ASA 8.x: ASDM を使用した SSL 証明書の更新 とインストール

目次

<u>概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>表記法</u> <u>手順</u> <u>確認</u> <u>トラブルシューティング</u> <u>SSL 証明書を ASA から他の ASA ヘコピーする方法</u> 関連情報

概要

このドキュメントの手順は、1 つの例であり、任意の証明書ベンダーまたは独自のルート証明書 サーバを使用する場合のガイドラインとして使用できます。 証明書ベンダーが特定の証明書パラ メータ要件を必要とすることがありますが、本ドキュメントの目的は SSL 証明書更新および 8.0 ソフトウェアを使用する ASA へのインストールのための一般的な手順を示すことです。

<u>前提条件</u>

<u>要件</u>

このドキュメントに関する固有の要件はありません。

<u>使用するコンポーネント</u>

この手順は、ASA バージョン 8.x および ASDM バージョン 6.0(2) 以降に適用されます。

本ドキュメントの手順は、証明書がインストールされ SSL VPN アクセスに使用される、有効な 設定に基づいています。 この手順は、現在の証明書を削除しない限りネットワークに影響を与え ません。 手順では、オリジナルのルート CA を発行したものと同じルート証明書を使用して、現 在の証明書の新しい CSR を発行する方法をステップごとに説明します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があり ます。 ドキュメント表記の詳細は、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してください。

<u>手順</u>

次の手順を実行します。

1. 更新する証明書の下の [Configuration] > [Device Management] > [Identity Certificates] を順に 選択し、[Add] をクリックします。図 1

🔂 Cisco ASDM 6.1 for ASA - 172	72.16.242.232	
<u>File Mew Tools Wigards Window</u>	dow Help Look For:	62 allerthe
🚮 Home 🦓 Configuration 🔯 M	Monitoring 🥁 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help	CISCO
Device Management 🗇 🕀 🗵	Configuration > Device Management > Certificate Management > Identity Certificates	
Management Access System Image/Configuration High Availability Logging Gild Users/AAA Certificate Management Gild Certificates Gild Certificates Move DNIS Move DNIS Move DNIS	Issued To Issued By Expiry Date Usage [cr=**epril.com] [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] 00:03:15 UTC Mar 11 2009 General Purpose Issued To [cr=MS-CA] [cr=MS-CA] [cr=MS-CA] Issued To [cr=MS-CA] [cr=MS-CA] [cr=MS-CA] Issued To [cr=MS-CA] [cr=MS-CA] [cr=MS-CA] Issued To [cr=MS-CA] [cr=MS-CA] [cr=MS-CA]	Add Show Details Delete Esport Instal Refresh
Bevice Setup		
👬 Fronal		
Remote Access VPN		
🙀 Ske-to-Site VPN		
Device Management		
?	Apply Reset	
Device configuration refreshed successfu	sfully. riscol 15 🔝 🔜 👔	🖥 8/29/08 8:52:53 PM UTC

 [Add Identity Certificate] で、[Add a new identity certificate] オプション ボタンを選択し、ドロップダウン メニューからキー ペアを選択します。注: ご利用の SSH キーを再生成するとその証明書が無効になるため、<Default-RSA-Key> を使用することは推奨されません。 RSA キーがない場合は、ステップ a と b を実行します。 それ以外の場合は、ステップ 3 に進みます。図 2

🖆 Add Identity Certificat	e	X
 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-Proxy
		Advanced
Add Certifi	cate Cancel	Help

(オプション)RSA キーがまだ設定されていない場合は、次のステップを実行し、それ以 外の場合はステップ 3 に進みます。[New] をクリックします。[Enter new key pair name] フ ィールドにキー ペアの名前を入力し、[Generate Now] をクリックします。図3

🖆 Add Key Pair			
Name:	🚫 Use default key pair name		
	Enter new key pair name: Certkey		
Size:	1024		
Usage:	💿 General purpose 💦 Special		
G	Senerate Now Cancel Help		

- 3. [Select] をクリックします。
- 4. 図 4 に示すように、該当する証明書の属性を入力します。 終了したら、[OK] をクリックします。 次に、[Add Certificate] をクリックします。図 4

🚰 Certificate Subject DN					X	
DN A Att Vali	ttribute ribute: ue:	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 の出力:

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

5. [Identity Certificate Request] ポップアップ ウィンドウで、Certificate Signing Request (CSR; 証明書署名要求) をテキスト ファイルに保存し、[OK] をクリックします。

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	
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	
Save CSR to file: C:\Certificates\ASACertCSR.txt Browse	
OK Cancel Help	

🔂 Cisco ASDM 6.1 for ASA - 172.	16.242.232				
<u>File Yew Tools Wigards Window</u>	Fielb		Look Far:	65	alah
🚮 Home 🙈 Configuration 🔯 Mo	nitoring 🔚 Save 🔇 R	efresh 🔇 Back 🕥 Forwe	rd 🦻 Help		cisco
Device Management = + ×	Configuration > Device N	Management > Certificate M	anagement > Identity Certificates	L	
🖬 🌈 Management Access					
🖶 🥵 System Image/Configuration	Jee red To	Jacuard For	Everieu Date	Ukana	
H Logana	[on=".spnt.com]	[m=M5-CA]	00:03:16 UTC Mar 11 2009	General Purpose	
🖶 🚮 Users(AAA	[A5A5540.company.com] [Not Available]	Pending	Unknown	. Show Details
Certhicate Management Sector Certificates					Delete
dentity Certificates					Export
E A DHCP					Instal
🗉 📆 Advanced					Laford .
					Nerresh
	Identity certificate can b	e used to authenticate SSL, such	as ASDM, access to the security appliar	rce on a given interface. You can do	to 55. Settinos
	to make such configurati	on.			
Device Setup					
👯 Firewal					
Remote Access VPN					
🙀 Ske-to-Site VPN					
Device Management					
*			Apply Reset		
Configuration changes saved successfully			ciscol 15		29/08 9:56:23 PM UTC

- 7. 証明書要求を証明書管理者に送信します。証明書管理者は、サーバで証明書を発行します。 これは、Web インターフェイス、電子メールを使用しても可能であり、または直接、証明 書発行プロセスのルート CA サーバへも送信できます。
- 8. 更新された証明書をインストールするには、次のステップを実行します。図 6 に示すように 、[Configuration] > [Device Management] > [Identity Certificates] の下にある保留状態の証明 書要求を選択し、[Install] をクリックします。[Install Identity Certificate] ウィンドウで、 [Paste the certificate data in base-64 format] オプションボタンを選択し、[Install Certificate] をクリックします。注: あるいは、証明書がテキストベースのファイルまたは電子メールで はなく、.cer ファイルに発行された場合は、[Install from a file] を選択して該当する PC 上の ファイルを検索し、[Install ID certificate file] をクリックしてから [Install Certificate] をクリ ックします。図 7

🖆 Install Identity certificate	×
Identity Certificate	
O Install from a file: Browse	
O 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 の出力:

リックして確定します。図

crypto ca import ASDM_TrustPoint0 certificate

WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ !--- output truncated wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa 6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit

9. 証明書が正常にインストールされたことを確認するウィンドウが表示されます。 [OK] をク

🕵 li	🖆 Information		
(i	Certificate import succeeded.	
8		ОК	

10. 新しい証明書が [Identity Certificates] に表示されることを確認します。図 9

🔂 Cisco ASDM 6.1 for ASA - 172.	16.242.232				
Ele Yew Tools Wigards Window	Help		Look Par:	Go	alada
📣 Home 🙈 Configuration 🔯 Mor	nitoring 🛄 Sava 🙉 R	tefresh 🙆 Back 🕥 Forma	rd 🦻 Help		cisco
Device Management 41 A X	Configuration > Device (Management > Certificate N	ananement > Identity Certificat	es	
E P Management Access	Contractor structure and the structure	The inspection of the second second second	PRINTER AND A PRINTED AND AND AND AND AND AND AND AND AND AN		
🖶 🍰 System Image/Configuration					
🖶 🎯 High Availability	Issued To	Issued By	Expiry Date	Usage	Add
H Coging	[cr=1.vpn1.com] [cr=4545540.company.	[m=MS-CA]	22:49:31 UTC Aut 29 2009	General Purpose General Purpose	Show Details
🖶 🛃 Certificate Management					Delete
B P DHOP					Espore
Achapced					Instal
0 20 Horaco					Refresh
	Identity certificate can b	e used to authenticate SSL, sud	n as ASDM, access to the security appl	ance on a given interface. You can g	o to <u>SSL Settings</u>
	to make such configurati	ion.			
Revice Setup					
👯 Firewali					
Remote Access VPN					
🙀 Ste-to-Site VPN					
Device Management					
». •			Apply Reset		
Configuration changes saved successfully.			cisco1 15	🕞 🛃 🔂 🔒 👘	29/08 10:05:53 PM UTC

11. 新しい証明書をインターフェイスにバインドするには、次にステップを実行します。図 10 に示すように、[Configuration] > [Device Management] > [Advanced] > [SSL Settings] を順 に選択します。[Certificates] の下でインターフェイスを選択し、[Edit] をクリックします。 図 10

🖆 Cisco ASDM 6.1 for ASA - 172	.16.242.232				
Elle Yew Looks Wigards Window	v Help		Look Far:	Go	
🛃 Home 🦓 Configuration 📴 M	onitoring 🔚 Sava 🔇 R	efresh 🔇 Back 🔘 Forward 4	? нею		CISCO
Device Management 🗗 🕂 🗡	Configuration > Device N	tanagement > Advanced > 55L5	ettings		
Advanced Advanced	Configure SSL parameters. Server SSL Version: Any Encryption Available Algorithms DE Certificates Specify which certificates	These parameters affect both ASDM an Client SSL Version: 4-405 S-SHAL if any, should be used for SSL authentic	nd SSL VFN access. Any V Add >> Active Algorit Remove	hms RC4-SHA1 AES128-SHA1 AES256-SHA1 3DE5-SHA1 3DE5-SHA1	Move Up () Move Down
Phoney Queue	associated with a certifica	te of their own.			
E- 📲 WCCP	Interface	Trustpoint	Load Balancin	ng Trustpoint	Edit
Bento Setup	outside	for-front.conHor-6	5-04) 811()		
Firewall					
Remote Access VPN Reto-Site VPN Device Management	Falback Certificate: N	me	Apply Reset		
Configuration changes saved successfully	6		cisco1 15	🔝 🛃 🔂 🔒 🚳	9/08 10:08:53 PM UTC

12. ドロップダウン メニューから新しい証明書を選択し、[OK] をクリックし、[Apply] をクリ ックします。ssl encryption rc4-shal aes128-shal aes256-shal 3des-shal

ssl trust-point ASDM_TrustPoint0 outside 2 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	
ОК	[cn=ASA5540.company.com, ou=LAB, o=Cisco Systems,	

13. ASDM または CLI で設定を保存します。

<u>確認</u>

次のサンプル出力に示すように、CLI を使用して ASA に新しい証明書が正しくインストールされ たことを確認できます。

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:///\win2k3-base1\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-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)#

<u>トラブルシューティング</u>

(オプション)CLI で、正しい証明書がインターフェイスに適用されていることを確認します。

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)#

<u>SSL 証明書を ASA から他の ASA ヘコピーする方法</u>

これは、エクスポートできるキーを生成した場合に実行できます。 証明書を PKCS ファイルにエ クスポートする必要があります。 これには、関連付けられたすべてのキーのエクスポートが含ま れます。

CLI で証明書をエクスポートするには、次のコマンドを使用しします。

ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase> 注: パスフレーズ: pkcs12 ファイルを保護するために使用されます。

CLI で証明書をインポートするには、次のコマンドを使用します。

SA(config)#crypto ca import <trust-point-name> pkcs12 <passphrase> 注: このパスフレーズは、ファイルをエクスポートしたときに使用したものと同じでなければなり ません。

ASA フェールオーバー ペアの場合、SSL 証明書を ASA から他の ASA にコピーするには、 ASDM を使用することもできます。 それには次のステップを実行します。

- 1. プライマリ ASA に ASDM によってログインし、『Tools』 を選択 して下さい----> **バックア** ップコンフィギュレーション。
- 2. すべて、または証明書だけをバックアップできます。
- 3. スタンバイで、開いた ASDM は『Tools』 を選択 し、 ----> 復元 設定。

関連情報

- Cisco 適応型セキュリティ アプライアンスに関するサポート ページ
- ASA 8.x WebVPN で使用するサードパーティ ベンダーの証明書を手動でインストールする設 定例

・<u>テクニカルサポートとドキュメント - Cisco Systems</u>