ASA 8.x: Verleng en Installeer het SSL-certificaat met ASDM

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Procedure Verifiëren Problemen oplossen Hoe SSL-certificaten van de ene ASA naar de andere kopiëren Gerelateerde informatie

Inleiding

De procedure in dit document is een voorbeeld en kan als richtlijn worden gebruikt bij elke certificatenverkoper of uw eigen basiscertificeringsserver. Soms worden er speciale certificaateparameter-vereisten vereist door uw certificaathouder, maar dit document is bedoeld om de algemene stappen te leveren die vereist zijn om een SSL-certificaat te vernieuwen en het op een ASA te installeren die software 8.0 gebruikt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Deze procedure heeft betrekking op ASA versie 8.x met ASDM versie 6.0(2) of hoger.

De procedure in dit document is gebaseerd op een geldige configuratie met een certificaat dat is geïnstalleerd en gebruikt voor SSL VPN-toegang. Deze procedure heeft geen invloed op uw netwerk zolang het huidige certificaat niet wordt verwijderd. Deze procedure is een stap-voor-stap proces voor het uitgeven van een nieuw CSR voor een huidig certificaat met het zelfde wortelcertificaat dat de originele wortel CA verstrekte.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Procedure

Voer de volgende stappen uit:

1. Selecteer het certificaat dat u onder Configuratie > Apparaatbeheer > Identity Certificaten wilt verlengen en klik op **Toevoegen.Figuur 1**

🔂 Cisco ASDM 6.1 for ASA - 172	2.16.242.232				
<u>File Yew Tools Wizards Windo</u>	w <u>H</u> elp		Look For:	Go	ahaha
🎲 Home 🆓 Configuration 📴 M	Aonitoring 🔚 Sava 🔇 Refresh	🕒 Back 🕥 Forward P	Help		CISCO
Device Management 🗇 🕀 🔀	Configuration > Device Manage	ment > Certificate Manageme	ent > Identity Certificates		
문 🌈 Management Access 교 🗯 🛱 System Image/Configuration					
🖶 🎯 High Availability	Issued To	Issued By	Expiry Date	Usage	Add
🖶 🚮 Users/AAA	to the second	[01=H5+04] [1	10:00:015 01C Mar 11 2009	General Purpose	_ Show Details _
금 등을 Certificate Management - 월급 CA Certificates					Delete
E Pastic Certificates					Export
B DNS Advanced					Instal
					Refresh
	Identity certificate can be used to to make such configuration.	o authenticate SSL, such as ASDM,	access to the security appliance	on a given interface. You can go	to <u>SS. Settings</u>
🛃 Device Setup					
👯 Firowali					
Remote Access VPN					
🙀 Ske-to-Site VPN					
Device Management					
2		Ap	By Reset		
Device configuration refreshed successfu	uly.		tiscol 15	🗟 🛃 📊 🔛 🖓	29/08 8:52:53 PM UTC

 Selecteer onder Add Identity Certificate (identiteitsbewijs) de radioknop Add a new Identity Certificate en kies uw sleutelpaar in het vervolgkeuzemenu.Opmerking: het is niet aanbevolen om <Default-RSA-Key> te gebruiken, omdat als u de SSH-toets regenereert, u het certificaat ongeldig maakt. Als u geen RSA-toets hebt, moet u stappen a en b voltooien. Ga verder met Stap 3.Figuur 2

🖆 Add Identity Certificat	e		
 Import the identity certif 	icate from a file:		
Decryption Passphrase:			
File to Import From:		Browse	
 Add a new identity certif 	icate:		
Key Pair:	CertKey	Show	New
Certificate Subject DN:	ASA5540.company.com	Select	
🔲 Generate self-signed	certificate		
Act as local certif	icate authority and issue dynamic ce	ertificates to TLS-P	roxy
		_	
			Advanced
Add Certifi	cate Cancel	Help	ļ

(Optioneel) Voltooi deze stappen als u nog geen RSA-toets hebt ingesteld en anders naar Stap 3 overslaat.Klik op **Nieuw...**Voer de naam van het sleutelpaar in het veld **Nieuwe naam van het nieuwe sleutelpaar in** en klik op **Nu genereren.Figuur 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. Klik op Selecteren.
- 4. Voer de juiste certificeringseigenschappen in zoals in afbeelding 4. Klik na voltooiing op **OK**. Klik vervolgens op **Certificaat toevoegen.Figuur 4**

	🖆 Certificate Su	ubject DN				×
DN Attribute to be Added Add>> Attribute: Common Name (CN) Add>> Value: Common Name (CN) Add>> Value: Common Name (O) Cos Systems Delete Delete State (St) Coation (L) Email Address (EA) OK Cancel Help	DN Attribute Attribute: Value:	to be Added Common Name (CN) Common Name (CN) Department (OU) Company Name (O) Country (C) State (St) Location (L) Email Address (EA)	Add>> Delete	Attribute Common Name (CN) Department (OU) Company Name (O) Country (C) State (St) Help	Value ASA5540.comp LAB Cisco Systems US CA	

CLI-uitvoer:

pto 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
ypto ca enroll ASDM_TrustPoint0

5. Sla in het dialoogvenster **Identity certificaataanvraag** op (CSR) in een tekstbestand en klik op OK.Afbeelding 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. (Optioneel) Controleer in ASDM of de CSR in behandeling is, zoals in afbeelding 6. Figuur 6

🕵 Cisco ASDM 6.1 for ASA - 172	2.16.242.232				
<u>File Yew Tools Wizards Window</u>	w <u>H</u> elp		Look Far:	Go	duala
📣 Home 🙈 Configuration 🔯 M	lonitoring 🛄 Save 💦 Refresh	Back C Forward	Help		cisco
Device Management AL A	Configuration > Device Manag	ement > Certificate Manager	nent > Identity Fertificates		
E- 🐨 Management Access	Comparison of the Contract Office		inelity of an additional and additional		
🖶 😂 System Image/Configuration					
🖶 🥪 High Availability	Issued To	Issued By	Expiry Date	Usage	Add
🖶 🚮 Logging	[A5A5540.company.com]	[Not Available]	Panding	Unknown	. Show Details
🖃 🔛 Certificate Management					Delete
CA Certificates					Event
B 💕 DHCP					estrac
Advanced					Instal
					Refresh
	Identity certificate can be used	to authenticate SSL, such as ASD	N, access to the security appliance	on a given interface. You can go	to <u>55. Settinos</u>
	to make such configuration.				
Bevice Setup					
📆 Firewal					
Remote Access VPN					
🙀 Site-to-Site VPN					
Device Management					
20 *			pply Reset		
Configuration changes saved successfully	ń.		ciscol 15	🗟 🛃 🚹 🔛 🔒 🕸	29/08 9:56:23 PM UTC

- 7. Dien het certificaatverzoek in bij de certificaatbeheerder, die het certificaat op de server afgeeft. Dit kan via een web interface, e-mail of rechtstreeks naar de root CA server worden verzonden voor het uitgeven van certificaten.
- 8. Voltooi deze stappen om het hernieuwde certificaat te installeren.Selecteer het hangende certificaatverzoek onder Configuration > Apparaatbeheer > Identity Certificaten, zoals in afbeelding 6, en klik op Install.Selecteer in het venster Installeer Identity Certificate de certificaatgegevens in het radioknop van de basis-64-indeling en klik op Installeer.N.B.: Als het certificaat ook wordt afgegeven in een .cer-bestand in plaats van in een tekstbestand of een e-mail, kunt u ook Installeer uit een bestand selecteren, naar het juiste bestand op uw pc bladeren, op Installeer ID-certificaatbestand klikken en vervolgens op Installeer.Figuur 7

🖆 Install Identity certificate 🛛 🛛
Identity CertificateBrowse
• 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-uitvoer:

crypto ca import ASDM_TrustPoint0 certificate

 $\tt WIID2DCCAsCgAwIBAgIKYb9 wewAAAAAAJzANBgkqhkiG9 w0 BAQUFADAQMQ$

!--- output truncated wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit

9. Het venster verschijnt waarin wordt bevestigd dat het certificaat is geïnstalleerd. Klik op "OK"

🕵 Informa	tion 🔀	
į	Certificate import succeeded.	
	ОК	

om dit te bevestigen.Figuur 8

10. Zorg ervoor dat uw nieuwe certificaat onder Identity Services Engine verschijnt. Afbeelding 9

🚰 Cisco ASDM 6.1 for ASA - 172	16.242.232					
<u>Fi</u> le <u>W</u> ew <u>T</u> ools Wigards <u>W</u> indow	v <u>H</u> elp			Look Far:		©lulu
🚮 Home 🍕 Configuration 🔯 M	onitoring 🔚 Sava 🔇 R	efresh 🕝 Back 🕥	Forward 💡 Help			CISCO
Device Management	Configuration > Device N	lanagement > Certific	ate Management >	Identity Certificat	<u>e</u>	
🖻 👔 Management Access						
System Image/Configuration	Issued To	Issued By	Expiry	Date	Usace	Add
E Logging	[on=*.vpn1.com]	[cn=MS-CA]	00:03:	16 UTC Mar 11 2009	General Purpose	Chan Databa
🖶 🚱 Users(AAA	[cn=A5A5540.company.c	com, [cn=MS-CA]	22:49:	31 UTC Aug 29 2009	General Purpose	200W Decals
- A Certificates						Delete
dentity Certificates						Export
B B DNS						Instal
🗊 🛐 Advanced						Befrech
	Identity certificate can be	e used to authenticate SS	L, such as ASDM, acces	s to the security appl	lance on a given interface. You	can go to 55, Settings
	to make such configuration	on.				
0						
Device Setup						
📆 Frewal						
Remote Access VPN						
🙀 Site-to-Site VPN						
Device Management						
*			Apply	Reset		
Configuration changes saved successfully	r		cisco 1	15		මු 8/29/08 10:05:53 PM UTC

11. Voltooi deze stappen om het nieuwe certificaat aan de interface te binden:Kies Configuratie
 > Apparaatbeheer > Geavanceerd > SSL-instellingen, zoals in afbeelding 10.Selecteer uw interface onder Certificaten en klik op Bewerken.Afbeelding 10

🚰 Cisco ASDM 6.1 for ASA - 172	.16.242.232				
File Yew Tools Wigards Window	v Help		Look Par:	G	• dealer
🚳 Home 🦓 Configuration 📴 M	onitoring 🔚 Sava 🔇 Re	fresh 🔇 Back 🕥 Forward 🢡	Help		CISCO
Device Management 🗗 🕀 🗡	Configuration > Device M	anagement > Advanced > SSL Set	tings		
Management Access System Image/Configuration High Availability Logging GetRicate Management Second Certificates Second Certificates Second Certificates Second Certificates Second Certificates Advanced Second Certificates Second Certificates	Configure SSL pavameters. T Server SSL Version: Any Encryption Available Algorithms RC DCS Certificates Specify which certificates, associated with a certificates	These parameters affect both ASOM and Clent 55L Version: Ar 4405 53HAL if any, should be used for SSL authentic te of their own.	SSL VFN access. y Active Algorian emove 1 active Algorian emove 2 active Algo	tims RC4-SHA1 AES128-SHA1 AES256-SHA1 30ES-SHA1 30ES-SHA1 stellbeck certificate will be used on int	Mave Up :: Move Down
SS. Settings	Interface	Trucknoint	Load Palanci	na Tuurtaalat	Edt
E- WCC+	Incide	indscholler.	Local balance	ng masipalik	
	outside	(or-1.ven).con)(or-45	541 61 f}		
💑 Device Setup					
Freval					
Remote Access VPN	Falback Certificate: •• No	ne	*		
Ste-to-Ste VPN			poly Reset		
 Configuration changes saved a recessful. 	·		riscol 15	B B D A.	(29/08 10:08:53 PM LITC
Contrajor Contra o rengeo por es successi dij			10		and a response of the

- 12. Kies uw nieuwe certificaat in het vervolgkeuzemenu, klik op OK en klik op Toepassen. ssl encryption rc4-shal aes128-shal aes256-shal 3des-shal
 - ssl trust-point ASDM_TrustPoint0 outside

Afbeelding 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=M5-CA]: 611f8630000000000026 [cn=ASA5540.company.com, ou=LAB, o=Cisco Systems,				

13. Bewaar uw configuratie in ofwel ASDM ofwel in de CLI.

Verifiëren

U kunt de CLI-interface gebruiken om te controleren of het nieuwe certificaat correct in de ASA is geïnstalleerd, zoals in deze voorbeelduitvoer wordt weergegeven:

```
ASA(config)#show crypto ca certificates
Certificate
Status: Available
Certificate Serial Number: 61bf707b000000000027
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)#

Problemen oplossen

(Optioneel) Controleer op de CLI of het juiste certificaat op de interface wordt toegepast:

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)#

Hoe SSL-certificaten van de ene ASA naar de andere kopiëren

Dit kan als je exportbare sleutels had gegenereerd. U moet het certificaat exporteren naar een PKCS-bestand. Dit houdt in dat alle bijbehorende sleutels moeten worden geëxporteerd.

Gebruik deze opdracht om uw certificaat via CLI te exporteren:

ASA(config)#crypto ca export

Opmerking: Wachtwoord - gebruikt om het bestand pkcs12 te beschermen.

Gebruik deze opdracht om uw certificaat te importeren via CLI:

SA(config)#crypto ca import

N.B.: Dit wachtwoord dient hetzelfde te zijn als bij het exporteren van het bestand.

Dit kan ook via ASDM worden gedaan voor een ASA failover-paar. Volg deze stappen om dit uit te voeren:

- 1. Meld u aan bij de primaire ASA via ASDM en kies Gereedschappen--> Back-upconfiguratie.
- 2. U kunt back-ups maken van alles of alleen van de certificaten.
- 3. Open ASDM in de standby-modus en kies Gereedschappen ---> Herstel de configuratie.

Gerelateerde informatie

- Ondersteuning van Cisco-pagina voor adaptieve security applicatie (ASA)
- <u>ASA 8.x Installeer Verkrakers van 3 partijen handmatig voor gebruik met WebVPN-</u> <u>configuratievoorbeeld</u>
- <u>Technische ondersteuning en documentatie Cisco Systems</u>