Configurazione di Cisco VPN 3000 Concentrator 4.7.x per ottenere un certificato digitale e un certificato SSL

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Installare i certificati digitali sul concentratore VPN Installare i certificati SSL sul concentratore VPN Rinnova certificati SSL sul concentratore VPN Informazioni correlate

Introduzione

Questo documento include istruzioni dettagliate su come configurare i Cisco VPN serie 3000 concentrator per l'autenticazione con l'utilizzo di certificati digitali o di identità e certificati SSL.

Nota: in Concentrator VPN, è necessario disabilitare il bilanciamento del carico prima di generare un altro certificato SSL, in quanto ciò impedisce la generazione del certificato.

Per ulteriori informazioni sullo stesso scenario con PIX/ASA 7.x, consultare il documento sulla procedura per ottenere un certificato digitale da una CA di Microsoft Windows usando ASDM su un'ASA.

Per ulteriori informazioni sullo stesso scenario delle piattaforme Cisco IOS®, fare riferimento all'<u>esempio di configurazione della registrazione di certificati Cisco IOS con i comandi di</u> registrazione avanzata.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato Cisco VPN 3000 Concentrator versione 4.7.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Installare i certificati digitali sul concentratore VPN

Attenersi alla seguente procedura:

- 1. Per selezionare la richiesta di certificato digitale o di identità, scegliere Amministrazione > Gestione certificati >
 - Registra.

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

 Scegliere Amministrazione > Gestione certificati > Registrazione > Certificato di identità e fare clic su Registra tramite richiesta PKCS10 (manuale).

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. Compilare i campi richiesti e quindi fare clic su **Registra**.Questi campi vengono compilati in questo esempio.**Nome comune**: altiga30**Unità organizzativa** - IPSECCERT (l'unità organizzativa deve corrispondere al nome di gruppo IPSec

configurato)**Organizzazione**—Cisco Systems**Località**: RTP**Stato/Provincia**—Carolina del Nord**Paese**—US**Nome di dominio completo** - (non utilizzato qui)**Dimensione chiave**—512**Nota:** se si richiede un certificato SSL o un certificato di identità utilizzando il protocollo SCEP (Simple Certificate Enrollment Protocol), queste sono le uniche opzioni RSA disponibili.RSA 512 bitRSA 768 bitRSA 1024 bitRSA 2048 bitDSA 512 bitDSA 768 bitDSA 1024

bit

Administration Certificate Management Enroll Identity Certificat	te PKCS10					
Enter the information to be included in the certificate request. The CA's certificate must be installed as a Certificate Authority before installing the certificate you requested. Please wait for the 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)	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. Dopo aver fatto clic su **Registra**, vengono visualizzate diverse finestre. La prima finestra conferma che è stato richiesto un

certificato.

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.
 <u>Go to Certificate Management</u> <u>Go to Certificate Enrollment</u> <u>Go to Certificate Installation</u>

Viene inoltre visualizzata una nuova finestra del browser in cui è visualizzato il file di richiesta PKCS.

https://172.18.124.214/FILE/pkcs0001.txt - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	- 192
(← Back - → - ② ③ ④ 🏠 ③Search ④Favorites ③Media ③ 🛃 - ④ 🖾 🖃 🕄	
Address 🕘 https://172.18.124.214/FILE/pkcs0001.txt 💌 🔗 Go	Links »
iwon - 🗞 - 📕 🖸 🔀 Money -	More∛
NASDAQ®	>
BEATH NEW GERTTERGATE BEANEOT	~
MIIBKDCBOwIBADBYMREwDwYDVQQDEwhhbHRp22EzMDESMBAGA1UEC×MJSVBTRUND RVJUMRYwFAYDVQQKEwIDaXNjbyBTeXNO2W1zMQwwCgYDVQQHEwNSVFAxFjAUBgNV BAgTDUSvcnRoQ2Fyb2xpbmExCzAJBgNVBAYTA1VTMFowDQJKoZIhvcNAQEBBQAD SQAwRgJBAIaj+mtJ/UozTMMwO1oNMiqw4kmgIhIG2E/BIZc+xokG4rBp11rq4DkM J3XOVB8yiUkzjvdlgh+ckmjBaiqy3I8CAQUwDQYJKoZIhvcNAQEEBQADQQAurnDB DOdRWJg/dVvGAM2HKGrLTdjoIYGsxTfXLSoQIERerU4TQCrhqaSNv1cdLsQFPxV1 zVIeLhhpRfOA4hw1 END NEW CERTIFICATE REQUEST	
🕘 Done 🕒 🕒 🕲 Internet	

5. Sul server Autorità di certificazione (CA), evidenziare la richiesta e incollarla nel server CA per inviare la richiesta. Fare clic su **Next**

(Avanti).		
Microsoft Certificate Services - Microsoft Internet Explorer		
File Edit. New Favorites Tools Help		
4+Back + + - O 3 1 O Search Freveries Otherary		
Address Dttp://172.10.124.96/certsrv/	- 0	Go
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. Once you acquire a cer will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, of depending upon the type of certificate you request.	tificate, and mo	, you re
Select a task: C Retrieve the CA certificate or certificate revocation list Request a certificate Check on a pending certificate		
	Next	>.

6. Selezionare **Richiesta avanzata** e fare clic su **Avanti**.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edt. View Favorites Tools Help	
4-Back + + · () () () Search () Favorites () History () + ()	
Address a http://172.18.124.96/certsrv/certrqus.asp	💌 🖓 Go 🛛 Lin
Microsoft Certificate Services jtrahim-pc	Home
Choose Request Type	
Please select the type of request you would like to make:	
C User certificate request.	
Web Browser Centricate E-Mail Protection Contingete	
Advanced request	
	Next >

7. Selezionare Invia una richiesta di certificato utilizzando un file PKCS #10 con codifica Base64 o una richiesta di rinnovo utilizzando un file PKCS #7 con codifica Base64, quindi fare clic su

Avanti.		
Microsoft Certificate Services - Microsoft Internet Explorer		
File Edit View Favorites Tools Help		
4-Back + + - 3 2 3 3 Search @Favorites 3History		
Address Dhttp://172.18.124.96/certsry/certrgad.asp	• (જેલ) [U
Microsoft Certificate Sentces Ifrahim-pc		Home
Advanced Certificate Requests		
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy authority (CA) will determine the certificates that you can obtain.	y of the certific	ation
 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	CS #7 file.	
 Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station. You must have an enrollment agent certificate to aubmit a request for another user. 		
	Next>	

 Tagliare e incollare il file PKCS nel campo di testo sotto la sezione Richiesta salvata. Quindi fare clic su Invia.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
4-Back - → - ◎ 2 ④ @Search @Favorites @History &- @	
Address Addres	▼ (² Go) U
Microsoft Certificate Services jifrahim-pc	Home
Submit A Saved Request	
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an server) into the request field to submit the request to the certification authority (CA).	external application (such as a web
Saved Request:	
PFbNOQ/TmdWKORBoUkDPFw8CAQUwDQYJKo2IhvcN. GLWTjSu7B3LupgKAlqF2IBQfxGI37D+wHEEp+6z4 MgG4AhkM END NEW CERTIFICATE REQUEST (PKCS#10 or #7):	
Browse for a file to insert.	
Additional Attributes:	
	Submit>

9. Rilasciare il certificato di identità sul server

CA.							
Certification Authority							_ 6
Action Yew		C?					
Tree	Request ID	Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region	Request Or
Certification Authority (Local)	- 	BEGIN ME	Trilien Hoder Scholeston All Texts Petresh Deny Help	3(23(2001 9:13 AM	GHOSTENJUSR_	. 05	Cisco Syste

10. Scaricare la radice e i certificati di identità. Sul server CA selezionare Verifica un certificato in sospeso e fare clic su

Avanti.			
Microsoft Certificate Services - Microsoft Internet Explorer			-
File Edit View Favorites Tools Help			
4+8ack - → - ② 🗗 🖄 QSearch @Favorites @History 23- 2			
Address 1 http://172.10.124.96/certsrv/	•	260	Ju
Microsoft Certificate Services Itahim-pc		He	m
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 cert will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, a depending upon the type of certificate you request.	tificat and m	e, yoi Iore	1
Select a task: C Retrieve the CA certificate or certificate revocation list C Request a certificate			
Check on a pending certificate			
	Ne	 t>	I

11. Selezionare **Codificato Base 64** e fare clic su **Scarica certificato CA** sul server CA.



12. Salvare il certificato di identità nell'unità

Save As					? ×
Save in	: 🚺 Desktop		•	+ 🖿 💣 📰 •	<
History Desktop	My Document My Computer	s Places			
My Documents	File name:	certnew.cer			Save
My Network P	Save as type:	Security Certificate		•	Cancel

 Sul server CA selezionare Recupera il certificato CA o l'elenco di revoche di certificati per ottenere il certificato radice. Quindi fare clic su Avanti.

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. Salvare il certificato radice nell'unità

Save As					?×
Save in:	Desktop		•	+ 🛍 💣 💷	
History History Desktop My Documents My Computer	My Documen My Computer My Network I Certnew.cer	ts Places			
	File name:	certroot.cer		•	Save
My Network P	Save as type:	Security Certificate			Cancel

15. Installare i certificati radice e di identità nel concentratore VPN 3000. A tale scopo, selezionare Amministrazione > Gestione certificati > Installazione > Installa il certificato ottenuto mediante la registrazione. In Stato registrazione fare clic su Installa.

Select a enrollment request to	install						
Gunallin ant Status							
Subject	Issuer	Date	Use	Reason	Method	Status	Actions
altica 30 at Cierco Systems	N/A	05/22/2003	D	Initial	Manual	In Progress	View Install Delete

Workstation.



17. Fare clic su Sfoglia e selezionare il file del certificato radice salvato nell'unità locale.Selezionare Installa per installare il certificato di identità nel concentratore VPN. Amministrazione | La finestra Gestione certificati viene visualizzata come conferma e il nuovo certificato di identità viene visualizzato nella tabella Certificati di identità.

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

Nota: completare la procedura seguente per generare un nuovo certificato in caso di errore del certificato.Selezionare **Amministrazione > Gestione certificati**.Fare clic su **Elimina** nella casella Azioni relativa all'elenco dei certificati SSL.Selezionare **Amministrazione > Riavvio del sistema**.Selezionare **Save the active configuration at time of reboot**, scegliere **Now** (Salva la configurazione attiva al momento del riavvio), quindi fare clic su **Apply (Applica)**. È ora possibile generare un nuovo certificato al termine del ricaricamento.

Installare i certificati SSL sul concentratore VPN

Se si utilizza una connessione protetta tra il browser e VPN Concentrator, VPN Concentrator richiede un certificato SSL. È inoltre necessario un certificato SSL sull'interfaccia utilizzata per gestire il concentratore VPN e per WebVPN, nonché per ogni interfaccia che termina i tunnel WebVPN.

I certificati SSL dell'interfaccia, se inesistenti, vengono generati automaticamente quando VPN 3000 Concentrator viene riavviato dopo l'aggiornamento del software VPN 3000 Concentrator. Poiché un certificato autofirmato è generato automaticamente, non è verificabile. Nessuna autorità di certificazione ha garantito la propria identità. Tuttavia, questo certificato consente di stabilire un contatto iniziale con il concentratore VPN utilizzando il browser. Se si desidera sostituirlo con un altro certificato SSL autofirmato, eseguire la procedura seguente:

1. Scegliere Amministrazione > Gestione

Certifica	1 11.								
Administ	ration Certificate	e Managem	ent				Mor	ıday	, 05 January 2004 16:31
									Retresh
This sectio • <u>Clic</u> • <u>Clic</u> Certifica	n lets you view and <u>k here to enroll with</u> <u>k here to install a ce</u> <u>te Authorities [<u>y</u> Subject</u>	manage certif a Certificate / rtificate /iew All CRL C	icates on the VPN 3 Authority Saches Clear All CRI Issuer	3000 Concer <u>L Caches</u>] (or	urrent: 1, max	imun ion	: 20) SCEP Issuer		Actions
ms-root-si	ha-06-2001 at cisco	ms-r	oot-sha-06-2001 at	cisco	06/04/202	2	No	Vie	w Configure Delete
Identity	Certificates (cum Subject	ent: 1, maximu	m: 20)	Issuer			Expiration		Actions
Gateway A	A at Cisco Systems		ms-root-sha-D6-	2001 at cisco 02/04/2004 Viet			View	<u>Renew</u> <u>Delete</u>	
SSL Cer	tificates								
Interface	Subject	t	Issuer		Expiration			Acti	ons
Private	10.5.6.1 at Cisco Sy	stems, Inc.	10.5.6.1 at Cisco Sy	stems, Inc.	02/01/2006	View	<u>Renew</u> <u>Delete</u> <u>E</u>	xport	Generate Enroll Import
SSH Ho:	st Key								
	Key Size	K	еу Туре	Date Generated					Actions
1024 bits		RSA		01/05/2004					Generate

2. Per visualizzare il nuovo certificato nella tabella Certificato SSL e sostituire quello esistente, fare clic su **Genera**.Questa finestra consente di configurare i campi per i certificati SSL generati automaticamente da Concentrator VPN. Questi certificati SSL sono destinati alle interfacce e al bilanciamento del

carico.		
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 fo	or 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)	Franklin	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		

Se si desidera ottenere un certificato SSL verificabile, ovvero un certificato rilasciato da un'Autorità di certificazione, vedere la sezione <u>Installazione dei certificati digitali sul</u> <u>concentratore VPN</u> in questo documento per utilizzare la stessa procedura utilizzata per

ottenere i certificati di identità. In questo caso, nella finestra **Amministrazione > Gestione** certificati > Registrazione fare clic su Certificato SSL (anziché su Certificato di identità).Nota: consultare la sezione *Amministrazione | Sezione Certificate Management* di <u>VPN 3000</u> <u>Concentrator Reference Volume II: Administration and Monitoring Release 4.7</u> per informazioni complete sui certificati digitali e i certificati SSL.

Rinnova certificati SSL sul concentratore VPN

In questa sezione viene descritto come rinnovare i certificati SSL:

Se si tratta del certificato SSL generato dal concentratore VPN, passare alla sezione **Amministrazione > Gestione certificati** su SSL. Fare clic sull'opzione **renew** per rinnovare il certificato SSL.

Se si tratta di un certificato concesso da un server CA esterno, attenersi alla seguente procedura:

1. Per eliminare i certificati scaduti dall'interfaccia pubblica, scegliere Amministrazione > Gestione certificati >Elimina in *Certificati*

Subject	Issner	Issuer Expira		Actions	
lentity Certificates (current: 0	maximum: 2)				
Thawte Test CA Root at Thawte Certification Certification		est CA Root at Thawte on	12/31/2020	No	View Configure Delet
Subject		Issuer	Expiration	SCEP Issuer	Actions
<u>Click here to enroll with a C</u> <u>Click here to install a certific</u> ertificate Authorities [<u>View A</u>]	rtificate Authority ate CRL Caches Clear A	ll CRL Caches] (current: 1, m	aximum: 6)		
his section lets you view and man	age certificates on t	he VPN 3000 Concentrator			
					Refre
				And a state of the	

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 Delste 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

Fare clic su **Sì** per confermare l'eliminazione del certificato SSL.

Subject

N=pearlygates.ocp.org	
DU=Domain Control Validated - QuickSSL Premium(R)
DU=See www.geotrust.com/resources/cps (c)07	
DU=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 Encipherment
	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:95
	Validity 8/16/2007 at 17:26:35 to 8/16/2008 at 17:26:35
CRI	L Distribution Point http://crl.geotrust.com/crls/secureca.crl

Are you sure you want to delete this certificate?



2. Per generare il nuovo certificato SSL, scegliere Amministrazione > Gestione certificati > Genera

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
o 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 Enzoll 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	<u>View Renew Delete Export Generate Enroll Import</u>

Informazioni correlate

- <u>Cisco VPN serie 3000 Concentrator Support Page</u>
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico Cisco Systems