ASA 8.x: ةداەش تيبثتو ديدجت SSL مادختساب ASDM

المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>الاحراء</u> <u>التحقق من الصحة</u> <u>استكشاف الأخطاء وإصلاحها</u> <u>كيفية نسخ شهادات SSL من ASA إلى آخر</u> <u>معلومات ذات صلة</u>

<u>المقدمة</u>

الإجراء الوارد في هذا المستند هو مثال ويمكن إستخدامه كدليل إرشادي مع أي مورد شهادات أو خادم شهادات رئيسي خاص بك. قد يتطلب مورد الشهادة الخاص متطلبات معلمة الشهادة الخاصة، ولكن هذا المستند يهدف إلى توفير الخطوات العامة المطلوبة لتجديد شهادة SSL وتثبيتها على ASA الذي يستخدم برنامج 8.0.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

لا توجد متطلبات خاصة لهذا المستند.

<u>المكونات المستخدمة</u>

يتعلق هذا الإجراء بإصدارات ASA 8.x مع الإصدار 6.0(2) من ASDM أو الإصدارات الأحدث.

يستند الإجراء الوارد في هذا المستند إلى تكوين صالح مع تثبيت شهادة واستخدامها للوصول إلى SSL VPN. لا يؤثر هذا الإجراء على شبكتك طالما لم يتم حذف الشهادة الحالية. هذا الإجراء هو عملية تدريجية حول كيفية إصدار CSR جديد لشهادة حالية بنفس شهادة الجذر التي أصدرت المرجع المصدق الجذر الأصلي.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

<u>الإجراء</u>

أكمل الخطوات التالية:

1. حدد الشهادة التي تريد تجديدها تحت التكوين > إدارة الأجهزة > شهادات الهوية، ثم انقر على **إضافة.شكل 1**

G Cisco ASDM 6.1 for ASA - 172	.16.242.232		
<u>File Yew Tools Wigards Window</u>	v ∐elp	Look Far:	© alatha
🚮 Home 🖓 Configuration 🔯 M	mitoring 🔚 Sava 🔇 Refresh 🔇 Back 🕥 Forma	rd 🦻 Help	CISCO
Device Management 🖃 🕀 🔀	Configuration > Device Management > Certificate M	lanagement > Identity Certificates	
🖶 🌈 Management Access			
🖶 🎯 High Availability	Issued To Issued By	Expiry Date	Usage Add
🖶 🚮 Users/AAA		00:00:15 01C Har 11 2009	_ Show Details _
End Certificate Management			Delete
Edentity Certificates			Export
🕀 📕 DNS			Instal
m 🔊 vavaucea			Refresh
	Identity certificate can be used to authenticate SSL, such to make such configuration.	as ASDM, access to the security appliance of	n a given interface. You can go to <u>59, Settings</u>
	to mere such comparation		
A Device Setup			
Freedal			
Remote Access VPN			
🙀 Ste-to-Site VPN			
Device Management			
2		Apply Reset	
Device configuration refreshed successfu	ly.	riscol 15	🗟 🜆 📊 🛛 🔒 8/29/08 8:52:53 PM UTC

2. تحت إضافة شهادة هوية، حدد زر **إضافة شهادة هوية جديدة**، واختر زوج المفاتيح من القائمة المنسدلة.**ملاحظة:** لا يوصى باستخدام <default-RSA-key> لأنك إذا قمت بإعادة إنشاء مفتاح SSH الخاص بك، فأنك تبطل ترخيصك. إذا لم يكن لديك مفتاح RSA، فأكمل الخطوتين A و B. وإلا استمر في الخطوة 3.**شكل 2**

🖆 Add Identity Certificat	e 🔀
🔵 Import the identity certifi	cate from a file:
Decryption Passphrase:	
File to Import From:	Browse
 Add a new identity certifi 	cate:
Key Pair:	CertKey 🖌 Show New
Certificate Subject DN:	ASA5540.company.com Select
Generate self-signed	certificate
Act as local certifi	cate authority and issue dynamic certificates to TLS-Proxy
	Advanced
Add Certific	ate Cancel Help

(إختياري) أكمل هذه الخطوات إذا لم يكن لديك مفتاح RSA تم تكوينه بعد، وإلا فانتقل إلى الخطوة 3.طقطقت **جديد..**.أدخل اسم زوج المفاتيح في حقل **إدخال اسم زوج مفاتيح جديد**، وانقر **إنشاء الآنِ.شكل 3**

🕵 Add K	ey Pair 🛛 🔀
Name:	🔘 Use default key pair name
	Enter new key pair name: Certkey
Size:	1024
Usage:	💿 General purpose 💦 Special
G	enerate Now Cancel Help

- 3. انقر فوق **تحديد**.
- 4. أدخل سمات الشهادة المناسبة كما هو موضح في الشكل 4. طقطقت ما إن يتم، o<mark>k. ثم انقر على **إضافة** شهادة.الشكل 4</mark>

🚰 Certificate Subject DN 🛛 🛛 💽			×			
				Attribute	Value	
ON Attribute to be Added				Common Name (CN)	ASA5540.comp	
	Attribute:	Common Name (CN) 💌	Add>>	Company Name (O)	Cisco Systems	
	Value:	Common Name (CN)	Delete	Country (C)	US	
	Tanato I	Department (OU) Company Name (O) Country (C) State (St)	Delete	State (St)	CA	
		Location (L) Email Address (EA)				
OK Cancel Help						

إخراج واجهة سطر الأوامر:

crypto ca trustpoint ASDM_TrustPoint0 keypair CertKey id-usage ssl-ipsec

	crypto ca enroll ASDM_TrustPoi	int0
	enrollment terminal	
subject-name	CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA	
	fqdn 5540-uwe	
	id-usage ssl-ipsec	

5. في الإطار المنبثق **طلب شهادة الهوية**، احفظ طلب توقيع الشهادة (CSR) في ملف نصي، وانقر **موافق.شكل 5**

🖆 Identity Certificate Request 🛛 🛛 🔀		
To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.		
You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.		
Save CSR to file: C:\Certificates\ASACertCSR.txt Browse		
OK Cancel Help		

6. (إختياري) تحقق في ASDM من أن CSR معلق، كما هو موضح في الشكل 6.**الشكل 6**

🛸 Cisco ASDM 6.1 for ASA - 172.16.242.232					
<u>File View Tools Wigards Window</u>	v Help		Look Par:	Go	alada
📣 Home 🗞 Configuration 🔯 M	onitoring 🛄 Sava 🙉 Refres	th 🙆 Back 🕥 Forward	🤊 Help		cisco
Device Management 31 4 X	Configuration > Device Many	agement > Certificate Mana	• • • • • • • • • • • • • • • • • • •		
E C Management Access	Comparison as a second second	opening in a second money i purse	Contractor - Anderson - Anderson		_
🖶 🍰 System Image/Configuration					
🖶 🎯 High Availability	Issued To	Issued By	Expiry Date	Usage	. Add
E Coging	[on=*.vpnt.com]	[m=MS-CA]	00:03:16 UTC Mar 11 2009	General Purpose	Show Details
E Certificate Management	(AsAsAccorpany.com)	[Incompania]	Parking or	Unknown	
- A Certificates					Delete
E Contractes					Export
🕀 🚚 DNS					Instal
🗉 📆 Advanced					Defeet
					- Norresal
	Identity certificate can be use	ed to authenticate SSL, such as A	SDM, access to the security appliant	te on a given interface. You can g	o to <u>55. Settinos</u>
	to make such configuration.				
A Device Setup					
Eyosal					
Remote Access VPN					
🚰 Ske-to-Site VPN					
🔣 Device Management					
20 V			Apply Reset		
Configuration changes saved successfully	6		ciscol 15	🗟 🚂 📊 🛛 🔒 🕯	/29/08 9:56:23 PM UTC

- 7. أرسل طلب الشهادة إلى مسؤول الشهادة الذي يصدر الشهادة على الخادم. يمكن أن يكون ذلك من خلال واجهة ويب، بريد إلكتروني، أو مباشرة إلى خادم CA الجذر لعملية إصدار الشهادة.
- 8. أكمل هذه الخطوات لتثبيت الشهادة المتجددة.حدد طلب الشهادة المعلقة تحت تشكيل > إدارة الأجهزة > شهادات الهوية، كما هو موضح في الشكل 6، وانقر **تثبيت**.في نافذة "تثبيت شهادة الهوية"، حدد **زر** الخيار **لصق بيانات الشهادة بتنسيق 64-base**، وانقر على **تثبيت الشهادة.ملاحظة:** بدلا من ذلك، إذا تم إصدار الشهادة في ملف .cer بدلا من ملف نصي أو بريد إلكتروني، يمكنك أيضا تحديد **تثبيت من ملف**، والتصفح إلى الملف المناسب على الكمبيوتر، وانقر فوق **تثبيت ملف شهادة المعرف** ثم انقر فوق **تثبيت الشهادة.**

🖆 Install Identity certificate 🛛 🛛 🔀
Identity Certificate
Install from a file: Browse Browse Browse
Ng9SqvsXWWkJmS8ss9Qvz5D+K2uSLPcEAuuT7JhUVC1jbTZh1GLpqBheEeMk/8jY fui6ZdrSloUbodDEy6IiodF8QeQgCEdl1omR5W9bP5t2aTPT5J7lG3ckEM0kseqC wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa 6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== END CERTIFICATE
Install Certificate Cancel Help

خراج واجهة سطر الأوامر:

crypto ca import ASDM_TrustPoint0 certificate

WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ

output truncated wPevLEO16TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa ---!
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit

9. يظهر إطار يؤكد أن الشهادة مثبتة بنجاح. انقر فوق "موافق" للتأكيد.**الشكل 8**

🕵 Informa	tion 🛛 🔀
į	Certificate import succeeded.
	ОК

10. تأكد من ظهور شهادتك الجديدة تحت شهادات الهوية.**الشكل 9**



11. أتمت هذا steps in order to ربطت الشهادة الجديدة إلى القارن:أختر **التكوين > إدارة الأجهزة > خيارات متقدمة > إعدادات SSL**، كما هو موضح في الشكل 10.حدد الواجهة الخاصة بك تحت الشهادات، وانقر **تحرير.الشكل 1**0

😤 Cisco ASDM 6.1 for ASA - 172.16.242.232				
<u>File Yew Tools Wigards Window</u>	Help		Look Far:	6 allulu
🚮 Home 🦓 Configuration 📴 Mo	mitoring 🔚 Sava 🔇 Refresh 🔇	Back 🕥 Forward 🦻 Halp		CISCO
Device Management 🖃 🕂 🔀	Configuration > Device Manageme	nt > Advanced > SSL Settings		
High Availability High Availability High Availability Counting	Configure SSL parameters. These parameters SSL Version: Any Encryption Available Algorithms RC4-405 DES-SHAL DES DES-SHAL DES-SHA	Add >> Clent SSL Version: Add >> Add >> Add >> Clent SSL Version: Add >> Clent SSL version: Add >> Clent SSL version: Clent SSL version: Version: Version:	N access. Active Algorithms Active Algorithms RC4-SHA1 ACS128-SHA1 ACS28-SHA1 ACS256-SHA3 access. R each interface. The fallback certificate will Load Balancing Trustpoint	be used on interfaces not
💑 Device Setup				
Firewall				
Remote Access VPN	Falback Certificate: None		¥	
🙀 Ske-to-Site VPN				
Device Menagement				
» v		Apply	Reset	
Configuration changes saved successfully		cisco 1	15 🐻 🛃 🚮	8/29/08 10:08:53 PM UTC

12. أختر ترخيصك الجديد من القائمة المنسدلة، وانقر موافق، وانقر تطبيق. ssl encryption rc4-shal aes128-shal aes256-shal 3des-shal ssl trust-point ASDM_TrustPoint0 outside

	الشكل 11		
🖆 Select SSL Certificate 🛛 💽			
Specify enrolled trustpoints to be us interface. To enroll a trustpoint, go l Certificate > Enrollment.	ed for SSL authentication and VPN load balancing on the outside to Configuration > Features > Device Administration >		
Interface:	outside		
Primary Enrolled Certificate:	[cn=ASA5540.company.com, ou=LAB, o=Cisco Systems, 💌		
Load Balancing Enrolled Certificate:	None [cn=*.vpn1.com]:[cn=MS-CA]: 611f8630000000000026		
ОК	[cn=ASA5540.company.com, ou=LAB, o=Cisco Systems,		

13. احفظ التكوين الخاص بك في ASDM أو على واجهة سطر الأوامر.

<u>التحقق من الصحة</u>

يمكنك إستخدام واجهة سطر الأوامر (CLI) للتحقق من تثبيت الشهادة الجديدة على ASA بشكل صحيح، كما هو موضح في إخراج النموذج هذا:

```
ASA(config)#show crypto ca certificates
Certificate
Status: Available
Certificate Serial Number: 61bf707b00000000027
Certificate Usage: General Purpose
(Public Key Type: RSA (1024 bits
:Issuer Name
cn=MS-CA
:Subject Name
```

cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems st=CA c=US CRL Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\\win2k3basel\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008 end date: 22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate Status: Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage: Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---'old' certificate CRL Distribution Points: [1] http://win2k3-basel/CertEnroll/MS-CA.crl [2] file://\\win2k3-basel\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006 end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available Certificate Serial Number: 611f86300000000026 Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points: [1] http://win2k3-basel\CertEnroll\MS-CA.crl [2] file://\\win2k3-basel\CertEnroll\MS-CA.crl Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009 #(Associated Trustpoints: test ASA(config

استكشاف الأخطاء وإصلاحها

(إختياري) تحقق على واجهة سطر الأوامر (CLI) من تطبيق الشهادة الصحيحة على الواجهة:

ASA(config)**#show running-config ssl** ssl trust-point ASDM_TrustPoint0 outside Shows that the correct trustpoint is tied to the outside interface that terminates SSL VPN. ---! #(ASA(config

<u>كيفية نسخ شهادات SSL من ASA إلى آخر</u>

يمكن القيام بذلك إذا قمت بإنشاء مفاتيح قابلة للتصدير. تحتاج لتصدير الترخيص إلى ملف PKCS. ويتضمن ذلك تصدير جميع المفاتيح المقترنة.

أستخدم هذا الأمر لتصدير شهادتك عبر CLI:

ASA(config)#crypto ca export

ملاحظة: عبارة المرور - تستخدم لحماية ملف PKCS12.

أستخدم هذا الأمر لاستيراد ترخيصك عبر CLI:

SA(config)#crypto ca import

ملاحظة: يجب أن تكون عبارة المرور هذه هي نفسها المستخدمة عند تصدير الملف.

كما يمكن القيام بذلك من خلال ASDM لزوج تجاوز فشل ASA. أكمل الخطوات التالية لتنفيذ ما يلي:

- 1. قم بتسجيل الدخول إلى ASA الأساسي عبر ASDM واختر **أدوات—> تكوين النسخ الاحتياطي**.
 - 2. يمكنك نسخ كل شيء إحتياطيا أو الشهادات فقط.
 - 3. في وضع الاستعداد، افتح ASDM واختر **أدوات —> إستعادة التكوين**.

<u>معلومات ذات صلة</u>

- <u>صفحة دعم أجهزة الأمان المعدلة (ASA) من Cisco</u>
- ASA 8.x يركب يدويا شهادات مورد الطرف الثالث للاستخدام مع مثال تكوين WebVPN
 - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما