ASA 8.x: Renueve y instale el certificado SSL con el ASDM

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados Convenciones Procedimiento Verificación Troubleshooting Cómo copiar los Certificados SSL a partir de un ASA a otro Información Relacionada

Introducción

El procedimiento en este documento es un ejemplo y se puede utilizar como guía de consulta con cualquier vendedor del certificado o su propio servidor del certificado raíz. Los requisitos especiales del parámetro del certificado son requeridos a veces por su vendedor del certificado, pero este documento se piensa para proporcionar los pasos generales requeridos renovar un certificado SSL y instalarlo en un ASA que utilice el software 8.0.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este procedimiento pertenece a las Versiones de ASA 8.x con la versión 6.0(2) o posterior del ASDM.

El procedimiento en este documento se basa en una configuración válida con un certificado instalado y usado para el acceso SSL VPN. Este procedimiento no afecta su red mientras el certificado actual no se borre. Este procedimiento es un proceso gradual en cómo publicar un nuevo CSR para un certificado actual con el mismo certificado raíz que publicó la original raíz CA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Si la red está funcionando, asegúrese de haber comprendido el impacto

Convenciones

Consulte <u>Convenciones de Consejos Técnicos de Cisco</u> para obtener más información sobre las convenciones sobre documentos.

Procedimiento

Complete estos pasos:

 Seleccione el certificado que usted quiere renovar debajo de la configuración > de la Administración de dispositivos > de los certificados de identidad, y entonces el haga click en AddEigura 1

riadi igulu i					
🔂 Cisco ASDM 6.1 for ASA - 172	.16.242.232				
<u>File Yew Tools Wizards Window</u>	v <u>H</u> elp		Look Far		60 Julialia
🚳 Home 😪 Configuration 🔯 M	onitoring 🛄 Save 🙉 Re	fresh 🙆 Back 🕥 Forw	ard 🦻 Help		cisco
Device Management 3 4 X	Configuration > Device M	anagement > Certificate I	• Management > Identity Certifi	cates	
🖃 🐨 Management Access					
🖶 🥵 System Image/Configuration					
🖶 🤐 High Availability	Issued To	Issued By	Expiry Date	Usage	Add
🖶 📆 Users(AAA	to re-repristoring	[[UI=N5+04]	100:05:15 UTC Har 11 20	oa senera Purpose	. Show Details
🖶 🛃 Certificate Management					Delete
Contractes					Event
B 🗗 DHCP					Esper
⊕ Advanced					Instal
					Refresh
	Identity certificate can be	used to authenticate SSL, suc	h as ASDM, access to the security a	ppliance on a given interface. You ca	n go to <u>55. Settinos</u>
	to make such configuratio	n.			
0					
Device Setup					
📆 Frewal					
Remote Access VPN					
🙀 Site-to-Site VPN					
Device Management					
20			Apply Reset]	
Device configuration refreshed successful	ly.		ciscol 15	🗟 🛃 📊 🛛 🕞	8/29/08 8:52:53 PM UTC

2. Bajo agregue el certificado de identidad, seleccione el agregar un nuevo botón de radio del certificado de identidad, y elija su par clave del menú desplegable.Nota: No se recomienda para utilizar el <Default-RSA-Key> porque si usted regenera su clave de SSH, usted invalida su certificado. Si usted no tiene una clave RSA, completa camina a y el B. Si no continúe al paso 3.Figura 2

🖆 Add Identity Certificat	e	X
 Import the identity certification 	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 ce	rtificates to TLS-Proxy
		Advanced
Add Certifi	cate Cancel	Help

(Opcional) complete estos pasos si usted no hace una clave RSA configurar todavía, si no salto al paso 3.Haga clic **nuevo....**Ingrese el nombre del par clave en el **nuevo campo de nombre del par clave del ingresar**, y el tecleo **ahora genera**.**Figura 3**

🕵 Add K	ey Pair	×
Name:	🚫 Use default key pair name	
	Enter new key pair name: Certkey	
Size:	1024	
Usage:	⊙ General purpose ○ Special	
G	ienerate Now Cancel Help	

- 3. Tecleo selecto.
- Ingrese los atributos apropiados del certificado tal y como se muestra en del cuadro 4. Una vez que está completado, haga clic la AUTORIZACIÓN. Entonces haga clic agregan el certificado. 'Figura 4'

	×
Value ASA5540.comp LAB Cisco Systems US CA	
	Value ASA5540.comp LAB Cisco Systems US CA

CLI	hecho	sa	lir:
<u> </u>	1100110	ou	

rypto ca trustpoint ASDM_TrustPoint0
keypair CertKey
id-usage ssl-ipsec
fqdn 5540-uwe
<pre>subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA</pre>
enrollment terminal
crypto ca enroll ASDM_TrustPoint0

5. En la ventana emergente de la **petición del certificado de identidad**, salve su pedido de firma de certificado (CSR) a un archivo de texto, y haga clic la **AUTORIZACIÓN.Figura 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. (Opcional) verifique en el ASDM que el CSR esté pendiente, tal y como se muestra en del cuadro 6. **'Figura 6'**

🔂 Cisco ASDM 6.1 for ASA - 172.	16.242.232				
Ele Yew Tools Wigards Window	Help		Look Far:	G	2 duala
📣 Home 🙈 Configuration 🔯 Mo	nitoring 🛄 Sava 🙉 Re	resh 🙆 Back 🕥 Forwar	🤊 Help		cisco
Device Management and A X	Configuration > Device M	anagement > Certificate Ma	o	-	
R: 🕐 Management Access	Contraster State 1 - Row Those 1				
🖶 🥵 System Image/Configuration					
🖶 🎯 High Availability	Issued To	Issued By	Expiry Date	Usage	. Add
Hind Cogging	[on=*.vpn1.com] [ASA5540.company.com]	[m=MS-CA] [Not Available]	00:03:15 UTC Mar 11 2009	General Purpose	Show Details
🕀 🛃 Certificate Management	Carbano Sancing and Social Records	[recent and real	h to be given		
CA Certificates					
					Export
🕀 🚑 DNS					Instal
E 25 Advanced					Refresh
	Identity certificate can be	used to authenticate SSL, such	as ASDM, access to the security appl	iance on a given interface. You can o	io to 59. Settinos
	to make such configuration	۱.			
🛃 Device Setup					
📆 Froxal					
Remote Access VPN					
🙀 Ske-to-Site VPN					
Device Management					
*			Apply Reset		
Configuration changes saved successfully.			tiscol 15		3/29/08 9:56:23 PM UTC

- 7. Presente el pedido de certificado al administrador del certificado, que publica el certificado en el servidor. Esto puede estar a través de una interfaz Web, email, o directamente raíz CA al servidor para el proceso del problema del certificado.
- 8. Complete estos pasos para instalar el certificado renovado.Seleccione el pedido de certificado pendiente conforme a la configuración > a la Administración de dispositivos > a los certificados de identidad, tal y como se muestra en del cuadro 6, y el tecleo instala.En la ventana del certificado de identidad del instalar, seleccione la goma los datos del certificado en el botón de radio del formato del base 64, y el tecleo instala el certificado.Nota: Alternativamente, si el certificado se publica en un archivo de .cer bastante entonces un archivo o un email basado texto, usted puede también seleccionar instala de un archivo, hojea al archivo apropiado en su PC, tecleo instala el archivo de certificado ID y después hace clic instala el certificado.Figura 7

🖆 Install Identity certificate	$\mathbf{\times}$
Identity Certificate	_
O Install from a file: Browse	
 Paste the certificate data in base-64 format: 	
Ng9SqvsXWWkJmS8ss9Qvz5D+K2uSLPcEAuuT7JhUVC1jbTZh1GLpqBheEeMk/8jY fui6ZdrSloUbodDEy6IiodF8QeQgCEdl1omR5W9bP5t2aTPT5J7lG3ckEM0kseqC wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa 6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== END CERTIFICATE	<
Install Certificate Cancel Help	

CLI hecho salir:

crypto ca import ASDM_TrustPoint0 certificate

WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ

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

9. Una ventana aparece que confirma el certificado está instalada con éxito. "OK" del tecleo a

	🕵 Informati	on	×
	į	Certificate import succeeded.	
8		ОК	

confirmar.Figura 8

10. Asegúrese que su nuevo certificado aparezca bajo los certificados de identidad. Figura 9

🔂 Cisco ASDM 6.1 for ASA - 172	.16.242.232					
Elle Yew Iools Wigards <u>W</u> indow	v Help			Look Far:		©
🛃 Home 🦓 Configuration 🔯 M	onitoring 🔚 Save 🔇 Refresh	Back 🕥	Forward 🦻 H	leip		cisco
Device Management Device Management	Configuration > Device Manag	ement > Certifi	cate Manageme	nt > Identity Certifica	ates	
Management Access						_
🖶 🎒 System Image/Configuration						
🖶 🤐 High Availability	Issued To	Issued By		Expiry Date 048244 UTC May 11 200	Usage Concert Discourse	
🖶 🎲 Users(AAA	[cn=A5A5540.company.com,	[m=MS-CA]	2	2:49:31 UTC Aug 29 200	9 General Purpose	Show Details
E Certificate Management						Delete
Identity Certificates						Export
B 💕 DHCP						
🗑 🚙 Dres 🗊 🛐 Advanced						376534
						Refresh
	Identity certificate can be used to make such configuration	i to authenticate St	SL, such as ASDM,	access to the security ap	pliance on a given interface. Ye	su can go to <u>55, Settinos</u>
	to make such coningeration.					
💑 Device Setup						
📆 Firewal						
Remote Access VPN						
🙀 Site-to-Site VPN						
🔣 Device Management						
20 *			App	Reset		
Configuration changes saved successfully	6		cis	co1 15	🗟 🛃 🔂	🔒 8/29/08 10:05:53 PM UTC

11. Complete estos pasos para atar el nuevo certificado a la interfaz:Elija la **configuración > la Administración de dispositivos > avanzó > las configuraciones SSL**, tal y como se muestra en del cuadro 10.Seleccione su interfaz bajo los Certificados, y el tecleo **edita.Figura 10**

🚰 Cisco ASDM 6.1 for ASA - 172	.16.242.232				
File Yew Tools Wigards Window	v Help		Look Far:	Go	de de
🛃 Home 🦓 Configuration 📴 M	onitoring 🔚 Sava 🔇 R	efresh 🔇 Back 🕥 Forward 🤺	? Help		CISCO
Device Management 🗗 🕂 🔀	Configuration > Device N	lanagement > Advanced > SSLS	ettings		
Advanced Advanced	Configure SSL parameters. Server SSL Version: Any Encryption Available Algorithms 06 Certificates Specify which certificates,	These parameters affect both ASDM at Clent SSL Version: 4-405 S-SHAL	nd SSL VFN access. Any Add >> Add >> Active Algor Remove :	RC4-SHA1 RC4-SHA1 AES128-SHA1 AES256-SHA1 30E5-SHA1 30E5-SHA1	Move Up () Move Down
- E Phoney Queue	associated with a certifica	ite of their own.			
🖻 - 🔐 WCCP	Interface	Trustpoint	Load Balanc	ing Trustpoint	Edit
Revice Setup	outside	[cr.–*, vpn1.ccn][co.–f	G-CAT BUIE		
🕄 Fyroxall					
Remote Access VPN	Falback Certificate: N	one -	*		
*			Apply Reset		
Configuration changes saved successfully	r.		cisco1 15	📓 🛃 🔚 🔒 🗤	29/08 10:08:53 PM UTC

12. Elija su nuevo certificado del menú desplegable, haga clic la AUTORIZACIÓN, y el tecleo se aplica.

	•							
ssl	encryption	rc4-sha1	aes128-sh	al a	aes256-s	ha1	3des-s	sha1
ssl	trust-point	: ASDM_Tru	ustPoint0	outs	side			

Figura 11

🖆 Select SSL Certificate 🛛 🛛 🔀							
Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the outside interface. To enroll a trustpoint, go to Configuration > Features > Device Administration > Certificate > Enrollment.							
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]: 611f863000000000026						
Cancer Ca							

13. Salve su configuración en el ASDM o en el CLI.

Verificación

Usted puede utilizar la interfaz CLI para verificar que el nuevo certificado está instalado al ASA

```
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-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3base1\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-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\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-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\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)#

Troubleshooting

(Opcional) verifique en el CLI que el certificado correcto esté aplicado a la interfaz:

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)**#**

Cómo copiar los Certificados SSL a partir de un ASA a otro

Esto puede ser hecha si usted había generado las claves exportables. Usted necesita exportar el certificado a un archivo PKCS. Esto incluye la exportación de todas las claves asociadas.

Utilice este comando de exportar su certificado vía el CLI:

ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>

Nota: Passphrase - usado para proteger el archivo del pkcs12.

Utilice este comando de importar su certificado vía el CLI:

SA(config) #crypto ca import <trust-point-name> pkcs12 <passphrase>

Nota: Este passphrase debe ser lo mismo según lo utilizado al exportar el archivo.

Esto se puede también hacer con el ASDM para un par de fallas ASA. Complete estos pasos para realizar esto:

- 1. Inicie sesión al ASA primario vía el ASDM y elija las herramientas--> configuración de respaldo.
- 2. Usted puede respaldo todo o apenas los Certificados.
- 3. En el espera, el ASDM abierto y elige las herramientas --> configuración del Restore.

Información Relacionada

- Página de soporte adaptante del dispositivo de seguridad de Cisco (ASA)
- El ASA 8.x instala manualmente los Certificados del vendedor de las de otras compañías para el uso con el ejemplo de configuración del WebVPN
- Soporte Técnico y Documentación Cisco Systems