليمات المضمنة مع محرك أقراص USB المحمول في الموجه. **ملاحظة**: هناك القليل أو منعدم من إدراج محرك أقراص USB المحمول في الموجه. هذه الخطوة، ولذلك يمكن لأي موظف في المهارات التقنية التي تنطوي عليها هذه الخطوة، ولذلك يمكن لأي موظف في المكتب أداؤها بسهولة.
6. بمجرد تمهيد الموجه، فإنه يقرأ التكوين من **usbflash0:/ciscortr.cfg**. بمجرد تشغيل الموجه، يتم إرسال طلب بروتوكول تسجيل الشهادة البسيط (SCEP) إلى خادم CA.
7. على خادم CA يمكن تكوين منح يدوي أو تلقائي استنادا إلى نهج أمان الشركة. عند تكوينه لمنح الشهادات يدويا، يجب إجراء التحقق خارج النطاق من طلب SCEP (التحقق من صحة عنوان IP، التحقق من صحة بيانات الاعتماد للموظفين الذين يقومون بعملية النشر، إلخ). قد تختلف هذه الخطوة بناء على خادم CA المستخدم.
8. بمجرد إستلام إستجابة SCEP بواسطة الموجه الذي تم التحدث به، والذي يحتوي الآن على شهادة صالحة، تتم مصادقة جلسة عمل تبادل مفاتيح الإنترنت (IKE) مع مركز VPN وتم إنشاء النفق بنجاح.

تفويض قائم على SUDI

تنطوي الخطوة 7 على التحقق اليدوي من طلب توقيع الشهادة المرسل عبر بروتوكول SCEP، والذي قد يكون مرهقا وعرضة للتنفيذ للموظفين غير الفنيين. لزيادة الأمان والأتمتة العملية، يمكن إستخدام شهادات جهاز التعرف على الجهاز الفريد الآمن (SUDI). شهادات SUDI هي شهادات مضمنة في أجهزة ISR 4K. يتم توقيع هذه الشهادات بواسطة Cisco CA. تم إصدار لكل جهاز مصنع بشهادة مختلفة، كما تم تضمين الرقم التسلسلي للجهاز وسلسلة الشهادة. يتم تخزين شهادة SUDI، جوز المفاتيح المرتبط، والاسم الشائع للشهادة. يتم تصدير الشهادات الخاصة بها بالكامل في شريحة مساعد الثقة المقاومة للعبث. علاوة على ذلك، يتم توقيع الشهادة بشكل مشفر بشريحة Trust Anchor مما يجعل هذه المعلومات الهوية من المستحيل تقريبا.

يمكن إستخدام مفتاح SUDI الخاص لتوقيع طلب SCEP الذي تم إنشاؤه بواسطة الموجه. يمكن لخادم CA التحقق من التوقيع وقراءة محتويات شهادة SUDI الخاصة بالجهاز. يمكن لخادم CA إستخراج المعلومات من شهادة SUDI (مثل الرقم التسلسلي) وإجراء التخويل بناء على تلك المعلومات. يمكن إستخدام خادم RADIUS لطلب تفويض كهذا.

يقوم المسؤول بإنشاء قائمة بالموجهات الفرعية وأرقامها التسلسلية المقترنة بها. يمكن قراءة الأرقام التسلسلية من حالة الموجه من قبل الموظفين غير الفنيين. يتم تخزين هذه الأرقام التسلسلية في قاعدة بيانات خادم RADIUS ويأذن الخادم بطلبات SCEP استنادا إلى تلك المعلومات التي تسمح بمنح الشهادة تلقائيا. لاحظ أن الرقم التسلسلي مرتبط بشكل مشفر بجهاز معين عبر شهادة SUDI الموقعة من Cisco، لذلك من المستحيل تزويرها.

وخلاصة القول، إن خادم CA تم تكوينه لمنح الطلبات التي تلبي كل المعايير تلقائيا:

- تم التوقيع باستخدام مفتاح خاص مرتبط بشهادة موقعة من قبل Cisco SUDI CA
- معتمد من قبل خادم RADIUS بناء على معلومات الرقم التسلسلي المأخوذة من شهادة SUDI

سيناريوهات النشر

يتعرض خادم CA مباشرة للإنترنت، مما يسمح للعملاء بإجراء التسجيل قبل بناء النفق. يمكن حتى تكوين خادم CA على نفس الموجه مثل موزع VPN. الميزة في هذا المخطط هي البساطة. أما العيب في تمثل في انخفاض مستوى الأمن لأن خادم CA يتعرض بشكل مباشر لمختلف أشكال الهجمات عبر الإنترنت.

ولكن من الممكن توسيع المخطط من خلال تكوين خادم سلطة التسجيل. دور خادم هذه التسجيل هو تقييم طلبات توقيع الشهادات الصالحة وإعادة توجيهها إلى خادم CA. الـ CA يحتوي خادم RA نفسه على المفاتيح الخاص بـ CA والذي يمكنه إنشاء الشهادات بنفسه. في مثل هذا النشر، الـ CA يجب أن يكون خادم معرض للإنترنت، مما يزيد من الأمان الإجمالي.

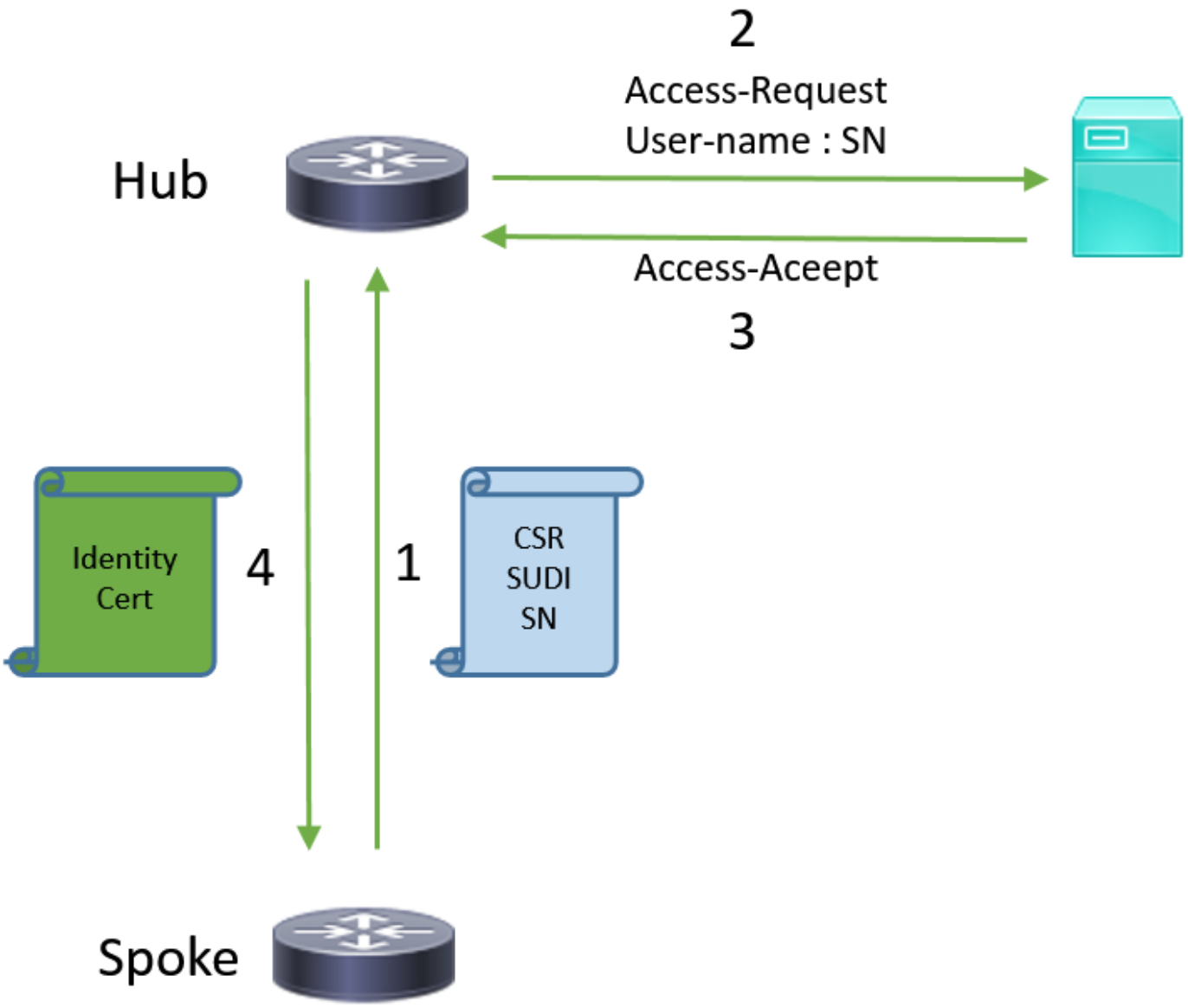
تدفق الشبكة

1. الموجه المتصل بإنشاء طلب SCEP، ويوقعه باستخدام المفتاح الخاص لشهادة SUDI الخاصة به ويرسله إلى خادم CA.

2. إذا تم توقيع الطلب بشكل صحيح، يتم إنشاء طلب RADIUS. يتم إستخدام الرقم التسلسلي كمعلمة اسم مستخدم.

3. يقبل خادم RADIUS الطلب أو يرفضه.

4. في حالة قبول الطلب، يقوم خادم CA بمنح الطلب. في حالة رفضه، يرد خادم CA بالحالة "معلق" ويعيد العميل محاولة الطلب بعد انتهاء صلاحية المؤقت الاحتياطي.



التكوين باستخدام CA فقط

```
!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
```

التكوين باستخدام CA و RA

!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

التكوينات/القالب

يعرض هذا النموذج من الإخراج تكوين المكتب البعيد FlexVPN مثالي يتم وضعه على محرك أقراص Flash في الملف **usbflash0:/ciscortr.cfg**.

```
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"
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

[دعم أداة مترجم الإخراج (للعملاء المسجلين فقط) بعض الأوامر show.](#) استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرج الأمر show.

يمكنك التحقق على ال"Talk" إذا كانت الأنفاق مرتفعة:

```
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
```

يمكنك أيضا التحقق من "تم التحدث" إذا تم تسجيل الشهادة بشكل صحيح:

```
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
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

المحاذير والمشكلات المعروفة

معرف تصحيح الأخطاء من Cisco CSCuu93989 - قد يتسبب معالج التكوين في إيقاف تدفق PnP على الأنظمة الأساسية G2 في عدم تحميل النظام التكوين من usbflash:/ciscortr.cfg. وبدلاً من ذلك، قد يتوقف النظام عند مهلة "معالج التكوين":

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

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

ملاحظة: تأكد من إستخدام إصدار يحتوي على إصلاح لهذا الخلل.

ZTD عبر USB مقابل ملفات التكوين الافتراضية

لاحظ أن ميزة **ملفات التكوين الافتراضية** التي يستخدمها هذا المستند هي ميزة مختلفة عن **النشر من دون لمس عبر USB** الموضحة في نظرة عامة على نشر ISR السلسلة Cisco 800 Series.

	النشر دون لمس عبر منفذ USB	**ملفات التكوين الافتراضية**
الأنظمة الأساسية المدعومة	يقتصر على عدد قليل من موجهات 8xx. للحصول على تفاصيل، راجع نظرة عامة على نشر ISR السلسلة 800 من Cisco	جميع موجهات الخدمات المتكاملة (ISR) من الجيل الثاني و 43xx و 44xx.
اسم الملف	*.cfg	ciscoCortr.cfg
ينفذ التشكيل على برق محلي	نعم، تلقائيا	لا، مدير الحدث المضمن مطلوب

انظر الاعتماد المزيد من الأنظمة الأساسية من قبل ميزة **ملفات التكوين الافتراضية**، تم إختيار هذه التقنية للحل الوارد في هذه المقالة.

ملخص

تتيح ميزة التكوين الافتراضي عبر منفذ USB (باستخدام اسم الملف **ciscortr.cfg** من محرك أقراص الفلاش يعمل عبر منفذ USB) لمسؤولي الشبكات إمكانية نشر شبكات VPN الخاصة بموجه Office البعيد (VPN) فقط) دون الحاجة إلى تسجيل الدخول إلى الجهاز في الموقع البعيد.

معلومات ذات صلة

- بروتوكول تسجيل الشهادة البسيط (SCEP)
- النشر دون لمس عبر منفذ USB
- شبكات VPN/FlexVPN/من موقع إلى موقع
- الدعم التقني والمستندات - Cisco Systems
- تقنية المراسلة من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).