مادختساب Cisco VPN Client و PIX نيب IPSec تاداەش نيوكت لاتم

المحتويات

<u>المقدمة</u> المتطلبات الأساسية <u>المكونات المستخدمة</u> <u>الاصطلاحات</u> <u>تسجيل PIX وتكوينه</u> <u>التكوينات</u> <u>تموين عميل MPX من Cisco والاتصال ب PIX</u> <u>تثييت برامج تشغيل البطاقة الذكية من eToken</u> <u>التحقق من الصحة</u> <u>استكشاف الأخطاء وإصلاحها</u> <u>معلومات ذات صلة</u>

<u>المقدمة</u>

يوضح هذا المستند كيفية تكوين نفق IPSec VPN بين جدار حماية PIX وعميل Cisco VPN 4.0.x. كما يسلط مثال التكوين في هذا المستند الضوء على إجراء تسجيل مرجع التصديق (CA) لكل من موجه Cisco IOS® وعميل Cisco VPN، بالإضافة إلى إستخدام البطاقة الذكية كتخزين شهادات.

ارجع إلى <u>تكوين IPSec بين موجهات Cisco IOS وعميل Cisco VPN باستخدام شهادات Entrust</u> لمعرفة المزيد حول تكوين IPSec بين موجهات Cisco IOS وعميل Cisco VPN باستخدام شهادات Entrust.

ارجع إلى <u>تكوين هيئات شهادات الهوية المتعددة على موجهات Cisco IOS</u> لمعرفة المزيد حول تكوين هيئات شهادات الهوية المتعددة على موجهات Cisco IOS.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

لا توجد متطلبات خاصة لهذا المستند.

<u>المكونات المستخدمة</u>

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

• جدار حماية Cisco PIX الذي يشغل البرنامج الإصدار 6.3(3)

• Cisco VPN Client 4.0.3 على كمبيوتر يعمل بنظام التشغيل Windows XP

• يستخدم خادم Microsoft Windows 2000 CA في هذا المستند كخادم CA.

• يتم تخزين الشهادات الموجودة على عميل Cisco VPN باستخدام البطاقة الذكية <u>Aladdin</u> e-Token.

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

<u>الاصطلاحات</u>

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

<u>تسجيل PIX وتكوينه</u>

في هذا القسم، تقدم لك المعلومات لتكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم <u>أداة بحث الأوامر</u> (<u>للعملاء</u> المسجلين فقط).

<u>التكوينات</u>

يستخدم هذا المستند هذه التكوينات.

- <u>تسجيل الشهادة على جدار حماية PIX</u>
 - <u>تكوين جدار حماية PIX</u>

تسجيل الشهادة على جدار حماية PIX
Define a hostname and domain name for the router! ! The fully qualified domain name (FQDN) is used ! as the identity of the router during certificate enrollment. pix(config) #hostname sv2-11
sv2-11(config)#domain-name cisco.com
Confirm that you have the correct time set on the!
Clock set
This command clears the PIX RSA keys. ca zeroize! rsa
Generate RSA (encryption and authentication) keys!
ca gen rsa key
Select the modulus size (512 or 1024). ! Confirm!
the keys generated. show ca mypub rsa
Define the CA identity. Ca ident Kobe!
IU.I.I.2:/Certsrv/mscep/mscep.dll
ca comi nobe la 1 20 chopt
[ca enroll kobe [ipaddress
Confirm the certificate and validity. show ca cert!
تکوین جدار حمایة PIX

(PIX Version 6.3(3 interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto shutdown interface ethernet3 auto shutdown interface ethernet4 auto shutdown interface ethernet5 auto shutdown nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 intf2 security4 nameif ethernet3 intf3 security6 nameif ethernet4 intf4 security8 nameif ethernet5 intf5 security10 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname sv2-11 domain-name cisco.com fixup protocol dns maximum-length 512 fixup protocol ftp 21 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol http 80 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol sip 5060 fixup protocol sip udp 5060 fixup protocol skinny 2000 fixup protocol smtp 25 fixup protocol sqlnet 1521 fixup protocol tftp 69 names access-list 101 permit tcp any host 209.165.201.21 eq www access-list 120 permit ip 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 pager lines 24 mtu outside 1500 mtu inside 1500 mtu intf2 1500 mtu intf3 1500 mtu intf4 1500 mtu intf5 1500 ip address outside 209.165.201.20 255.255.255.224 ip address inside 10.1.1.10 255.255.255.0 ip address intf2 127.0.0.1 255.255.255.255 no ip address intf3 no ip address intf4 no ip address intf5 ip audit info action alarm ip audit attack action alarm ip local pool vpnpool 10.0.0.10-10.0.0.100 no failover failover timeout 0:00:00 failover poll 15 no failover ip address outside no failover ip address inside no failover ip address intf2 no failover ip address intf3 no failover ip address intf4 no failover ip address intf5 pdm history enable

arp timeout 14400 nat (inside) 0 access-list 120 static (inside,outside) 209.165.201.21 10.1.1.2 netmask 255.255.255.255 0 0 access-group 101 in interface outside route outside 0.0.0.0 0.0.0.0 209.165.201.30 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute +aaa-server TACACS+ protocol tacacs aaa-server RADIUS protocol radius aaa-server LOCAL protocol local no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable sysopt connection permit-ipsec 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 isakmp enable outside isakmp policy 10 authentication rsa-sig isakmp policy 10 encryption 3des isakmp policy 10 hash md5 isakmp policy 10 group 2 isakmp policy 10 lifetime 86400 vpngroup vpncert address-pool vpnpool vpngroup vpncert idle-time 1800 ******* vpngroup vpncert password ca identity kobe 10.1.1.2:/certsrv/mscep/mscep.dll ca configure kobe ra 1 20 crloptional telnet timeout 5 ssh timeout 5 console timeout 0 terminal width 80 Cryptochecksum: 2ae252ac69e5218d13d35acdf1f30e55 end : [OK] #(sv2-11(config

<u>تسجيل شهادات عميل شبكة VPN من Cisco</u>

تذكر تثبيت جميع برامج التشغيل والأدوات المساعدة اللازمة الواردة مع جهاز البطاقة الذكية على الكمبيوتر الشخصي المراد إستخدامه مع عميل شبكة VPN من Cisco.

توضح هذه الخطوات الإجراءات المستخدمة لتسجيل عميل Cisco VPN لشهادات MS. يتم تخزين الشهادة على مخزن <u>Aladdin</u> e-Token Smartcard.

- 1. قم بتشغيل متصفح وانتقل إلى صفحة خادم الشهادات (http://CAServeraddress/certsrv/، في هذا المثال).
 - 2. حدد **طلب شهادة** وانقر **التالي**.

Address 🕘 http://209.165.201.21/certsrv/

Microsoft Certificate Services -- kobe

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

→ Go

Lin

Home

Select a task:

- O Retrieve the CA certificate or certificate revocation list
- Request a certificate
- O Check on a pending certificate

	Next >
طلب ، حدد طلب متقدم وانقر بعد	3. في نافذة إختيار نوع الد ذلك .
Microsoft Certificate Services kobe	<u>Home</u>
Choose Request Type	
Please select the type of request you would like to make:	
 User certificate request: 	
Web Browser Certificate E-Mail Protection Certificate	
 Advanced request 	
	Next >

 4. حدد إرسال طلب شهادة إلى المرجع المصدق هذا باستخدام نموذج وانقر بعد ذلك.

Microsoft Certificate Services kobe	<u>Home</u>
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a co following methods. Note that the policy of the certification author the certificates that you can obtain.	mputer using one of the ority (CA) will determine
 Submit a certificate request to this CA using a form. 	
 Submit a certificate request using a base64 encoded PK0 renewal request using a base64 encoded PKCS #7 file. 	CS #10 file or a
Request a certificate for a smart card on behalf of another Card Enrollment Station. You must have an enrollment agent certificate to submit a request for	user using the Smart or another user.
	Next >

5. املأ كل العناصر في نموذج طلب الشهادة المتقدمة.تأكد من أن القسم أو الوحدة التنظيمية (OU) تتوافق مع اسم مجموعة عملاء شبكة VPN من Cisco، كما تم تكوينها في اسم مجموعة PIX vpn. حدد موفر خدمة الشهادات الصحيح (CSP) المناسب للإعداد الخاص بك.

Microsoft Certific	cate Services kobe		Home
Advanced Ce	rtificate Request		
Identifying Infor	mation:		
identifying mon		1	
Name:	ericetoken		
E-Mail:			
Company:	cisco]	
Department:	vpncert		
City:	ctd]	
State:	nsw].	
Country/Region:	AU		
Intended Purpos	e:		
	Client Authentication Certificate 💌		
Key Ontions			
nej options.			
CSP:	e loken Base Cryptographic Provider	×	
Key Usage:	○Exchange ○Signature ⑧Both		
Key Size:	512 Min: 384 (common key sizes: <u>512</u> <u>1024</u>) Max:1024		
	Oreate new key set		
	Set the container name		
	◯ Use existing key set		
	Enable strong private key protection		
	Mark keys as exportable		
	Use local machine store		
Additional Ontio	You must be an administrator to generate		
		2.0	
Hash Algorithm:	SHA-1 Only used to sign request.		
	Save request to a PKCS #10 file		
-4 L1	<u>^</u>		
Attributes:	< <u>></u>		
		Submit	>

6. حدد **نعم** لمتابعة التثبيت عند الحصول على تحذير التحقق من صحة البرامج النصية المحتملة.

Potential Scripting Violation	\mathbf{X}
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to reque certificate for you. Do you want to request a certificate now?	est a
Yes No	
تسجيل الشهادة باستدعاء مخزن eToken. أدخل كلمة المرور وانقر فوق	7. يقوم ت
eToken Base Cryptographic Provider	
eToken	
Input eToken password	
eToken: [eToken [AKS ifdh 0]	
Password: ******	
Login to your eToken to enable using/creating/removing your private key.	- 61
لى تثبيت هذه -	مواقق 8. انقر عا
.ö. Microsoft Certificate Services kobe H	الشهاد ome
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	

9. حدد **نعم** لمتابعة التثبيت عند الحصول على تحذير التحقق من صحة البرامج النصية المحتملة.

Potential S	cripting Violation
L CC yr D	his Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your ertificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that ou do not trust to run on this computer and gain access to your data. o you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
	ـــــــــــــــــــــــــــــــــــــ
Root C	ertificate Store 🔀
1	Do you want to ADD the following certificate to the Root Store? Subject : kobe, vpn, apt-vpn, ctd, nsw, AU Issuer : Self Issued

Time Validit	y : Monday, 25 August 2003 through Thursday, 25 August 200
Serial Numb	per : 43C2EE28 43CE56A6 4457F2D2 23EDFED2
Thumbprint	(sha1): 3D47C8F6 2703B88D C2BD4F68 7B5300A0 3A927B4E
Thumbprint	(md5) : A1E23E81 08538FA4 6BB4F187 49EC774F

No

Yes

11. يظهر إطار الشهادة المثبتة ويؤكد التثبيت

الجذري



12. أستخدم عارض تطبيق الرمز المميز لعرض الشهادة المخزنة على البطاقة الذكية.

🚍 eToken Propertie	5				
eToken					
×	Advanced 🕗 Ref	resh 김 Help			
ето	ken [PRO]				
Local Machine	etails Settings Cert	ificates & keys			
	ericetoken		Delete		
	C Exchange key <beb2b14a-e935-4476-bfb3-8e22d95< td=""></beb2b14a-e935-4476-bfb3-8e22d95<>				
eToken [AKS if					
	Version	V3			
	Serial number	11 00 00 00 00 00 5d 41 81 23			
	Signature algorithm	RSA_SHA1RSA	· 🖽 👘		
	Valid from	Tuesday, 14 October 2003 2:24:58 AM	-		
	Valid to	Thursday, 14 October 2004 2:34:58 AM			
	Subject Key container	AU, nsw, ctd, cisco, vpncert, ericetoken beb2b14a.e935.4476.bfb3.8e22d95e3d19	~		
			Bafraah		
			- Herresh		
			More		

<u>تكوين عميل Cisco VPN لاستخدام الشهادة للاتصال ب PIX</u>

توضح هذه الخطوات الإجراءات المستخدمة لتكوين عميل Cisco VPN لاستخدام الشهادة لاتصالات PIX.

1. قم بتشغيل عميل Cisco VPN. تحت "إدخالات الاتصال" انقر فوق **جديد** لإنشاء اتصال جديد.

onnection Entries Status	Certificates Log	Options Help	
<u>Connect to to_pix</u>	Ctrl+O	a 🔀	Cisco Systems
Disconnect	Ctrl+D	nditu Delete	مناتق منابة
Create Shortcut		-pairy Delete	
Modify		Host	Tran
D <u>e</u> lete		11030	
Dyplicate			
Set as Default Connect	ion Entry		
<u>N</u> ew			
Import	20	_	
Exit VPN Client	Ctrl+Q		i .
1			<u> </u>
Connection Entry: to	_pix		
Connection Entry: to Description: co <u>H</u> ost: 20	_pix Innection to pix		
Connection Entry: to Description: co <u>H</u> ost: 20 Authentication	_pix Innection to pix 19.165.201.20 Transport Back	up Servers Dial-Up	
Connection Entry: to Description: co Host: 20 Authentication	_pix Innection to pix 19.165.201.20 Transport Back cation	kup Servers Dial-Up	
Connection Entry: to Description: co <u>H</u> ost: 20 Authentication	_pix onnection to pix 19.165.201.20 Transport Back cation	up Servers Dial-Up	
Connection Entry: to Description: co <u>H</u> ost: 20 Authentication <u>G</u> roup Authention <u>N</u> ame: <u>P</u> assword:	_pix onnection to pix 19.165.201.20 Transport Back cation	kup Servers Dial-Up	
Connection Entry: to Description: co Host: 20 Authentication <u>G</u> roup Authentio Name: Password: Confirm Passwor	_pix Innection to pix 19.165.201.20 Transport Back cation	kup Servers Dial-Up	
Connection Entry: to Description: co Host: 20 Authentication Mame: Password: Confirm Password Confirm Password	_pix onnection to pix 19.165.201.20 Transport Back cation d:	up Servers Dial-Up	
Connection Entry: to Description: co Host: 20 Authentication Mame: Password: Confirm Password Name: Ferreetor	_pix onnection to pix 19.165.201.20 Transport Back cation d: entication	kup Servers Dial-Up	
Connection Entry: to Description: co Host: 20 Authentication Mame: Password: Confirm Password Confirm Password Mame: encetor	_pix onnection to pix 09.165.201.20 Transport Back cation d: entication tificate Chain	cup Servers Dial-Up	
Connection Entry: to Description: co Host: 20 Authentication Mame: Password: Confirm Password Confirm Password Mame: Pricetok Mame: Certificate Author	_pix Innection to pix I9.165.201.20 Transport Back cation d:	kup Servers Dial-Up	
Connection Entry: to Description: co Host: 20 Authentication Name: Password: Confirm Password Name: ericetok Name: ericetok	_pix Innection to pix 19.165.201.20 Transport Back cation d:	up Servers Dial-Up	

3. أخترت in order to بدأت ال cisco VPN زبون توصيل إلى ال PIX، ال مرغوب توصيل مدخل وطقطقة **توصيل**.

🤌 VPN Client - Versio	n 4.0.3 (Rel)		
Connection Entries Status	Certificates Log	Options Help	a tita an and
Connect to to_pix	Ctrl+O	a 🔀	CISCO SYSTEMS
<u>D</u> isconnect	Ctrl+D	ndifu Delete	ale die
C <u>r</u> eate Shortcut			
Modiry		Host	Trans
D <u>e</u> lete		209.165.201.20	IPSe
Dyplicate			
Set as Default Connect	ion Entry	-	
<u>N</u> ew			
Import			
E <u>x</u> it VPN Client	Ctrl+Q		
		-	
Not connected.			/

<u>تثبيت برامج تشغيل البطاقة الذكية من eToken</u>

توضح هذه الخطوات تثبيت برامج تشغيل <u>Aladdin</u> eToken Smartcard.

1. افتح معالج إعداد بيئة وقت تشغيل eToken 3.51.



اقبل شروط إنفاقية الترح. التالي.



🙀 eToken Run Time Environment 3	3.51 Setup 📃 🗖 🔀
Ready to Install the Application Click Next to begin installation.	eToken Your Key to eSecurity RTE
	Please click Next to begin installation.
	<pre></pre>

4. تم تثبيت برامج تشغيل البطاقة الذكية من eToken الآن. انقر فوق **إنهاء**" للخروج من معالج الإعداد.



<u>التحقق من الصحة</u>

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** <u>أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل</u> إ<u>خراج أمر</u> العرض.

• **show crypto isakmp sa –** يعرض جميع اقترانات أمان تبادل مفتاح الإنترنت (IKE) الحالية (SAs) في نظير. SV2-11(config)#**show crypto isa sa** Total : 1

> Embryonic : 0 pending dst state created src QM_IDLE 0 1 209.165.201.19 209.165.201.20 • show crypto ipSec—يعرض الإعدادات المستخدمة من قبل اقترانات الأمان الحالية. SV1-11(config)#show crypto ipsec sa interface: outside Crypto map tag: mymap, local addr. 209.165.201.20 (local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0 (remote ident (addr/mask/prot/port): (10.0.0.10/255.255.255.255/0/0 current_peer: 209.165.201.19:500 dynamic allocated peer ip: 10.0.0.10 {}=PERMIT, flags pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4# pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7# pkts compressed: 0, #pkts decompressed: 0# pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0# send errors 0, #recv errors 0# local crypto endpt.: 209.165.201.20, remote crypto endpt.: 209.165.201.19

path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: c9a9220e :inbound esp sas (spi: 0xa9857984(2844096900 , transform: esp-3des esp-md5-hmac { ,in use settings ={Tunnel slot: 0, conn id: 1, crypto map: mymap (sa timing: remaining key lifetime (k/sec): (4607996/28746 IV size: 8 bytes replay detection support: Y :inbound ah sas :inbound pcp sas :outbound esp sas (spi: 0xc9a9220e(3383304718 , transform: esp-3des esp-md5-hmac { ,in use settings ={Tunnel slot: 0, conn id: 2, crypto map: mymap (sa timing: remaining key lifetime (k/sec): (4608000/28748 IV size: 8 bytes replay detection support: Y :outbound ah sas :outbound pcp sas

استكشاف الأخطاء وإصلاحها

ارجع إلى <u>أستكشاف أخطاء PIX وإصلاحها لتمرير حركة مرور البيانات على نفق IPSec المنشأ</u> للحصول على مزيد من المعلومات حول أستكشاف أخطاء هذا التكوين وإصلاحها.

<u>معلومات ذات صلة</u>

- <u>مراجع أوامر جدار حماية PIX الآمن من Cisco</u>
 - <u>طلبات التعليقات (RFCs)</u>
 - <u>صفحة دعم IPSec (بروتوكول أمان IP)</u>
 - <u>صفحة دعم عميل شبكة VPN من Cisco</u>
- <u>صفحة دعم جدران الحماية من السلسلة PIX 500</u>
 - <u>الدعم الفني Cisco Systems</u>

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