Configuración del Cisco VPN 3000 Concentrator 4.7.x para Obtener un Certificado Digital y un Certificado SSL

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Instalación de certificados digitales en el concentrador VPN Instalación de certificados SSL en el concentrador VPN Renovación de Certificados SSL en el Concentrador VPN Información Relacionada

Introducción

Este documento incluye instrucciones paso a paso sobre cómo configurar los Cisco VPN 3000 Series Concentrators para autenticarse con el uso de certificados digitales o de identidad y certificados SSL.

Nota: En el VPN Concentrator, el balanceo de carga debe desactivarse antes de generar otro certificado SSL, ya que esto impide la generación del certificado.

Refiérase a <u>Cómo obtener un Certificado Digital de una CA de Microsoft Windows utilizando</u> <u>ASDM en un ASA</u> para obtener más información sobre el mismo escenario con PIX/ASA 7.x.

Consulte <u>Ejemplo de Configuración de la Inscripción de Certificados de Cisco IOS Usando</u> <u>Comandos de Inscripción Mejorados</u> para obtener más información sobre el mismo escenario con las Plataformas Cisco IOS®.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el Cisco VPN 3000 Concentrator que ejecuta la versión 4.7.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Instalación de certificados digitales en el concentrador VPN

Complete estos pasos:

 Elija Administration > Certificate Management > Enroll para seleccionar la solicitud de certificado digital o de identidad.

Administration | Certificate Management | Enroll

This section allows you to create an SSL or identity certificate request. The identity certificate request allows the VPN 3000 Concentrator to be enrolled into the PKI. The certificate request can be sent to a CA, which will issue a certificate. The CA's certificate must be installed as a Certificate Authority before installing the certificate you requested.

Choose the type of certificate request to create:

Identity certificate

SSL certificate

<< Go back to Certificate Management

2. Elija Administration > Certificate Management > Enrollment > Identity Certificate y haga clic en Enroll via PKCS10

Request(Manual).

Administration | Certificate Management | Enroll | Identity Certificate

Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. <u>Click here to install a new CA using SCEP before enrolling</u>.

- Enroll via PKCS10 Request (Manual)
 - Enroll via SCEP at RSAv57RootMD5srvCN
 - Enroll via SCEP at TestCA6-8 at Cisco

<< Go back and choose a different type of certificate

3. Rellene los campos solicitados y, a continuación, haga clic en Inscribirse.Estos campos se rellenan en este ejemplo.Nombre común: altiga30Unidad organizativa: IPSECCERT (la OU debe coincidir con el nombre de grupo IPsec configurado)Organización: Cisco SystemsLocalidad: RTPEstado/Provincia: Carolina del NortePaís: EE. UU.Nombre de dominio completamente calificado —(no se utiliza aquí)Tamaño de clave: 512Nota: Si solicita un certificado SSL o un certificado de identidad mediante el protocolo simple de

inscripción de certificados (SCEP), estas son las únicas opciones RSA disponibles.512 bits RSA768 bits RSA1024 bits RSA2048 bits RSADSA 512 bitsDSA 768 bitsDSA 1024

bits

Administration Certificate Management Enroll Identity Certific	ate PKCS10
Automation Contracto Management Current Mentaly Service	
Enter the information to be included in the certificate request. The C ₂ before installing the certificate you requested. Please wait for the	l's certificate must be installed as a Certificate Authority e operation to finish.
Common Name (CN) altiga30	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU) IPSECCERT	Enter the department.
Organization (O) Cisco Systems	Enter the Organization or company.
Locality (L) RTP	Enter the city or town.
State/Province (SP) NorthCarolina	Enter the State or Province.
Country (C) US	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E- Mail Address)	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Key Size RSA 512 bits 💌	Select the key size for the generated RSA/DSA key pair.
Enroll Cancel	

4. Después de hacer clic en **Inscribirse**, aparecen varias ventanas. La primera ventana confirma que ha solicitado un

certificado.

Administration | Certificate Management | Enrollment | Request Generated

A certificate request has been generated. In a few seconds, a new browser window will open up with the certificate request. The request can be saved as a file, or copied then pasted into a CA's management interface.

The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt**. When you are done, you should delete this file; go to the <u>File Management page</u> to delete the certificate request.

- Go to Certificate Management
- · Go to Certificate Enrollment
- · Go to Certificate Installation

También se abre una nueva ventana del navegador que muestra el archivo de solicitud PKCS.

https://172.18.124.214/FILE/pkcs0001.txt - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	歌
← Back - → - ② 🔄 🚰 ② Search 🐼 Favorites ③ Media 🎯 🖓 - 🎒 🗃 🗐 😒	
Address 🕘 https://172.18.124.214/FILE/pkcs0001.txt 🔹 🔗 Go	Links »
iwon - 🗞 - 🎆 🖸 🖓 Money -	More [⊉]
NASDAQ®	
DECTN NEW ORDERTSTONE DECUECT	^
MIIBKDCBOwIBADByMREwDwYDVQQDEwhhbHRp22EzMDESMBAGA1UECxMJSVBTRUND RVJUMRYwFAYDVQQKEw1DaXNjbyBTeXNOZW1zMQwwCgYDVQQHEwNSVFAxFjAUBgNV BAgTDUSvcnRoQ2Fyb2xpbmExCzAJBgNVBAYTA1VTMFowDQYJKo2IhvcNAQEBBQAD SQAwRgJBAIaj+mtJ/UozTMMwOioNMiqw4kmgHIG2E/BIZc+xokG4rBp11rq4DkM J3XOVB8y1Ukzjvdlgh+ckmjBaiqy3I8CAQUwDQYJKo2IhvcNAQEEBQADQQAurnDB DOdRWJg/dVvGAM2HKGrLTdjoIYGsxTfXLSoQIERerU4TQCrhqa5NvlcdLsQFPxV1 zVleLhhpRfOA4hw1 END NEW CERTIFICATE REQUEST	<pre>Image: Image: Image Image: Image: Image</pre>
🔕 Done 🕒 🔮 Internet	11.

5. En el servidor de la Autoridad de certificación (CA), resalte la solicitud y péguela en el servidor de la CA para enviar la solicitud. Haga clic en Next (Siguiento)

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Pavorites Tools Help	
4-Back	
Address Phttp://172.10.124.96/centsrv/	• (ଚିରେ Un
Microsoft Certificate Services – jfrahim-pc	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. On will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt you depending upon the type of certificate you request.	ce you acquire a certificate, you ir e-mail messages, and more
Select a task: C Retrieve the CA certificate or certificate revocation list Request a certificate Check on a pending certificate	
	Next>

6. Seleccione **Advanced request** y haga clic en **Next**.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edt View Favorites Tools Help	
⇔Back + → - ② 3 3 3 Search @Favorites @History 2 + 3	
Address http://172.18.124.96/certsrv/certrqus.asp	▼ _e rido jun
Microsoft Certificate Senices jitahim-pc	Home
Choose Request Type	
Please select the type of request you would like to make:	
C User certificate request.	
Web Brower Certificate E-Mel Protection Certificate	
Advanced request	
	Next>

7. Seleccione Enviar una solicitud de certificado utilizando un archivo PKCS #10 codificado en base64 o una solicitud de renovación usando un archivo PKCS #7 codificado en base64 y, a continuación, haga clic en

Siguiente.	
Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
4+Back + → - ② 3 3 ③ Search ⊕ Favorites ③History ⓑ- 3	
Address Ather http://172.18.124.96/certsrv/certrgad.asp	▼ (PG0 U
Microsoft Certificate Sentces Jfrahim-pc	Home
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the following methods authority [CA] will determine the certificates that you can obtain.	 Note that the policy of the certification
 Submit a certificate request to this CA using a form. 	
Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #10 file or a	ase64 encoded PKCS #7 file.
 Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Sta You must have an enrollment agent certificate to submit a request for another user. 	ation.
	Next >
<u>-</u>	

Corte y pegue el archivo PKCS en el campo de texto de la sección Solicitud guardada. A continuación, haga clic en Enviar.

Microsoft Certificate Services - Microsoft Internet Explorer		
File Edit View Favorites Tools Help		
4-Back - → - ◎ 2 △ ②Search @Favorites @History 2- @		
Address R http://172.18.124.96/certsrv/certrqut.asp	-	(₽G0 U
Microsoft Certificate Services - jfrahim-pc		Hom
Submit A Saved Request		
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external applicat server) into the request field to submit the request to the certification authority (CA).	ion (such as a v	veb
Saved Request: Provide Request: Provide Request: (PKCS #10 or #?): Provide for a file to insert.		
Additional Attributes:		
	Subr	mit≯

9. Ejecute el certificado de identidad en el servidor de la

CA.							
Certification Authority			and the second second				_ 0
Action Yew		12					
Tree	Request ID	Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region	Request Or
Certification Authority (Local)	197	DEGJN N	T-Ran Linder Scholtston All Tasks ♦ Issue Refresh Help	3/23/2001 9:13 AM	GHOSTANUR	05	Cisco Syste

10. Descargue los certificados raíz y de identidad. En el servidor de la CA, seleccione **Comprobar un certificado pendiente** y haga clic en

Siguiente.			
Microsoft Certificate Services - Microsoft Internet Explorer			-10
File Edit View Favorites Tools Help			
4-8ack - → - ◎ ② ③ ③ Search @Favorites ③History ◎- ④			
Address Phtp://172.10.124.96(certsrv)	•	200	Ju
Microsoft Certificate Services Jhahim-pc		H	ome
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 c will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages depending upon the type of certificate you request.	entifica , and r	te, yo nore	u
Select a task:			
C Retrieve the CA certificate or certificate revocation list			
C Request a certificate			
Check on a pending certificate			
	N	< bos	I

11. Seleccione **Base 64 codificada** y haga clic en **Descargar certificado de CA** en el servidor de CA.



12. Guarde el certificado de identidad en la unidad

ve As	E. – 1				?
Save in:	🕜 Desktop		•	+ 🖿 💣 📰+	
	My Documen	ts			
History	Wy Compute	r Places			
1					
Desktop					
-					
ly Documents					
My Computer					
	File name:	Colline March		-	Save
y Network P	nie name.				
	Save as type:	Security Certificate		· ·	Lancel

13. En el servidor de la CA, seleccione **Recuperar el certificado de la CA o la lista de revocación de certificados** para obtener el certificado raíz. Luego haga clic en Next (Siguiente).

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit - View Favorites Tools Help	
4-Back - → - () () () () Search () Favorites () History () + ()	
Address D http://172.18.124.96/certsrv/	▼ (*Go) U
Microsoft Certificate Services - jfrahim-pc	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure prog will be able to securely identify yourself to other people over the web, sign your e-mail messages, en depending upon the type of certificate you request.	gram. Once you acquire a certificate, you crypt your e-mail messages, and more
Select a task: Retrieve the CA certificate or certificate revocation list Request a certificate Check on a pending certificate	

14. Guarde el certificado raíz en la unidad

local. Save As					? X
Save in:	Desktop		•	+	•
History History Desktop My Documents My Computer	My Document My Computer My Network F Certnew, cer	ts Places			
	File name:	certroot.cer		•	Save
My Network P	Save as type:	Security Certificate			Cancel

15. Instale los certificados raíz e identidad en el VPN 3000 Concentrator. Para hacer esto, seleccione Administration > Certificate Manager > Installation > Install certificate from enrollment. En Estado de inscripción, haga clic en Instalar.

Select a enrollment request to	install.						
Enrollment Status							
Subject	Issuer	Date	Use	Reason	Method	Status	Actions
altica30 at Cierco Systems	N/A	05/22/2003	D	Initial	Manual	In Progress	View Install Delete

16. Haga clic en Cargar archivo desde la estación de

trabajo.



17. Haga clic en Examinar y seleccione el archivo de certificado raíz que guardó en la unidad local.Seleccione Install para instalar el certificado de identidad en el concentrador VPN. La Administración | La ventana Administración de certificados aparece como confirmación y el nuevo certificado de identidad aparece en la tabla Certificados de identidad.

Administration Certificate Management Install Ide	entity Certificate Upload File from Workstation
Enter the name of the identity certificate file.	
T "	
Filename	Browse
Install Cancel	

Nota: Complete estos pasos para generar un nuevo certificado si falla el certificado.Seleccione Administration > Certificate Management.Haga clic en Eliminar en el cuadro Acciones de la lista de certificados SSL.Seleccione Administration > System Reboot.Seleccione Guardar la configuración activa en el momento del reinicio, elija Ahora y haga clic en Aplicar. Ahora puede generar un nuevo certificado después de que se complete la recarga.

Instalación de certificados SSL en el concentrador VPN

Si utiliza una conexión segura entre su navegador y el concentrador VPN, el concentrador VPN requiere un certificado SSL. También necesita un certificado SSL en la interfaz que utiliza para administrar el concentrador VPN y para WebVPN, y para cada interfaz que termina los túneles WebVPN.

Los certificados SSL de la interfaz, si no existen, se generan automáticamente cuando el concentrador VPN 3000 se reinicia después de actualizar el software del concentrador VPN 3000. Dado que un certificado autofirmado se genera automáticamente, este certificado no se puede verificar. Ninguna autoridad certificadora ha garantizado su identidad. Sin embargo, este certificado le permite establecer un contacto inicial con el concentrador VPN mediante el navegador. Si desea sustituirlo por otro certificado SSL autofirmado, siga estos pasos:

1. Elija Administration > Certificate

Management.

V										
Administration Certificate Management Monday, 05 January 2004 16:31:1										
Ketresh										
This sectio	This section lets you view and manage certificates on the VPN 3000 Concentrator.									
 <u>Clic</u> 	k here to enroll with	a Certificate	Authority							
 <u>Clic</u> 	<u>:k here to install a ce</u>	rtificate								
aa										
Certifica	te Authorities [<u>V</u>	iew All CRL (Caches Clear All CRI	<u>L Caches</u>] (cu	arent: 1, maxi	man	: 20)			
	Subject		Issuer		Expirat	ion	SCEP Issuer		Actions	_
ms-root-si	ha-06-2001 at cisco	ms-	root-sha-06-2001 at	cisco	06/04/202	2	No	View Configure Delete		
-										
Identity	Certificates (cure	nt: 1, maximu	un: 20)							
	Subject			Issuer			Expiration		Actions	
Gateway /	A at Cisco Systems		ms-root-sha-06-	2001 at cisco)		02/04/2004	View	r <u>Renew Delete</u>	
								-		
SSL Cer	tificates									
Interface	Subject	:	Issuer		Expiration			Acti	0N9	
Private	10.5.6.1 at Cisco Sy:	stems, Inc.	10.5.6.1 atCisco Sy	stems, Inc.	02/01/2006	View	Renew Delete E:	xport	Generate) Enroll Impor	rt
									\sim .	
SSH Hos	st Key									
	Key Size	F	Сеу Туре		Date G	ener	ated		Actions	
1024 bits	-	RSA		01/05/2004		_			Gonerate	_
		1		16						

2. Haga clic en Generar para mostrar el nuevo certificado en la tabla de certificados SSL y reemplazar el certificado existente. Esta ventana le permite configurar campos para certificados SSL que el concentrador VPN genera automáticamente. Estos certificados SSL son para interfaces y para balanceo de

carga.	
Administration Certificate Management Generate SSL Cer	tificate
You are about to generate a certificate for the Public Interface .	The certificate will have the following DN for both Subject and Issuer.
The certificate will be valid for 3 years from yesterday.	
	_
Common Name (CN) 10.86.194.175	Enter the Common Name, usually the IP or DNS address of this interface
Organizational Unit (OU) VPN 3000 Concentrator	Enter the department.
Organization (O) Cisco Systems. Inc.	Enter the Organization or company.
Locality (L) FrankJin	Enter the city or town.
State/Province (SP) Massachusetts	Enter the State or Province.
Country (C) US	Enter the two-letter country abbreviation (e.g. United States = US).
RSA Key Size 1024-bits 💌	Select the key size for the generated RSA key pair.
Generate Cancel	

Si desea obtener un certificado SSL verificable (es decir, uno emitido por una Autoridad de Certificación), vea la sección <u>Instalación de Certificados Digitales en el Concentrador VPN</u> de este documento para utilizar el mismo procedimiento que utiliza para obtener certificados

de identidad. Pero esta vez, en la ventana Administration > Certificate Management > Enroll, haga clic en SSL certificate (en lugar de Identity Certificate).Nota: Consulte la Administración / Sección Administración de Certificados del Volumen II de Referencia del Concentrador VPN 3000: Administración y Monitoreo Versión 4.7 para obtener información completa sobre certificados digitales y certificados SSL.

Renovación de Certificados SSL en el Concentrador VPN

Esta sección describe cómo renovar los certificados SSL:

Si esto es para el certificado SSL generado por el VPN Concentrator, vaya a Administration > Certificate Management en la sección SSL. Haga clic en la opción Renovar y que renueva el certificado SSL.

Si se trata de un certificado concedido por un servidor CA externo, siga estos pasos:

1. Elija Administration > Certificate Management > Delete bajo *SSL Certificates* para eliminar los certificados caducados de la interfaz

	DISTRICT OF THE OWNER		We	dnesday, 19	September 2007 00:01
			Refrest		
his section lets you view and n	anage cer	tificates on the VPN 3000 Concer	trator.		
Click here to enroll with:	Certificat	e Authority			
Click here to install a cert	ificate				
ertificate Authorities [View	ALCRLC	aches Clear All CRL Caches] (currer	t: 1, maximum: 6)		
Subject		Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification		Thawte Test CA Root at Thawte 12/31 Certification		No	

No Identity Certificates

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View Renew Delete Export Generate Enroll Import
Public	pearlygates.ocp.org at pearlygates.ocp.org	Equifax Secure Certificate Aut at Equifax	08/16/2008	View Renew (Delete) Export Generate Enroll Import

Haga clic en **Yes** para confirmar la eliminación del certificado SSL.

Subject

CN=pearlygates.ocp.org	
OU=Domain Control Validated - QuickSSL Premium(R)
OU=See www.geotrust.com/resources/cps (c)07	
OU=GT94824223	
D=pearlygates.ocp.org	
C=US	

Issuer

OU=Equifax Secure Certificate Authority O=Equifax C=US

	Serial Number 07E267
	Signing Algorithm SHA1WithRSA
	Public Key Type RSA (1024 bits)
	Certificate Usage Digital Signature, Non Repudiation, Key Encipherment, Data Enciphermen
	MD5 Thumbprint 2C:EC:8D:8B:FE:59:9D:F8:04:A6:B2:1B:C5:09:9A:27
	SHA1 Thumbprint 6E:9A:7C:D3:02:FE:10:1C:75:79:00:AA:6A:73:84:54:C2:DC:BE:9
	Validity 8/16/2007 at 17:26:35 to 8/16/2008 at 17:26:35
CF	RL Distribution Point http://crl.geotrust.com/crls/secureca.crl

Are you sure you want to delete this certificate?



2. Elija Administration > Certificate Management > Generate para generar el nuevo certificado SSL.

Administration Certificate Management	Wednesday, 19 September 2007 00:05:
	Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- · Click here to enroll with a Certificate Authority
- Click here to install a certificate

Certificate Authorities [View All CRL Caches | Clear All CRL Caches] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View Configure Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface Subject Issue		Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View Renew Delete Export Generate Enroll Import
Public	No Certificate Installed.		(Generate) Enroll Import

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- · Click here to enroll with a Certificate Authority
- · Click here to install a certificate

Certificate Authorities [View All CRL Caches | Clear All CRL Caches] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View Configure Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View Renew Delete Export Generate Enroll Import
Public	10.1.1.5 at Cisco Systems, Inc.	10.1.1.5 at Cisco Systems, Inc.	09/18/2010	View Renew Delete Export Generate Enroll Import

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación Cisco Systems