مصادقة IPSec لعميل ASA/PIX 8.x و VPN باستخدام شهادات رقمية باستخدام مثال تكوين Microsoft CA

المحتويات

المقدمة

يوضح هذا المستند كيفية تثبيت شهادة رقمية لمورد من إنتاج جهة خارجية ودي على خادم IPSec مع خادم أقران VPN لمصادقة إلى عملاء VPN باستخدام ASA/PIX 8.x (ASA/PIX) "جهاز الأمان من Cisco" (CA). "مرجع شهادة Microsoft"

المتطلبات الأساسية

المتطلبات

يتطلب هذا المستند أن يكون لديك حق الوصول إلى مرجع مصدق لتسجيل الشهادة. وموردو CA الموثوق من جهات خارجية هم بالتيمور و Cisco و Entrust و iPlanet/Netscape و Microsoft و RSA و VeriSign.

يفترض هذا المستند عدم وجود تكوين شبكة VPN موجود مسبقا في ASA/PIX.

ملاحظة: يستخدم هذا المستند خادم Microsoft Windows 2003 كخادم CA للسيناريو.

ملاحظة: ارجع إلى تكوين CA على خادم Windows للحصول على معلومات كاملة حول كيفية

تكوين خادم Windows 2003 كمرجع مصدق.

المكونات المستخدمة

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

- ASDM الإصدار 6.0(2) و البرنامج الإصدار 8.0(2) من ASA 5510 الذي يشغل الإصدار
- عميل VPN الذي يشغل الإصدار 4.x من البرنامج والإصدارات الأحدث

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

المنتجات ذات الصلة

كما يمكن إستخدام تكوين ASA مع Cisco 500 Series PIX الذي يشغل الإصدار 8.x من البرنامج.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول الاصطلاحات المستندات.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

ملاحظة: ال ip ليس خاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أي كان استعملت في مختبر بيئة.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين ASA
- ملخص تكوين ASA
- تكوين عميل شبكة VPN

تكوين ASA

من أجل تثبيت الشهادة الرقمية لمورد الطرف الثالث على ASA، أكمل الخطوات التالية:

- [الخطوة 1. التحقق من دقة قيم التاريخ والوقت والمنطقة الزمنية](#)
- [الخطوة 2. إنشاء طلب توقيع شهادة](#)
- [الخطوة 3. مصادقة TrustPoint](#)
- [الخطوة 4. تثبيت الشهادة](#)
- [الخطوة 5. تكوين شبكة VPN للوصول عن بعد (IPSec) باستخدام الشهادة المثبتة حديثا](#)

الخطوة 1. التحقق من دقة قيم التاريخ والوقت والمنطقة الزمنية

إجراء ASDM

1. انقر على تكوين، ثم انقر على إعداد الجهاز.
2. قم بزيادة وقت النظام، واختر الساعة.
3. تحقق من صحة المعلومات المدرجة.

يجب أن تكون قيم التاريخ والوقت والمنطقة الزمنية دقيقة حتى يتم التحقق من صحة الشهادة.

مثال على سطر الأوامر

Cisco ASA
CiscoASA#show clock 05:37:37.904 UTC Fri Dec 21 2007

الخطوة 2. إنشاء طلب توقيع شهادة

مطلوب طلب توقيع شهادة (CSR) من أجل إصدار شهادة هوية من قبل جهة خارجية. يحتوي CSR على سلسلة اسم ASA المميز (DN) مع المفاتيح العام الذي تم إنشاؤه ل ASA. يستخدم ASA المفتاح الخاص الذي تم إنشاؤه لتوقيع CSR رقميا.

إجراء ASDM

1. انقر فوق تكوين، ثم انقر فوق إدارة الأجهزة.
2. قم بتوسيع إدارة الترخيص، واختر شهادات الهوية.
3. انقر فوق إضافة (Add).

4. انقر على زر إضافة شهادة هوية جديدة.

5. للحصول على زوج المفاتيح، انقر فوق جديد.

6. انقر على زر إدخال اسم زوج مفاتيح جديد. يجب عليك تعريف اسم زوج المفاتيح بشكل واضح لأغراض التعرف عليه.

7. انقر فوق إنشاء الآن.

يجب إنشاء زوج المفاتيح الآن.

8. لتحديد عنوان DN لموضوع الشهادة، انقر فوق تحديد، ثم قم بتكوين السمات المدرجة في هذا الجدول:

السمة	الوصف
سي إن	اسم المجال المؤهل بالكامل (FQDN) الذي سيتم استخدامه للاتصالات بجدار الحماية الخاص بك. على سبيل المثال: CiscoASA.cisco.com
أو	اسم القسم
O	اسم الشركة (تجنب استخدام الحروف الخاصة)
C	رمز البلد (شفرتان للحرف بدون علامات ترقيم)
سانت	الولاية (يجب أن تكون خالية تماما مثل: كاليفورنيا الشمالية)
L	مدينة

لتكوين هذه القيم، أختر قيمة من القائمة المنسدلة "سمات"، وأدخل القيمة، وانقر فوق إضافة.

ملاحظة: يتطلب بعض موردي الأطراف الثالثة تضمين سمات معينة قبل إصدار شهادة هوية. إذا لم تكن متأكدا من السمات المطلوبة، راجع بائع المنتجات للحصول على التفاصيل.

9. بمجرد إضافة القيم المناسبة، انقر فوق موافق.

يظهر مربع الحوار إضافة شهادة هوية مع تعبئة حقل DN لموضوع الشهادة.

10. طقطقة متقدم.

11. في حقل FQDN، أدخل FQDN الذي سيتم استخدامه للوصول إلى الجهاز من الإنترنت.

يجب أن تكون هذه القيمة هي FQDN نفسها التي استخدمتها للاسم الشائع (CN).

12. انقر فوق موافق، ثم انقر فوق إضافة شهادة.

تتم طباعة CSR إلى ملف txt، ثم يتم تخزين طلب CSR في ملف على الجهاز المحلي.

13. استخدم المفكرة لفتح الملف، ثم انسخ محتوى CSR. ملاحظة: تم حفظ طلب CSR في ملف باسم المعرف.txt في الموقع الذي حددته مسبقا.

14. ارجع إلى موقع الويب الخاص بـ Microsoft CA لتقديم CSR.

a. انقر فوق "طلب شهادة" ثم انقر فوق "طلب شهادة متقدمة"، ثم انقر فوق "إرسال طلب شهادة باستخدام ملف PKCS#10 مرمز بأساس 64".

ملاحظة: تأكد من وجود حساب مستخدم لـ ASA (خادم VPN) على خادم CA.

b. استخدم خادم CA 172.16.5.1 عبر الويب للوصول إلى صفحة تسجيل الدخول باستخدام بيانات اعتماد المستخدم vpnServer.

c. الصق المعلومات التي تم نسخها في حقل طلب محفوظ، ثم انقر فوق إرسال.

d. انقر فوق زر الاختيار Base 64 المرمز، ثم انقر فوق تنزيل الشهادة.

e. سيظهر نافذة تنزيل الملف. احفظه باسم cert_client_id.cer، وهو الشهادة التي سيتم تثبيتها على ASA.

مثال على الأوامر

Cisco ASA
!--- D

```
                                                    !--- Initiates certificate signing request. This

                                                                                                        $

!--- Displays the PKCS#10 enrollment request to the terminal. You will need to !--- copy this from the
```

الخطوة 3. مصادقة TrustPoint

بمجرد إستلام شهادة الهوية من مورد الطرف الثالث، يمكنك متابعة هذه الخطوة.

إجراء ASDM

1. قم بحفظ شهادة الهوية على الكمبيوتر المحلي.

2. إذا تم توفير شهادة مرمزة من نوع base64 غير موجودة كملف، يجب نسخ الرسالة base64 ولصقها في ملف نصي.

3. إعادة تسمية الملف بامتداد .cer

ملاحظة: بمجرد إعادة تسمية الملف بامتداد .cer، تظهر أيقونة الملف كشهادة، كما هو موضح.

4. قم بالنقر المزدوج على ملف الترخيص.

ملاحظة: إذا لم يكن لدى Windows معلومات كافية للتحقق من هذه الشهادة في علامة التبويب "عام"، يجب الحصول على شهادة المرجع المصدق (CA) الجذر أو شهادة المرجع المصدق الوسيط (CA) للجهة التي قامت بإصدار الشهادة. اتصل بمورد الجهة الخارجية أو بمسؤول CA للحصول على شهادة CA أو شهادة CA الوسيطة لإصدار الأصل.

5. انقر على علامة التبويب مسار الشهادة.

6. انقر على شهادة المرجع المصدق المرتبطة بشهادة الهوية الصادرة، وانقر فوق عرض الشهادة.

ظهر معلومات تفصيلية حول شهادة المرجع المصدق.

7. انقر فوق تفاصيل لمعرفة المزيد من المعلومات حول شهادة الهوية.

8. قبل تثبيت شهادة الهوية، يجب تنزيل شهادة المرجع المصدق من خادم CA وتثبيتها في ASA، كما هو موضح.

1. أتمت هذا steps in order to جلبت الـ CA شهادة من الـ CA لاذل يعين CA1.

a. قم بإجراء تسجيل الدخول إلى الويب إلى خادم CA 172.16.5.1 بمساعدة بياناتك الاعتماد المتوفرة لخادم VPN.

b. انقر على تنزيل شهادة CA أو سلسلة الشهادات أو CRL لفتح النافذة، كما هو موضح. طقطقت Base 64 السلكي زر بما أن الـ يرمز طريقة، وطقطقت تنزيل مرجع مصدق.

c. احفظ شهادة المرجع المصدق مع اسم certnew.cer على الكمبيوتر.

9. تصفح إلى المكان الذي قمت فيه بحفظ شهادة المرجع المصدق.

10. افتح الملف باستخدام محرر نصوص، مثل Notepad. انقر بزر الماوس الأيمن فوق الملف، واختر إرسال إلى > Notepad.

11. تظهر الرسالة التي تم ترميزها بالأساس 64 والمشابهة للشهادة الموجودة في هذه الصورة:

12. ضمن ASDM، انقر على تكوين، ثم انقر على إدارة الأجهزة.

13. قم بتوسيع إدارة الترخيص، واختر شهادات CA.

14. انقر فوق إضافة (Add).

15. انقر على زر لصق الشهادة بتنسيق PEM، وقم بلصق شهادة المرجع المصدق المقدمة من مورد الطرف الثالث في حقل النص. الأساسية 64

16. انقر على تثبيت الشهادة.

ظهر مربع حوار يؤكد أن التثبيت ناجح.

مثال على سطر الأوامر

Cisco ASA
!--- Initiates the prompt for paste-in of base64 CA intermediate certificate. ! This should be provide Enter the bas End with the wor **MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqA** **MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYK** **BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UE** **M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmS**

```
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPy
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAv
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9Iq
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxg
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBX
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQ
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQB
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud
pAPlWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJs
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9u
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25M
Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNWh0dHA6
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3Js
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHU
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8Ey
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8Gsr
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeO
9Ms7ABAu+pRIoi/E
```

```
!--- Manually

INFO: Certificate ha
Fingerprint:     98d6600
Do you accept

Trustpo

% Certi
```

الخطوة 4. تثبيت الشهادة

إجراء ASDM

أستخدم شهادة الهوية المقدمة من مورد الطرف الثالث من أجل إكمال الخطوات التالية:

1. انقر فوق تكوين، ثم انقر فوق إدارة الأجهزة.
2. قم بتوسيع إدارة الترخيص، ثم أختر شهادات الهوية.
3. حدد شهادة الهوية التي قمت بإنشائها في الخطوة 2

ملاحظة: يعرض تاريخ انتهاء الصلاحية مع القا.

4. انقر على تثبيت.

انقر على زر لصق بيانات الشهادة بتنسيق base-64، وقم بلصق شهادة الهوية

المقدمة من مورد الطرف الثالث في حقل النص.

انقر على تثبيت الشهادة.5.

يظهر مربع حوار لتأكيد أن الاستيراد ناجح.

مثال على سطر الأوامر

Cisco ASA

```
<#root>

CiscoASA(config)#

crypto ca import CA1 certificat


!--- Initiates prompt to paste the base64 identity !--- certificate provided by the third party vendor

%The fully-qualified domain name in the certificate will be: CiscoASA.cisco.com

Enter the base 64 encoded certificate
End with the word "quit" on a line by itself

!--- Paste the base 64 certificate provided by the third party vendor.

-----BEGIN CERTIFICATE----
MIIFpzCCBI+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBRMRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFTATBgoJkia
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUzOVoXDTA
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMSQw
IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14CqB9j3Hp
BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/oSQVauUsY7zCOsS8iqxq
2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/CaeqnGR
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ2lzY29BU0E
Y2lzY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KMl0xCFjAfBgNVHSM
GDAWgBTZrb8I8jqI8RRDL3mYfNQJpAPlWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qC
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJ
aWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNWh0dHA
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3J
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFwOi8vL0N
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2Vydml
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1jb20/Y0F
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3J
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1dlYi5jaXNjby5jb21fQ0ExLmN
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1UdEwEB/wQ
MAAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEBAIqCaA9
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB7wXQaGp
zRq4dxALll1JkIjhfeQY+7VSkZlGEpuBnENTohdhthz5vBjGlcROXIs8+3Ghg8h
```

```
YZZEM73e8EC0sEMedFb+KYpAFy3PPy4l8EHe4MJbdjUp/b90l5l6IzQP5l51YB0
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87ychngKB+
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtSt1nwLps
lL5nuPsd8MaexBc
-----END CERTIFICATE----
qui

INFO: Certificate successfully importe
CiscoASA(config)
```

الخطوة 5. تكوين شبكة VPN للوصول عن بعد (IPSec) الاستخدام الشهادة المثبتة حديثا

إجراء ASDM

أتمت هذه steps in order to تشكيل الوصول عن بعد VPN:

1. اختر تشكيل>الوصول عن بعد VPN>شبكة (زبون) منفذ > متقدم > IPSec > سياسات IKE>إضافة in order to خلقت ISAKMP سياسة 65535، كما هو موضح.

   طقطقة ok ويطبق.

2. اختر تشكيل > Remote Access VPN > شبكة (زبون) منفذ > متقدم > IPSec > مجموعات تحويل IPSec > إضافة in order to خلقت مجموعة تحويل Myset، كما هو موضح.

   طقطقة ok ويطبق.

3. اختر Configuration > Remote Access VPN (الوصول عن بعد) > Network (العميل) Access > Advanced > IPSec > Crypto Maps (خرائط التشفير) > Add لإنشاء خريطة تشفير باستخدام السياسة الديناميكية للأولوية 10، كما هو موضح.

   طقطقة ok ويطبق.

   ملاحظة: ال يدعم ASA 8. 0 SHA 2. أيضا ال يتم دعم عملاء IPSec الذين يستخدمون الشهادات التي تحتوي على تجزئة 256.

4. اختر Configuration > Remote Access VPN (الوصول عن بعد) > Network (Client) Access > Advanced > Group Policies (نهج المجموعة) > Add in order to خلقت DefaultGroup Group Policy، كما هو موضح.

   طقطقة ok ويطبق.

5. اختر تشكيل>الوصول عن بعد VPN>شبكة (زبون) منفذ>عناوين تعيين>عناوين>بركة>يضيف in order to تشكل ال vpnPool عناوين بركة ل ال VPN زبون مستعمل أن يكون تعيين ديناميكيا.

   طقطقة ok ويطبق.

6. اختر تشكيل>Remote Access VPN عن بعد>AAA إعداد>مستعمل محلي>يضيف in

order to تخلق ال vpn مستعمل حساب ل VPN زبون منفذ. أيضا، أجعل هذا المستخدم عضوا في DefaultRAGroup.

أخترت تشكيل>Remote Access VPN>شبكة (زبون) منفذ>IPSec توصيل توصيفات >7. تحرير in order to تحرر DefaultRAGgroup، كما هو موضح.

- أختر شهادة الهوية المناسبة من القائمة المنسدلة لحقل مصادقة نظير IKE.
- أختر مجموعة الخوادم كمجموعة محلية لحقل مصادقة المستخدم.
- أخترت vpnpool كالزبون عنوان بركة ل الزبون عنوان تعيين مجال.
- أختر DefaultGroup كنهج المجموعة لحقل "نهج المجموعة الافتراضية".

طقطقة ok وبطيق.

رماوألا رطس ىلع لاثم

Cisco ASA

<#root
CiscoASA(config)
crypto isakmp enable outsid
CiscoASA(config)
crypto isakmp policy 6553
CiscoASA(config-isakmp-policy)
authentication rsa-si
CiscoASA(config-isakmp-policy)
encryption 3de
CiscoASA(config-isakmp-policy)
hash md
CiscoASA(config-isakmp-policy)
group
CiscoASA(config-isakmp-policy)
lifetime 8640
CiscoASA(config-isakmp-policy)#exi
CiscoASA(config)
crypto isakmp identity aut
!--- Phase 1 Configuratio
CiscoASA(config)

```
                                                crypto ipsec transform-set myset esp-3des esp-md5-hma
                                                                                        CiscoASA(config)
                                                  crypto dynamic-map dynmap 10 set transform-set myse
                                                                                        CiscoASA(config)
                                                       crypto map mymap 10 ipsec-isakmp dynamic dynma
                                                                                        CiscoASA(config)
                                                                crypto map mymap interface outsid


                                                                        !--- Phase 2 Configuration


                                                                                        CiscoASA(config)
                                                                group-policy defaultgroup interna
                                                                                        CiscoASA(config)
                                                              group-policy defaultgroup attribute
                                                                   CiscoASA(config-group-policy)
                                                                   default-domain value cisco.co
                                                             CiscoASA(config-group-policy)# exi

                                          !--- Create a group policy "defaultgroup" with domain name !--- cisco.co


                                                                                        CiscoASA(config)
                                                                username vpnuser password Cisco12
                                                                                        CiscoASA(config)
                                                                  username vpnuser attribute
                                                                    CiscoASA(config-username)
                                                                      memberof  DefaultRAGrou
                                                                  CiscoASA(config-username)#exi

                                              !--- Create a user account "vpnuser" and added to !--- "DefaultGroup


                                                                                        CiscoASA(config)
                                                               tunnel-group DefaultRAGroup general-attribute


!--- The Security Appliance provides the default tunnel groups !--- for remote access (DefaultRAGroup)


                                                                                  CiscoASA(config-tunnel-general)
```

```
address-pool vpnpool

!--- Associate the vpnpool to the tunnel group using the address pool.

CiscoASA(config-tunnel-general)#
default-group-policy Defaultgroup

!--- Associate the group policy "Defaultgroup" to the tunnel group

CiscoASA(config-tunnel-general)# exit
CiscoASA(config)#
tunnel-group DefaultRAGroup ipsec-attributes
CiscoASA(config-tunnel-ipsec)#
trust-point CA1
CiscoASA(config-tunnel-ipsec)#exit

!--- Associate the trustpoint CA1 for IPSec peer !--- authentication
```

ملخص تكوين ASA

Cisco ASA

```
CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 192.168.1.5 255.255.255.0
!
interface Ethernet0/1
shutdown
nameif inside
security-level 100
ip address 10.2.2.1 255.255.255.0
!
interface Ethernet0/2
```

```
                                                    nameif DMZ
                                                  security-level 90
                                          ip address 10.77.241.142 255.255.255.192
                                                          !
                                                interface Ethernet0/3
                                                     shutdown
                                                    no nameif
                                                no security-level
                                                    no ip address
                                                          !
                                              interface Management0/0
                                                     shutdown
                                                    no nameif
                                                no security-level
                                                    no ip address
                                                          !
                                          passwd 2KFQnbNIdI.2KYOU encrypted
                                                   ftp mode passive
                                         dns server-group DefaultDNS
                                                 domain-name cisco.com
          access-list 100 extended permit ip 10.2.2.0 255.255.255.0 10.5.5.0
                                                                  255.255.255.0
                                                   pager lines 24
                                                 mtu outside 1500
                                                  mtu inside 1500
                                                    mtu DMZ 1500
                                      ip local pool vpnpool 10.5.5.10-10.5.5.20
                                                    no failover
                                     icmp unreachable rate-limit 1 burst-size 1
                                              asdm image disk0:/asdm-602.bin
                                                 no asdm history enable
                                                    arp timeout 14400
                                           nat (inside) 0 access-list 100
                                      route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1
                                 route outside 10.1.1.0 255.255.255.0 192.168.1.1 1
                               route outside 172.16.5.0 255.255.255.0 192.168.1.1 1
                                                  timeout xlate 3:00:00
              timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
                                           timeout uauth 0:05:00 absolute
                                dynamic-access-policy-record DfltAccessPolicy
                                                   http server enable
                                               http 0.0.0.0 0.0.0.0 DMZ
                                             http 0.0.0.0 0.0.0.0 outside
                                                 no snmp-server location
                                                 no snmp-server contact
        snmp-server enable traps snmp authentication linkup linkdown coldstart
                           crypto ipsec transform-set myset esp-3des esp-md5-hmac
                             crypto dynamic-map dynmap 10 set transform-set myset
                                  crypto map mymap 10 ipsec-isakmp dynamic dynmap
                                          crypto map mymap interface outside
                                                crypto ca trustpoint CA1
                                                    enrollment terminal
           subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco Systems, C=US,
                                                St=North Carolina,L=Rale
                                                      serial-number
                                                   keypair my.CA.key
                                                       crl configure
                                             crypto ca certificate chain CA1
                                            certificate 611ee59b000000000007
        308205a7 3082048f a0030201 02020a61 1ee59b00 00000000 07300d06 092a8648
```

```
86f70d01 01050500 30513113 3011060a 09922689 93f22c64 01191603 636f6d31
15301306 0a099226 8993f22c 64011916 05636973 636f3115 3013060a 09922689
93f22c64 01191605 54535765 62310c30 0a060355 04031303 43413130 1e170d30
37313231 35303833 3533395a 170d3039 31323134 30383335 33395a30 76310b30
09060355 04061302 55533117 30150603 55040813 0e4e6f72 74682043 61726f6c
696e6131 10300e06 03550407 13075261 6c656967 68311630 14060355 040a130d
43697363 6f205379 7374656d 73312430 22060355 0403131b 43697363 6f415341
2e636973 636f2e63 6f6d204f 553d5453 57454230 819f300d 06092a86 4886f70d
01010105 0003818d 00308189 02818100 b8e20aa8 332356b7 5b660073 5008d373
5d23c529 5b92472b 5e02a81f 63dc7a57 0667d754 5e7f98d3 d4239b42 ab8faf0b
e8a5d394 f80d01a1 4cc01d98 b1320e9f e849055a b94b18ef 308eb12f 22ab1a8e
db38f02c 2cf78e07 197f2d52 d3cb7391 a9ccb2d9 03f722bd 414b0a32 05aa053e
c45e2464 80606f8e 417f09a7 aa9c644d 02030100 01a38202 de308202 da300b06
03551d0f 04040302 05a0301d 0603551d 11041630 14821243 6973636f 4153412e
63697363 6f2e636f 6d301d06 03551d0e 04160414 2c242ddb 490cde1a fe2d63e3
1e1fb28c 974c4216 301f0603 551d2304 18301680 14d9adbf 08f23a88 f114432f
79987cd4 09a403e5 58308201 03060355 1d1f0481 fb3081f8 3081f5a0 81f2a081
ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43 4e3d5453 2d57324b 332d4143
532c434e 3d434450 2c434e3d 5075626c 69632532 304b6579 25323053 65727669
6365732c 434e3d53 65727669 6365732c 434e3d43 6f6e6669 67757261 74696f6e
2c44433d 54535765 622c4443 3d636973 636f2c44 433d636f 6d3f6365 72746966
69636174 65526576 6f636174 696f6e4c 6973743f 62617365 3f6f626a 65637443
6c617373 3d63524c 44697374 72696275 74696f6e 506f696e 74863568 7474703a
2f2f7473 2d77326b 332d6163 732e7473 7765622e 63697363 6f2e636f 6d2f4365
7274456e 726f6c6c 2f434131 2e63726c 3082011d 06082b06 01050507 01010482
010f3082 010b3081 a906082b 06010505 07300286 819c6c64 61703a2f 2f2f434e
3d434131 2c434e3d 4149412c 434e3d50 75626c69 63253230 4b657925 32305365
72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f 6e666967 75726174
696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443 3d636f6d 3f634143
65727469 66696361 74653f62 6173653f 6f626a65 6374436c 6173733d 63657274
69666963 6174696f 6e417574 686f7269 7479305d 06082b06 01050507 30028651
68747470 3a2f2f74 732d7732 6b332d61 63732e74 73776562 2e636973 636f2e63
6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b 332d4143 532e5453 5765622e
63697363 6f2e636f 6d5f4341 312e6372 74302106 092b0601 04018237 14020414
1e120057 00650062 00530065 00720076 00650072 300c0603 551d1301 01ff0402
30003013 0603551d 25040c30 0a06082b 06010505 07030130 0d06092a 864886f7
0d010105 05000382 0101008a 82680f46 fbc87edc 84bc45f5 401b3716 0045515c
2c81971d 0da51fe3 96870627 b41b4319 23284b30 5eafcedb 10c1ef05 d0686a61
cd1ab877 100b965d 499088e1 7de418fb b5529199 46129b81 9c4353a2 1761b61c
f9bc18c6 95c44e5c 8b3cfb71 a183c872 61964433 bddef040 b4b0431e 7456fe29
8a40172d cf3f2e25 f041dee0 c25b7635 29fdbf74 97997a23 340fe65e 75601d32
3522ec61 6aa39020 60f9a50e f963c593 88c80abd 9750e2bb e285933c 53697efd
b1e15148 fcca5cb3 cef27219 e0281fbc acf1c285 2b19b30f 6ea733c4 1f62ff3b
7e309bf7 69b8bb87 8abaf05a 7175cc29 ea7dcc87 7044e279 9b52b759 f02e9b1c
                                                  94be67b8 fb1df0c6 9ec417
                                                                      quit
                                certificate ca 7099f1994764e09c4651da80a16b749c
3082049d 30820385 a0030201 02021070 99f19947 64e09c46 51da80a1 6b749c30
0d06092a 864886f7 0d010105 05003051 31133011 060a0992 268993f2 2c640119
1603636f 6d311530 13060a09 92268993 f22c6401 19160563 6973636f 31153013
060a0992 268993f2 2c640119 16055453 57656231 0c300a06 03550403 13034341
31301e17 0d303731 32313430 36303134 335a170d 31323132 31343036 31303135
5a305131 13301106 0a099226 8993f22c 64011916 03636f6d 31153013 060a0992
268993f2 2c640119 16056369 73636f31 15301306 0a099226 8993f22c 64011916
05545357 6562310c 300a0603 55040313 03434131 30820122 300d0609 2a864886
f70d0101 01050003 82010f00 3082010a 02820101 00ea8fee c7ae56fc a22e603d
0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d 28ece906 02902f9a d1eb2b8d
f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd a1e906ec 88b32a19 38e5353e
6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621 876bd678 c8a37109 f074eabe
2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7 24b9e054 063c60a4 9b8d3c09
351bc630 05f69357 833b9197 f875b408 cb71a814 69a1f331 b1eb2b35 0c469443
1455c210 db308bf0 a9805758 a878b82d 38c71426 afffd272 dd6d7564 1cbe4d95
```

```
        b81c02b2 9b56ec2d 5a913a9f 9b95cafd dfffcf67 94b97ac7 63249009 fa05ca4d
        6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b 5f020301 0001a382 016f3082
        016b3013 06092b06 01040182 37140204 061e0400 43004130 0b060355 1d0f0404
        03020186 300f0603 551d1301 01ff0405 30030101 ff301d06 03551d0e 04160414
        d9adbf08 f23a88f1 14432f79 987cd409 a403e558 30820103 0603551d 1f0481fb
        3081f830 81f5a081 f2a081ef 8681b56c 6461703a 2f2f2f43 4e3d4341 312c434e
        3d54532d 57324b33 2d414353 2c434e3d 4344502c 434e3d50 75626c69 63253230
        4b657925 32305365 72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f
        6e666967 75726174 696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443
        3d636f6d 3f636572 74696669 63617465 5265766f 63617469 6f6e4c69 73743f62
        6173653f 6f626a65 6374436c 6173733d 63524c44 69737472 69627574 696f6e50
        6f696e74 86356874 74703a2f 2f74732d 77326b33 2d616373 2e747377 65622e63
        6973636f 2e636f6d 2f436572 74456e72 6f6c6c2f 4341312e 63726c30 1006092b
        06010401 82371501 04030201 00300d06 092a8648 86f70d01 01050500 03820101
        001abc5a 40b32112 22da80fb bb228bfe 4bf8a515 df8fc3a0 4e0c89c6 d725e2ab
        2fa67ce8 9196d516 dfe55627 953aea47 2e871289 6b754e9c 1e01d408 3f7f0595
        8081f986 526fbe1c c9639d6f 258b2205 0dc370c6 5431b034 fe9fd60e 93a6e71b
        ab8e7f84 a011336b 37c13261 5ad218a3 a513e382 e4bfb2b4 9bf0d7d1 99865cc4
        94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92 860152d4 f06b2b15 df306433
        c1bcc282 80558d70 d22d72e7 eed3195b d575dceb c0caa196 34f693ea f3beee4d
        aa2ef1c2 edba288f 3a678ecb 3809d0df b1699c76 13018f9f 5e3dce95 efe6da93
    f4cb3b00 102efa94 48a22fc4 7e342031 2406165e 39edc207 eddc6554 3fa9f396 ad
                                                                        quit
                                                  crypto isakmp enable outside
                                                    crypto isakmp policy 65535
                                                        authentication rsa-sig
                                                                encryption 3des
                                                                       hash md5
                                                                     group 2
                                                                  lifetime 86400
                                                  crypto isakmp identity auto
                                                              telnet timeout 5
                                                                 ssh timeout 5
                                                               console timeout 0
                                                  threat-detection basic-threat
                                          threat-detection statistics access-list
                                                                              !
                                                      class-map inspection_default
                                                 match default-inspection-traffic
                                                                              !
                                                                              !
                                       policy-map type inspect dns preset_dns_map
                                                                   parameters
                                                    message-length maximum 512
                                                      policy-map global_policy
                                                      class inspection_default
                                                    inspect dns preset_dns_map
                                                                  inspect ftp
                                                           inspect h323 h225
                                                            inspect h323 ras
                                                             inspect netbios
                                                                 inspect rsh
                                                               inspect rtsp
                                                             inspect skinny
                                                              inspect esmtp
                                                             inspect sqlnet
                                                             inspect sunrpc
                                                               inspect tftp
                                                                inspect sip
                                                              inspect xdmcp
                                                                              !
                                                    service-policy global_policy global
```

```
group-policy defaultgroup internal
group-policy defaultgroup attributes
default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
memberof DefaultRAGroup
tunnel-group DefaultRAGroup general-attributes
address-pool vpnpool
tunnel-group DefaultRAGroup ipsec-attributes
trust-point CA1
prompt hostname context
Cryptochecksum:dd6f2e3390bf5238815391c13e42cd21
: end
CiscoASA#
```

تكوين عميل شبكة VPN

أتمت اذه steps in order to شكلت ال VPN عميل.

1. أخترت بدايةجرمانرب>Cisco Systems VPN زبون>VPN زبون in order to أطلقت ال VPN زبون برمجية.

2. أتمت اذه steps in order to جلبت ال CA شهادة من ال CA دان ل يعين CA1، وركبت وه داخل cisco VPN زبون.

   a. قم بإجراء تسجيل الدخول إلى الويب في خادم CA 172.16.5.1 بمساعدة بياناتك. الاعتماد المقدمة إلى المستخدم الظاهري.

   ملاحظة: تأكد من وجود حساب مستخدم لمستخدم عميل شبكة VPN مع خادم CA.

   b. انقر على تنزيل شهادة CA أو سلسلة الشهادات أو CRL لفتح النافذة، كما وه موضح. طقطقت Base 64 السلكي زر بما أن ال يرمز طريقة، وطقطقت تنزيل مرجع مصدق.

   c. احفظ شهادة المرجع المصدق مع اسم certnew.cer على الكمبيوتر. وتم تخزينها بشكل افتراضي في مسار C:\Program Files\Cisco Systems\VPN Client.

   d. في عميل VPN، أختر علامة التبويب شهادات > إستيراد، وانقر فوق الزر إستيراد من Fileradio. انقر على إستعراض لاستيراد شهادة CA من الموقع المخزن في C:\Program Files\Cisco Systems\VPN Client، كما وه موضح.

   انقر فوق استيراد. تظهر نافذة نجاح، كما وه موضح.

   في صفحة الشهادات، تظهر CA Certificates CA1، كما وه موضح.

   ملاحظة: تأكد من إختيار خيار عرض شهادات CA/RA، كما وه موضح، وإلا فإن شهادات CA يجب ألا تظهر في نافذة الشهادة.

3. أتمت اذه steps in order to جلبت الهوية شهادة وركبت وه في ال VPN زبون.

   a. في CA Server CA1، أخترت طلب شهادة متقدم > إنشاء طلب وإرسال طلب شهادة >

إلى هذا CA للتسجيل لشهادة الهوية.

انقر على إرسال.

b.انقر فوق موافق in order to متابعة.

c.انقر على تثبيت هذه الشهادة.

d.انقر فوق موافق in order to متابعة.

e.يجب أن تتلقى رسالة الشهادة المثبتة، كما هو موضح.

f.لتثبيت شهادة الهوية المثبتة، قم بالخروج من عميل VPN وأعد تشغيله من أجل ظهور الشهادة الخاصة بعميل VPN، كما هو موضح.

4.لإدخال vpn مستخدم إنشاء جديد، انقر على إدخالات الاتصال في علامة تبويب الاتصال، كما هو موضح.

- أدخل عنوان IP للنظير البعيد (الموجه) في حقل المضيف.
- انقر على زر مصادقة الشهادة، واختر شهادة الهوية من القائمة المنسدلة، كما هو موضح.
- انقر فوق حفظ.

5.انقر على توصيل.

6.عندما طُلب، ال username وكلمة المرور ل xauth، وانقر فوق ok in order to ربط إلى الشبكة البعيدة.

7.يتصل عميل شبكة VPN مع ASA، كما هو موضح.

التحقق من الصحة

على ال ASA أنت يستطيع أصدرت عدة عرض أمر في الأمر خط in order to تحقق الحالة من شهادة.

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

- يعرض الأمر show crypto ca trustPoint نقاط الثقة التي تم تكوينها.

```
CiscoASA#show crypto ca trustpoints

                 Trustpoint CA1:
                   Subject Name:
                          cn=CA1
                        dc=TSWeb
                        dc=cisco
                          dc=com
Serial Number: 7099f1994764e09c4651da80a16b749c
                 Certificate configured.
```

- يعرض الأمر show crypto ca certificate جميع الشهادات المثبتة على النظام.

```
CiscoASA# show crypto ca certificate
                                                Certificate
                                              Status: Available
                                Certificate Serial Number: 3f14b70b00000000001f
                                        Certificate Usage: Encryption
                                    Public Key Type: RSA (1024 bits)
                                                 Issuer Name:
                                                       cn=CA1
                                                    dc=TSWeb
                                                    dc=cisco
                                                      dc=com
                                               Subject Name:
                                                cn=vpnserver
                                                    cn=Users
                                                    dc=TSWeb
                                                    dc=cisco
                                                      dc=com
                                     PrincipalName: vpnserver@TSWeb.cisco.com
                                                CRL Distribution Points:
 [1]  ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
                                CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
             [2]  http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
                                                Validity Date:
                                     start date: 14:00:36 UTC Dec 27 2007
                                     end   date: 14:00:36 UTC Dec 26 2008
                                        Associated Trustpoints: CA1

                                                  CA Certificate
                                               Status: Available
                        Certificate Serial Number: 7099f1994764e09c4651da80a16b749c
                                           Certificate Usage: Signature
                                    Public Key Type: RSA (2048 bits)
                                                 Issuer Name:
                                                       cn=CA1
                                                    dc=TSWeb
                                                    dc=cisco
                                                      dc=com
                                               Subject Name:
                                                       cn=CA1
                                                    dc=TSWeb
                                                    dc=cisco
                                                      dc=com
                                                CRL Distribution Points:
 [1]  ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
                                CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
             [2]  http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
                                                Validity Date:
                                     start date: 06:01:43 UTC Dec 14 2007
                                     end   date: 06:10:15 UTC Dec 14 2012
                                        Associated Trustpoints: CA1


                                                Certificate
```

```
                                                Subject Name:
                                                  Name: CiscoASA.cisco.com
                                              Status: Pending terminal enrollment
                                                      Key Usage: General Purpose
                                    Fingerprint:  1a022cf2 9771e335 12c3a530 1f9a0345
                                                      Associated Trustpoint: CA1
```

- يعرض الأمر show crypto ca crls قوائم إبطال الشهادات المخزنة مؤقتا (CRL).
- يعرض الأمر show crypto key mypubkey rsa جميع أزواج مفاتيح التشفير التي تم إنشاؤها.

```
                                                CiscoASA# show crypto key mypubkey rsa
                                              Key pair was generated at: 01:43:45 UTC Dec 11 2007
                                                        Key name: <Default-RSA-Key>
                                                        Usage: General Purpose Key
                                                         Modulus Size (bits): 1024
                                                                Key Data:

     30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509
     99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541
     f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b
     4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4 adeeb248 a10b1f68
2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001
                                              Key pair was generated at: 06:36:00 UTC Dec 15 2007
                                                        Key name: my.CA.key
                                                        Usage: General Purpose Key
                                                         Modulus Size (bits): 1024
                                                                Key Data:

     30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a
     a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7
     545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905
     5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2
d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001
                                              Key pair was generated at: 07:35:18 UTC Dec 21 2007
                                                                CiscoASA#
```

- يعرض الأمر show crypto isakmp sa معلومات نفق IKE 1.

```
                                        CiscoASA#show crypto isakmp sa

                                                              Active SA: 1
     Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
                                                          Total IKE SA: 1

                                                  1   IKE Peer: 10.1.1.5
                                      Type    : user            Role    : responder
                                      Rekey   : no              State   : MM_ACTIVE
```

- يعرض الأمر show crypto ipSec sa معلومات نفق IPSec.

```
CiscoASA#show crypto ipsec sa
                                    interface: outside
            Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5

                local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
        remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0)
                                current_peer: 10.1.1.5, username: vpnuser
                                    dynamic allocated peer ip: 10.5.5.10

                          #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
                        #pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144
                                #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
            #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
        #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
                                        #send errors: 0, #recv errors: 0

                local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5

                          path mtu 1500, ipsec overhead 58, media mtu 1500
                            current outbound spi: FF3EEE7D

                                         inbound esp sas:
                                      spi: 0xEFDF8BA9 (4024404905)
                                transform: esp-3des esp-md5-hmac none
                                     in use settings ={RA, Tunnel, }
                            slot: 0, conn_id: 4096, crypto-map: dynmap
                        sa timing: remaining key lifetime (sec): 28314
                                         IV size: 8 bytes
                                 replay detection support: Y
                                        outbound esp sas:
                                      spi: 0xFF3EEE7D (4282314365)
                                transform: esp-3des esp-md5-hmac none
                                     in use settings ={RA, Tunnel, }
                            slot: 0, conn_id: 4096, crypto-map: dynmap
                        sa timing: remaining key lifetime (sec): 28314
                                         IV size: 8 bytes
                                 replay detection support: Y
```

تدعم أداة مترجم الإخراج (للعملاء المسجلين فقط) بعض أوامر show. استعمل الـ OIT in order to شاهدت تحليل من عرض أمر إنتاج.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

فيما يلي بعض الأخطاء المحتملة التي يمكنك مواجهتها:

- خطأ: فشل تحليل الشهادة المستوردة أو التحقق منها

يمكن أن يحدث هذا الخطأ عندما تقوم بتثبيت شهادة الهوية وليس لديك شهادة CA

الوسيطة أو الجذر الصحيحة التي تم مصادقتها مع TrustPoint المقترنة. يجب عليك إزالة وإعادة المصادقة باستخدام شهادة CA الوسيطة أو الجذر الصحيحة. اتصل بمورد الجهة الخارجية للتحقق من حصولك على شهادة المرجع المصدق الصحيحة.

- الشهادة التي تحتوي على مفاتيح عام للأغراض العامة

قد يحدث هذا الخطأ عند محاولة تثبيت شهادة هوية في TrustPoint غير صحيح. تحاول تثبيت شهادة هوية غير صحيحة، أو أن زوج المفاتيح المقترن بـ TrustPoint لا يطابق المفاتيح العامة الموجودة في شهادة الهوية. قم بإصدار الأمر show crypto ca certificates trustPointName للتحقق من تثبيت شهادة هوية على TrustPoint الصحيح. ابحث عن السطر الذي يحدد نقاط الثقة المرتبطة: إذا تم سرد نقطة الثقة غير الصحيحة، فاستخدم الإجراءات الموضحة في هذا المستند لإزالة نقطة الثقة المناسبة وإعادة تثبيتها. تحقق أيضا من عدم تغيير زوج المفاتيح منذ إنشاء CSR.

- خطأ: ASA/PIX. SEV=Warning/3 IKE/0xE300081 معرف شهادة عن بعد غير صالح:

إن تلقى أنت صحة هوية مشكلة مع شهادة، هذا خطأ رسالة يستطيع ظهرت في الـ VPN زبون. أستخدم الأمر crypto isakmp identity auto في تكوين ASA/PIX لحل المشكلة.

معلومات ذات صلة

- صفحة دعم أجهزة الأمان المعدلة من Cisco
- صفحة دعم عميل شبكة VPN من Cisco
- تكوين خادم Microsoft كمرجع للشهادة (CA)
- الدعم التقني والمستندات - Cisco Systems

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).