ASA 8.x: Verlängern und Installieren des SSL-Zertifikats mit ASDM

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Vorgehensweise Überprüfen Fehlerbehebung Kopieren von SSL-Zertifikaten von einer ASA in eine andere Zugehörige Informationen

Einführung

Das Verfahren in diesem Dokument ist ein Beispiel und kann als Richtlinie für jeden Zertifikatanbieter oder Ihren eigenen Stammzertifikatserver verwendet werden. In manchen Fällen sind vom Zertifikatanbieter spezielle Zertifizierungsparameter erforderlich. Dieses Dokument enthält jedoch die allgemeinen Schritte, die erforderlich sind, um ein SSL-Zertifikat zu verlängern und auf einer ASA zu installieren, die 8.0-Software verwendet.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Verfahren bezieht sich auf ASA 8.x mit ASDM Version 6.0(2) oder höher.

Das Verfahren in diesem Dokument basiert auf einer gültigen Konfiguration mit einem installierten und für den SSL VPN-Zugriff verwendeten Zertifikat. Dieses Verfahren hat keine Auswirkungen auf Ihr Netzwerk, solange das aktuelle Zertifikat nicht gelöscht wird. Dieses Verfahren beschreibt Schritt für Schritt, wie ein neuer CSR für ein aktuelles Zertifikat mit demselben Root-Zertifikat ausgegeben wird, das die ursprüngliche Root-Zertifizierungsstelle ausgestellt hat.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Vorgehensweise

Gehen Sie wie folgt vor:

 Wählen Sie das Zertifikat aus, das Sie verlängern möchten, unter Konfiguration > Gerätemanagement > Identitätszertifikate, und klicken Sie dann auf Hinzufügen Abbildung 1

🔂 Cisco ASDM 6.1 for ASA - 173	2.16.242.232				
<u>File Yew Tools Wigards Windo</u>	w Help		Look Par:	Go	alada
🛃 Home 🦓 Configuration 🔯 M	fonitoring 🔚 Save 🔇 Refresh	C Back C Forward	🦻 нар		cisco
Device Management B P ×	Configuration > Device Manage	ement > Certificate Mana	gement > Identity Certificates		
🖶 👰 Management Access					
🖶 🏀 System Image/Configuration	Issued To	Issued By	Expiry Date	Usage	Add
E Coging	[m=*spnt.com]	[m=MS-CA]	00:03:16 UTC Nar 11 2009	General Purpose	Show Datata
🖶 👘 Users(AAA 🖃 🗐 Certificate Management					20040548
CA Certificates					Delete
The photoe in the second secon					Export
🕀 📑 DNS					Instal
a Shaaraa					Refresh
	Identity certificate cap be used (n authenticate 931, such as :	1900, arress to the security applianc	e op e diveo joherface. You cao co	to SN Settings
	to make such configuration.			a an a grait i kanacat toa tan gi	
A Device Setup					
📆 Fyroxall					
Remote Access VPN					
🔗 Site-to-Site VPN	_				
Device Management					
*			Apply Reset		
Device configuration refreshed successfu	uly.		riscol 15	🗟 🛃 📊 🔒 🕯	/29/08 8:52:53 PM UTC

2. Wählen Sie unter Identitätszertifikat hinzufügen die Optionsschaltfläche Neues Identitätszertifikat hinzufügen, und wählen Sie das Schlüsselpaar aus dem Dropdown-Menü aus.Hinweis: Es wird nicht empfohlen, <Default-RSA-Key> zu verwenden, da Sie das Zertifikat ungültig machen, wenn Sie Ihren SSH-Schlüssel neu generieren. Wenn Sie keinen RSA-Schlüssel haben, führen Sie die Schritte a und b aus. Fahren Sie andernfalls mit Schritt 3 fort.Abbildung 2

Add Identity Certificat	e	
 Import the identity certification 	icate from a file:	
Decryption Passphrase:		
File to Import From:		Browse
 Add a new identity certification 	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-Proxy
		Advanced
Add Certifi	cate Cancel	Help

(Optional) Führen Sie diese Schritte aus, wenn Sie noch keinen RSA-Schlüssel konfiguriert haben. Fahren Sie andernfalls mit Schritt 3 fort.Klicken Sie auf **Neu.**..Geben Sie den Namen des Schlüsselpaars in das Feld **Name des neuen Schlüsselpaars eingeben ein**, und klicken Sie auf **Jetzt generieren.Abbildung 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. Klicken Sie auf Auswählen.
- 4. Geben Sie die entsprechenden Zertifikatsattribute ein (siehe Abbildung 4). Klicken Sie abschließend auf **OK**. Klicken Sie anschließend auf **Zertifikat hinzufügen.Abbildung 4**

📧 Cert	ificate Su	ıbject DN				×
	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)	Value ASA5540.comp LAB Cisco Systems US CA	
		ОК	Cancel	Help		

CLI-Ausgabe:

crypto	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. Speichern Sie im Popup-Fenster **Identity Certificate Request** (Identitätszertifikatanforderung) Ihre Zertifikatsanforderung (CSR) in einer Textdatei, und klicken Sie auf **OK**.**Abbildung 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. (Optional) Überprüfen Sie im ASDM, dass die CSR aussteht, wie in Abbildung 6 gezeigt. **Abbildung 6**

🕵 Cisco ASDM 6.1 for ASA - 172	16.242.232				
<u>File Mew Tools Wigards Window</u>	- Help		Look Far:	Go	alada
🛃 Home 🙈 Configuration 🔯 Mo	initoring 🔚 Sava 💽 Re	dresh 🔇 Back 🕥 Forward	🦻 Help		cisco
Device Management 🗗 🕂 🗡	Configuration > Device M	anagement > Certificate Ma	nagement > Identity Certificates		
🖶 🌈 Management Access					
🖶 🥵 System Image/Configuration	Test and To	James' Ro	Enniry Date	lisane	Add
E Coging	[on=".spn1.com]	[m=MS-CA]	00:03:16 UTC Mar 11 2009	General Purpose	
🖶 🚮 Users(AAA	[ASA5540.company.com]	[Not Available]	Panding	Unknown	Show Details
- An Certificates					Delete
Certificates					Export
B B DNS					Instal
🗉 📆 Advanced					Befresh
	Identity certificate can be	used to authenticate SSL, such a	is ASDM, access to the security appliar	roe on a given interface. You can go	to <u>SS. Settinos</u>
	to make such configuratio	n.			
💑 Device Setup					
📆 Fyronal					
Remote Access VPN					
🚰 Site-to-Site VPN					
Device Management					
20			Apply Reset		
Configuration changes saved successfully			ciscol 15		/29/08 9:56:23 PM UTC

- 7. Senden Sie die Zertifikatsanforderung an den Zertifikatadministrator, der das Zertifikat auf dem Server ausstellt. Dies kann entweder über eine Webschnittstelle, per E-Mail oder direkt an den Stammserver der Zertifizierungsstelle erfolgen, um das Zertifikat auszustellen.
- 8. Führen Sie diese Schritte aus, um das erneuerte Zertifikat zu installieren.Wählen Sie die ausstehende Zertifikatsanforderung unter Configuration > Device Management > Identity Certificates (Konfiguration > Gerätemanagement > Identitätszertifikate) aus, wie in Abbildung 6 dargestellt, und klicken Sie auf Install (Installieren).Wählen Sie im Fenster Identitätszertifikat installieren das Optionsfeld Zertifikatsdaten in Base-64-Format einfügen aus, und klicken Sie auf Zertifikat installieren.Hinweis: Wenn das Zertifikat nicht in einer textbasierten Datei oder per E-Mail, sondern in einer CSER-Datei ausgegeben wird, können Sie auch Aus einer Datei installieren auswählen, die entsprechende Datei auf Ihrem PC aufrufen, auf ID-Zertifikatsdatei installieren klicken und dann auf Zertifikat installieren.Abbildung 7

🖆 Install Identity certificate	×
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-Ausgabe:

crypto ca import ASDM_TrustPoint0 certificate

 $\tt WIID2DCCAsCgAwIBAgIKYb9 wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ$

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

9. Es wird ein Fenster angezeigt, das bestätigt, dass das Zertifikat erfolgreich installiert wurde. Klicken Sie zur Bestätigung auf "OK". Abbildung 8

🕵 Informat	tion	×
į	Certificate import succeeded.	
	ОК	

10. Stellen Sie sicher, dass Ihr neues Zertifikat unter Identitätszertifikate angezeigt wird. Abbildung 9

🕵 Cisco ASDM 6.1 for ASA - 172	16.242.232					
<u>File Yew Tools Wigards Window</u>	w <u>H</u> elp			Look Far:		© alate
📣 Home 🙈 Configuration 🔯 M	lonitoring 🛄 Sava 🕼	Refresh 🙆 Back 🕥	Forward 🦻 Help			cisco
Device Management -1 1 X	Configuration > Devi	re Management > Factif	e ata Managamant '	Identity Cartificate		cisco
E Management Access	Company Science - Perty	een harrasperinens er sen sin	NAME PROPAGATION A	and the second second		
B 🔂 System Image/Configuration						
🖶 🎯 High Availability	Issued To	Issued By	Espir	y Dabe	Usage	Add
H- Coging	[on=".apn1.com]	[cn=MS-CA]	22:40	:16 UTC Mar 11 2009	General Purpose General Purpose	Show Details
🖶 🛃 Certificate Management	Personal States and St	an teacher francisco a	Derty	ins one may as abos	Contra la Fica poco	Delete
CA Certificates						
						Export
B A DNS						Instal
m 23 wavancea						Refresh
	Identity certificate c	ap he used to authenticate 5	51 . such as 05004, acres	ss to the security apple	ance on a given interface. You	ran on to 55. Settings
	to make such config.	nation.				can go to <u>alla socia bar</u>
💑 Device Setup						
👯 Firovali						
Remote Access VPN						
🚰 Ske-to-Site VPN						
Device Management						
2			Apply	Reset		
Configuration changes saved successfully	6		cisco 1	15	B 🛃 🖬 🚺	🔒 8/29/08 10:05:53 PM UTC

11. Gehen Sie wie folgt vor, um das neue Zertifikat an die Schnittstelle zu binden:Wählen Sie Configuration > Device Management > Advanced > SSL Settings (Konfiguration > Gerätemanagement > Erweitert > SSL-Einstellungen) aus, wie in Abbildung 10 dargestellt.Wählen Sie Ihre Schnittstelle unter Zertifikate aus, und klicken Sie auf Bearbeiten.Abbildung 10

GCisco ASDM 6.1 for ASA - 172	.16.242.232				
File Yew Tools Wizards Window	v Help			Look For:	© de de
🚮 Home 🦓 Configuration 📴 M	onitoring 🔚 Sava 🔇 R	efresh 🔇 Back 🔘 Forward	🥐 Help		CISCO
Device Management 🗇 🕀 🔀	Configuration > Device !	lanagement > Advanced > 55	Settings		
Management Access System Image (Configuration High Availability Leoging Gentificate Management Sign Cartificates Monocol Advanced Ackanced Sign Accentificates Sign Accentificates Monocol Sign Accentificates Sign A	Configure SSL parameters. Server SSL Version: Any Encryption Available Algorithms Certificates Specify which certificates	These parameters affect both ASDM Client SSL Version 44405 S-SHAL , if any, should be used for SSL auth	and SS. VPN access. Add >> Add >> Ad	tive Algorithms RC4-SHA1 AES128-SHA1 AES256-SHA1 3CES-SHA3 arface. The fallback certificate will be us	Move Up () Move Down
Priority Queue	associated with a certific	ate of their own.			
E-	Interface	Trustpoint	Lo	ad Balancing Trustpoint	Edit
	outside	fortorni.com}i(or	Logica) suitu		
💑 Device Setup					
Remote Access VPN	Falback Certificate:	lone -		~	
Carlos Ste VPN		(Apply R	eset	
Configuration changes saved successfully	r		cisco 1	15 📑 🛃 🔂	🔒 8/29/06 10:08:53 PM UTC

12. Wählen Sie aus dem Dropdown-Menü Ihr neues Zertifikat aus, klicken Sie auf **OK**, und klicken Sie auf **Übernehmen**.

ssl encryption rc4-shal aes128-shal aes256-shal 3des-shal ssl trust-point ASDM_TrustPoint0 outside						
Abbildung 11						
🖆 Select SSL Certificate	🖆 Select SSL Certificate 🛛 🛛 🔀					
Specify enrolled trustpoints to be use interface. To enroll a trustpoint, go t Certificate > Enrollment.	ed for SSL authentication and VPN load balancing on the outside :o Configuration > Features > Device Administration >					
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]: 611f8630000000000026 [cn=ASA5540.company.com, ou=LAB, o=Cisco Systems,					

13. Speichern Sie Ihre Konfiguration entweder im ASDM oder in der CLI.

<u>Überprüfen</u>

Sie können die CLI-Schnittstelle verwenden, um zu überprüfen, ob das neue Zertifikat korrekt auf

```
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-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)#

Fehlerbehebung

(Optional) Überprüfen Sie in der CLI, ob das richtige Zertifikat auf die Schnittstelle angewendet wird:

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)#

Kopieren von SSL-Zertifikaten von einer ASA in eine andere

Dies ist möglich, wenn Sie exportierbare Schlüssel generiert haben. Sie müssen das Zertifikat in eine PKCS-Datei exportieren. Dazu gehört auch der Export aller zugeordneten Schlüssel.

Verwenden Sie diesen Befehl, um das Zertifikat über die CLI zu exportieren:

ASA(config)#crypto ca export

Hinweis: Passphrase - wird zum Schutz der Datei pkcs12 verwendet.

Verwenden Sie diesen Befehl, um das Zertifikat über die CLI zu importieren:

Hinweis: Diese Passphrase sollte mit der beim Exportieren der Datei verwendeten Passphrase identisch sein.

Dies kann auch über ASDM für ein ASA-Failover-Paar erfolgen. Gehen Sie wie folgt vor:

- 1. Melden Sie sich über ASDM bei der primären ASA an, und wählen Sie **Tools -> Backup Configuration aus**.
- 2. Sie können alles oder nur die Zertifikate sichern.
- 3. Öffnen Sie im Standby-Modus ASDM, und wählen Sie **Tools -> Restore Configuration** (Konfiguration wiederherstellen) aus.

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliance (ASA)
- <u>ASA 8.x Manuelles Installieren von Drittanbieter-Zertifikaten zur Verwendung mit WebVPN -</u> <u>Konfigurationsbeispiel</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>